



AssuredSAN 4000 Series Service Guide

Copyright © 2012 Dot Hill Systems Corp. All rights reserved. Dot Hill Systems Corp., Dot Hill, the Dot Hill logo, AssuredSAN, AssuredSnap, AssuredCopy, AssuredRemote, EcoStor, and SimulCache are trademarks of Dot Hill Systems Corp. All other trademarks and registered trademarks are proprietary to their respective owners.

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, changes in the product design can be made without reservation and without notification to its users.



Adobe PostScript

Contents

About this guide	13
Intended audience	13
Prerequisites	13
Related documentation	13
Document conventions and symbols	14
1 Fault isolation methodology	15
Basic steps	15
Options available for performing basic steps	15
Performing basic steps	16
Stopping I/O	17
2 Troubleshooting using RAIDar	19
Problems using RAIDar to access a storage system	19
Determining storage-system status	19
Viewing information about all vdisks	20
Viewing information about a vdisk	20
Vdisk properties	20
Disk properties	21
Viewing information about an enclosure	21
Enclosure properties	22
Disk properties	22
Power supply properties	23
Controller module properties	23
Controller module: network port properties	23
Controller module: host port properties	24
Controller module: expansion port properties	24
Controller module: CompactFlash properties	24
Drive enclosure: I/O module properties	24
I/O modules: In port properties	25
I/O modules: Out port properties	25
Viewing the system event log	25
Clearing disk metadata	26
Isolating faulty disk drives	27
Identifying a faulty disk drive	27
Reviewing the event logs	27
Reconstructing a vdisk	28
Using recovery utilities	28
Quarantining vdisks	28
Removing a vdisk from quarantine	29
Correcting enclosure IDs	30
Problems after power-on or restart	30
Problems with performance degradation	30
3 Troubleshooting using the CLI	33
Isolating data path faults	33
Changing fault isolation settings	33
Resetting expander error counters	33
Disabling or enabling a PHY	33
Disabling or enabling PHY isolation	33
Isolating internal data path faults	34
Checking PHY status	34
Resolving PHY faults	34
Isolating external data path faults	35

Resolving external data path faults	35
Resetting a host channel on an FC storage system	35
Problems with performance degradation	35
Problems scheduling tasks	36
Errors associated with scheduling tasks	37
Deleting schedules and tasks	37
Command reference	37
Viewing help	37
Missing parameter data error	37
abort scrub	38
clear cache	38
clear disk-metadata	39
clear events	40
clear expander-status	40
create schedule	41
create task	42
delete schedule	43
delete task	43
rescan	43
reset host-link	44
restart	44
restore defaults	45
scrub vdisk	46
set advanced-settings	47
set debug-log-parameters	51
set expander-fault-isolation	52
set expander-phy	53
set led	54
set protocols	55
show controller-statistics	56
show debug-log-parameters	58
show disk-statistics	59
show events	63
show expander-status	66
show frus	69
show host-parameters	71
show host-port-statistics	72
show protocols	74
show redundancy-mode	75
show sensor-status	76
show vdisk-statistics	79
show volume-statistics	83
trust	84
4 Troubleshooting using event logs	87
Events and event messages	87
Reviewing events	87
Viewing the event log in the CLI	87
Viewing the event log in RAIDar	87
Saving log information to a file	88
Viewing an event log saved from RAIDar	89
5 Troubleshooting using system LEDs	91
Using enclosure status LEDs – front panel	91
Using disk drive module LEDs – front panel	91
Using controller module host port LEDs – rear panel	92
Using the controller module expansion port status LED – rear panel	92
Using controller module network port LEDs – rear panel	92
Using controller module status LEDs – rear panel	93

Using PSU LEDs – rear panel	93
Using expansion module LEDs – rear panel	94
Diagnostic steps	94
Is the enclosure front panel “Fault/Service Required” LED amber?	95
Is the controller rear panel “FRU OK” LED lit?	95
Is the controller rear panel “Fault/Service Required” LED amber?	95
Are both disk drive module LEDs off?	95
Is the disk drive module “Fault” LED amber?	96
Is a connected host port’s “Host Link Status” LED lit?	96
Is a connected port’s “Expansion Port Status” LED lit?	97
Is a connected port’s “Network Port Link Status” LED lit?	97
Is the PSU’s “Input Power Source” LED lit?	97
Is the “Voltage/Fan Fault/Service Required” LED amber?	98
Isolating a host-side connection fault	98
Isolating a controller module expansion port connection fault	100
6 Troubleshooting and replacing FRUs	103
ESD	103
Preventing ESD	103
Grounding methods to prevent ESD	103
Replacing chassis FRU components	104
Replacing a controller module or expansion module	104
Before you begin	105
Configuring PFU	105
Verifying component failure	106
Stopping I/O	106
Shutting down a controller module	106
Removing a controller module or expansion module	107
Installing a controller module or expansion module	108
Verifying component operation	110
Swapping controllers in the same enclosure	110
Updating firmware	111
Updating controller module firmware using RAIDar	111
Updating controller module firmware using FTP	112
Updating expansion module firmware using RAIDar	114
Updating expansion module firmware using FTP	114
Identifying cable faults	115
Identifying cable faults on the host side	116
Identifying cable faults on the drive enclosure side	116
Disconnecting and reconnecting SAS cables	116
Identifying disk drive module faults	116
Understanding disk-related errors	117
Disk drive errors	118
Disk channel errors	118
Identifying faulty disk drive modules	119
Updating disk drive firmware	119
Replacing a disk drive module	121
Air management modules	121
Before you begin	121
Verifying component failure	122
Removing a disk drive module	122
Installing a disk drive module	123
Determine if a disk is missing	124
Installing an air management module	124
Verifying component operation	125
Disk error conditions	125
Identifying vdisk faults	126
Replacing a PSU	128
Before you begin	128

Verifying component failure	129
PSUs	129
Removing a PSU	131
Installing a PSU	132
Connecting a power cable	133
Powering on enclosures	134
Verifying component operation	134
Removing enclosure bezel	134
Replacing ear bezels	135
Before you begin	135
Removing the ear bezels	136
Installing the ear bezels	137
Verifying component operation	137
Replacing an FC transceiver	137
Before you begin	137
Verifying component failure	138
Removing an SFP module	138
Installing an SFP module	138
Verifying component operation	139
Replacing a controller enclosure chassis	139
Before you begin	139
Verifying component failure	140
Preparing to remove a damaged storage enclosure chassis	140
Removing a damaged storage enclosure chassis from the rack	141
Installing the replacement storage enclosure chassis in the rack	141
Completing the process	142
Verifying component operation	142
7 Voltage and temperature warnings	145
Resolving voltage and temperature warnings	145
Sensors	145
PSU sensors	145
Cooling fan sensors	145
Temperature sensors	146
PSU voltage sensors	147
A Event descriptions	149
Introduction	149
Events and event messages	149
Event format in this appendix	149
Resources for diagnosing and resolving problems	149
Event descriptions	150
Troubleshooting steps for leftover disk drives	194
Using the trust command	194
PSU faults and recommended actions	195
Events sent as indications to SMI-S clients	195
B System LEDs	197
24-disk enclosure front panel LEDs	197
12-disk enclosure front panel LEDs	198
Disk drive LEDs	199
Controller enclosure: Rear panel layout	201
4720/4730 controller module: Rear panel LEDs	202
4520/4530 controller module: Rear panel LEDs	203
PSU LEDs	204
C Available FRUs	207
Product overview	207
FRUs addressing 24-drive enclosures	208
Enclosure bezel for 24-drive models	210

FRUs addressing 12-drive enclosures	211
Enclosure bezel for 12-drive model	213
Glossary	215
Index	221

Figures

1	Disengaging a controller module	108
2	Disconnecting a controller module	108
3	Removing a controller module	108
4	Inserting a controller module	109
5	Disengaging a disk drive module or blank	122
6	Removing a disk drive module or blank	123
7	Installing a disk drive module or blank	123
8	AC PSU	130
9	DC and AC PSUs with power switch	130
10	Removing a PSU	131
11	Orienting a PSU	132
12	AC PSU power cable, switchless unit	133
13	DC PSU power cable featuring D-shell and lug connectors	133
14	Ear bezel assembly	135
15	Ear bezel assembly: Exploded view	136
16	Sample SFP connector	137
17	Disconnect fibre-optic interface cable from SFP	138
18	Flip SFP actuator upwards	138
19	Flip SFP actuator downwards	138
20	Connect fibre-optic interface cable to SFP	139
21	24-disk enclosure with bezel installed	197
22	24-disk enclosure with bezel removed	197
23	12-disk enclosure with bezel installed	198
24	12-disk enclosure with bezel removed	198
25	Disk drives	199
26	4520/4530 controller enclosure: Rear panel layout	201
27	4720/4730 controller module	202
28	4520/4530 controller module	203
29	PSUs	205
30	Controller enclosure exploded view (2U24)	209
31	Controller enclosure assembly (2U24)	209
32	Controller enclosure architecture — internal components sub-assembly (2U24)	210
33	Partial controller enclosure assembly showing alignment for 24-drive enclosure bezel	210
34	Controller enclosure assembly with 24-drive enclosure bezel installed	210
35	Controller enclosure exploded view (2U12)	212
36	Controller enclosure assembly (2U12)	212
37	Controller enclosure architecture — internal components sub-assembly (2U12)	212
38	Partial controller enclosure assembly showing bezel alignment (2U12)	213
39	Controller enclosure assembly with bezel installed (2U12)	213

Tables

1	Related Documentation	13
2	Document conventions	14
3	Problems using RAIDar to access a storage system	19
4	Solutions to performance degradation	31
5	Solutions to performance degradation	36
6	Errors associated with scheduling tasks in the CLI.	37
7	Diagnostic LED status: Front panel "Fault/Service Required"	95
8	Diagnostic LED status: Rear panel "FRU OK"	95
9	Diagnostic LED status: Rear panel "Fault/Service Required"	95
10	Diagnostic LED status: Disk drive module	95
11	Diagnostic LED status: Disk drive "Fault" LED (LFF and SFF modules).	96
12	Diagnostic LED status: Rear panel "Host Link Status"	96
13	Diagnostic LED status: Rear panel "Expansion Port Status"	97
14	Diagnostic LED status: Rear panel "Network Port Link Status"	97
15	Diagnostic LED status: Rear panel PSU "Input Power Source"	97
16	Diagnostic LED status: Rear panel PSU "Voltage/Fan Fault/Service Required"	98
17	Standard SCSI sense key descriptions	117
18	Common ASC and ASCQ descriptions.	117
19	Disk channel error codes	118
20	Disk error conditions and recommended actions	125
21	Vdisk faults	126
22	PSU faults and recommended actions	129
23	PSU LED descriptions	134
24	Removing and replacing a controller enclosure chassis and its FRUs.	140
25	PSU sensor descriptions	145
26	Cooling fan sensor descriptions.	146
27	Controller module temperature sensor descriptions	146
28	PSU temperature sensor descriptions	146
29	Voltage sensor descriptions.	147
30	Disk error conditions and recommended actions	151
31	PSU faults and recommended actions	195
32	Events and corresponding SMI-S indications	195
33	LEDs: 2U24 enclosure front panel	197
34	LEDs: 2U12 enclosure front panel	198
35	LEDs: Disk drive	199
36	LEDs: Disks in LFF and SFF enclosures.	200
37	LEDs: Vdisks in LFF and SFF enclosures	200
38	Individual product models comprising 4000 Series	207
39	4000 Series product components for 24-drive enclosures	208
40	4000 Series product components for 12-drive enclosures	211

About this guide

This guide describes how to maintain and troubleshoot AssuredSAN™ 4000 Series products.

Intended audience

This guide is intended for storage system administrators and service personnel.

Prerequisites

Prerequisites for using this product include knowledge of:

- Network administration
- Storage system configuration
- SAN management and DAS
- FC, SAS, and Ethernet protocols
- RAID technology

Before you begin to follow procedures in this guide, you must have already installed enclosures and learned of any late-breaking information related to system operation, as described in the *AssuredSAN 4000 Series Setup Guide* and Release Notes.

Related documentation

Table 1 Related Documentation

For information about	See
Enhancements, known issues, and late-breaking information not included in product documentation	AssuredSAN 4000 Series Release Notes
Overview of product shipkit contents and setup tasks	Getting Started*
Regulatory compliance and safety and disposal information	AssuredSAN Product Regulatory Compliance and Safety*
Using a rackmount bracket kit to install an enclosure into a rack	AssuredSAN Rackmount Bracket Kit Installation* <i>or</i> AssuredSAN 2-Post Rackmount Bracket Kit Installation*
Product hardware setup and related troubleshooting	AssuredSAN 4000 Series Setup Guide
Using the web interface to configure and manage the product	AssuredSAN 4000 Series RAIDar User Guide
Using the CLI to configure and manage the product	AssuredSAN 4000 Series CLI Reference 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 2 Document conventions

Convention	Element
Blue text	Cross-reference links and e-mail addresses
Blue, underlined text	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

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

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

 **NOTE:** Provides additional information.

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

1 Fault isolation methodology

AssuredSAN 4000 Series storage systems provide many ways to isolate faults. This section presents the basic methodology used to locate faults within a storage system, and to identify the pertinent FRUs affected.

Use RAIDar to configure and provision the system upon completing the hardware installation. As part of this process, configure and enable event notification so the system will notify you when a problem occurs that is at or above the configured severity (see the topic about configuring event notification in the *AssuredSAN 4000 Series RAIDar User Guide*). With event notification configured and enabled, you can follow the recommended actions in the notification message to resolve the problem, as further discussed in the options presented below.

Basic steps

The basic fault isolation steps are listed below:

- Gather fault information. See [Gather fault information](#) on page 16.
- Review the event log. See [Use the event log to identify faults](#) on page 16.
- Determine where in the system the fault is occurring. See [Use LEDs to determine where a fault is occurring](#) on page 16.
- If required, isolate the fault to a data path component or configuration. See [Isolate the fault](#) on page 17.

Options available for performing basic steps

When performing fault isolation and troubleshooting steps, select the option or options that best suit your site environment. Four options are described below. Use of any option is not mutually exclusive to the use of another option. You can use RAIDar to check the health icons/values for the system and its components to ensure that everything is okay, or to view a problem component. If you discover a problem, both RAIDar and the CLI provide recommended-action text online. Options for performing basic steps are listed according to frequency of use:

- [Use RAIDar](#)
- [Use the CLI](#)
- [Monitor event notification](#)
- [View the enclosure LEDs](#)

Use RAIDar

RAIDar uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. RAIDar enables you to monitor the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. Use health information displayed in RAIDar to find each component that has a problem, and follow actions in the component Health Recommendations field to resolve the problem.

Use the CLI

As an alternative to using RAIDar, you can run the `show system` command in the CLI to view the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown, and those components will be listed as Unhealthy Components. Follow the recommended actions in the component Health Recommendation field to resolve the problem.

Monitor event notification

With event notification configured and enabled, you can view the event log to monitor the health of the system and its components. If a message tells you to check whether an event has been logged, or to view information about an event in the log, you can do so using either RAIDar or the CLI. Using RAIDar, you view the event log and then click on the event message to see detail about that event. Using the CLI, you run the `show events detail` command (with additional parameters to filter the output) to see the detail

for an event. The events will be listed in reverse chronological order (most recent messages are at the top of the list). RAIDar will only display the last 100 events.

View the enclosure LEDs

You can view the LEDs on the hardware (while referring to [System LEDs](#) for your enclosure model) to identify component status. If a problem prevents access to either RAIDar or the CLI, this is the only option available. However, monitoring/management is often done at a management console using storage management interfaces rather than relying on line-of-sight to LEDs of racked hardware components.

Performing basic steps

You can use any of the available options described above in performing the basic steps comprising the fault isolation methodology.

Gather fault information

When a fault occurs, it is important to gather as much information as possible. Doing so will help you determine the correct action needed to remedy the fault.

Begin by reviewing the reported fault:

- Is the fault related to an internal data path or an external data path?
- Is the fault related to a virtual component such as a volume or vdisk?
- Is the fault related to a physical component such as a disk drive module, controller module, or PSU?

By isolating the fault to one of the components within the storage system, you will be able to determine the necessary corrective action more quickly.

Use the event log to identify faults

The event log records all system events. Each event has a numeric code that identifies the type of event that occurred, and has one of the following severities:

- **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 immediate action is required.

See [Event descriptions](#) for information about specific events.

It is very important to review the log, not only to identify the fault, but also to search for events that might have caused the fault to occur. For example, a host could lose connectivity to a vdisk if a user changes channel settings without taking the storage resources assigned to it into consideration. In addition, the type of fault can help you isolate the problem to either hardware or software.

Use LEDs to determine where a fault is occurring

Once you have an understanding of the reported fault, review the enclosure LEDs. The enclosure LEDs are designed to immediately alert users of any system faults, and might be what alerted the user to a fault in the first place.

When a fault occurs, the Fault ID status LED on an enclosure's right ear illuminates (see the diagram pertaining to your product's front panel components in [System LEDs](#)). Check the LEDs on the rear of the enclosure to narrow the fault to a FRU, connection, or both. The LEDs also help you identify the location of a FRU reporting a fault.

Use RAIDar to verify any faults found while viewing the LEDs. RAIDar is also useful in determining where the fault is occurring if the LEDs cannot be viewed due to the location of the system. RAIDar provides you with a visual representation of the system and where the fault is occurring. It can also provide more detailed information about FRUs, data, and faults.

Isolate the fault

Occasionally, it might become necessary to isolate a fault. This is particularly true with data paths, due to the number of components comprising the data path. For example, if a host-side data error occurs, it could be caused by any of the components in the data path: controller module, cable, or data host.

Stopping I/O

When troubleshooting disk and connectivity faults, ensure you have a current full backup. As an additional data protection precaution, stop all I/O to the affected vdisks.

 **IMPORTANT:** Stopping I/O to a vdisk is a host-side task, and falls outside the scope of this document.

When on-site, you can verify that there is no I/O activity by briefly monitoring the system LEDs; however, when accessing the storage system remotely, this is not possible. Remotely, you can use the `show vdisk-statistics` command to determine if I/O has stopped. Perform the steps below:

1. Using the CLI, run the `show vdisk-statistics` command.
The `Number of Reads` and `Number of Writes` outputs show the number of these operations that have occurred since the statistic was last requested. Record the numbers displayed.
2. Run the `show vdisk-statistics` command a second time.
This provides you a specific window of time (the interval between requesting the statistics) to determine if data is being written to or read from the disk. Record the numbers displayed.
3. To determine if any reads or writes occur during this interval, subtract the set of numbers you recorded in [step 1](#) from the numbers you recorded in [step 2](#).
 - If the resulting difference is zero, I/O has stopped.
 - If the resulting difference is not zero, a host is still reading from or writing to this vdisk. Continue to stop IOPS from hosts, and repeat [step 1](#) and [step 2](#) until the difference in [step 3](#) is zero.

 **NOTE:** See *AssuredSAN 4000 Series CLI Reference Guide* for additional information.

2 Troubleshooting using RAIDar

Problems using RAIDar to access a storage system

The following table lists problems you might encounter when using RAIDar to access a storage system. For information about configuring system interfaces and user accounts, see *AssuredSAN 4000 Series RAIDar User Guide* or online help.

Table 3 Problems using RAIDar to access a storage system

Problem	Solution
You cannot access RAIDar in a web browser.	<ul style="list-style-type: none">• Verify that you entered the correct IP address for the controller's network port, and do not include a leading zero in the address (for example, enter 10.1.4.33 not 10.1.4.033).• If the system has two controllers, enter the IP address of the partner controller's network port.• Ask the administrator whether the system is configured to allow RAIDar access via HTTP or HTTPS. Depending on the answer, enter either <code>http://ip-address/index.html</code> or <code>https://ip-address/index.html</code>.
You cannot sign in to RAIDar (unable to authenticate login).	<ul style="list-style-type: none">• Verify that you are entering the correct user name and password.• Ask the system administrator to verify that RAIDar access is enabled for the user account.
You cannot navigate beyond RAIDar's Sign In page (login successful).	<ul style="list-style-type: none">• Set the browser's local-intranet security option to medium or medium-low. For Internet Explorer 8, adding each controller's network IP address as a trusted site can avoid access issues.• Verify that the browser is set to allow cookies at least for the IP addresses of the storage-system network ports.
RAIDar pages do not display properly.	<ul style="list-style-type: none">• Use a color monitor and set its color quality to the highest setting.• Prevent RAIDar pages from being cached by disabling web page caching in your browser.• Check whether another user has changed the system configuration or user-account preferences.
Menu options are not available.	<ul style="list-style-type: none">• The options are not relevant to the system's current state. For example, if no volumes have been created, options to map and unmap volumes are not available.• The user account has a monitor (view only) role and therefore cannot access panels where system settings can be changed. Login with a different user account.
You cannot access online help.	<ul style="list-style-type: none">• Ensure pop-up windows are enabled.

Determining storage-system status

The storage system can have the following health values:

-  OK. The system is operating normally.
-  Degraded. At least one component is degraded.
-  Fault. At least one component has a fault.
-  Unknown. Health status is not available.

If the system or a physical subcomponent has a fault or is degraded, the Degraded or Fault icon is displayed to the left of that component in the Configuration View panel. If you see either of these icons, select the component and in its overview panel look for the Health Reason value. This value gives a short explanation of the health problem.

Viewing information about all vdisks

In the Configuration View panel, right-click Vdisks and select **View > Overview**. The Vdisks Overview table shows the following health fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  Unknown

A second table shows the following status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Status
 - CRIT: Critical. The vdisk is online but isn't fault tolerant because some of its disks are down.
 - FTDN: Fault tolerant with down disks. The vdisk is online and fault tolerant, but some of its disks are down.
 - FTOL: Fault tolerant and online.
 - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.
 - QTCR: Quarantined critical. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed. For instance, one disk is missing from a mirror or RAID-5.
 - QTDN: Quarantined with down disks. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed and would be fault tolerant. For instance, one disk is missing from a RAID-6.
 - QTOF: Quarantined offline. The vdisk is offline and quarantined because multiple disks are missing and user data is incomplete.
 - STOP: The vdisk is stopped.
 - UNKN: Unknown.
 - UP: Up. The vdisk is online and does not have fault-tolerant attributes.

Viewing information about a vdisk

In the Configuration View panel, right-click a vdisk and select **View > Overview**. The Vdisk Overview table shows the health of the selected vdisk and the disks in that vdisk.

Vdisk properties

When you select the vdisk component, the Properties for *Vdisk* table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  Unknown
- Health Reason. If a vdisk's health is not OK, this entry lists the reasons for the health state. If a vdisk's health is OK, no information is displayed.
- Health Recommendation. If a vdisk's health is not OK, this entry lists recommendations for correcting the health. If a vdisk's health is OK, no information is displayed.
- Status. Status values are described in [Status](#) on page 20.

- Current Job.
 - Disk Scrub: Disks in the vdisk are being scrubbed.
 - Expand: The vdisk is being expanded.
 - Initialize: The vdisk is being initialized.
 - Reconstruct: The vdisk is being reconstructed.
 - Verify: The vdisk is being verified.
 - Media Scrub: The vdisk is being scrubbed.

A second table displays information about unhealthy components. If all components are healthy, this table displays the text, "There is no data for your selection".

Disk properties

When you select the Disks component, a Disk Sets table and enclosure view appear. The enclosure view table has two tabs. The Tabular tab shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health. Shows whether the disk is healthy or has a problem.

 OK

 Degraded

 Fault

 N/A

 Unknown

If the disk's health is not OK, select it in the Configuration View panel to view details about it.

- State. Shows how the disk is used.
 - AVAIL: Available
 - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
 - SPARE: Spare assigned to a vdisk
 - GLOBAL SP: Global spare
 - LEFTOVR: Leftover

This also shows any job running on the disk.

- Current Job
 - DRSC: Disks in the vdisk are being scrubbed.
 - EXPD: The vdisk is being expanded.
 - INIT: The vdisk is being initialized.
 - RCON: The vdisk is being reconstructed.
 - VRFY: The vdisk is being verified.
 - VRSC: The vdisk is being scrubbed.
- Status. Up (operational) or Not Present.

The Graphical tab shows the locations of the vdisk's disks in system enclosures and each disk's health and state.

Viewing information about an enclosure

In the Configuration View panel, right-click an enclosure and select **View > Overview**. You can view information about the enclosure and its components in a front or rear graphical view, or in a front or rear tabular view.

- Front Graphical. Shows a graphical view of the front of each enclosure and its disks.
- Front Tabular. Shows a tabular view of each enclosure and its disks.
- Rear Graphical. Shows a graphical view of components at the rear of the enclosure.
- Rear Tabular. Shows a tabular view of components at the rear of the enclosure.

In any of these views, select a component to see more information about it. Components vary by enclosure model. If any components are unhealthy, a table at the bottom of the panel identifies them. When a disk is selected, you can view properties or historical performance statistics.

Enclosure properties

When you select an enclosure, a table shows the following health fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.

Disk properties

When you select a disk, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK. The disk is operating normally.
 -  Degraded
 -  Fault
 -  N/A
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
 - Up: The 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.
- How Used.

Two values are listed together: the first is How Used and the second is Current Job. For example, for a disk used in a vdisk (VDISK) that is being scrubbed (VRSC), VDISKVRSC displays.

 - How used:
 - AVAIL: Available.
 - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
 - GLOBAL SP: Global spare.
 - LEFTOVR: Leftover.
 - VDISK: Used in a vdisk.
 - VDISK SP: Spare assigned to a vdisk.

- Current Job.
 - DRSC: Disks in the vdisk are being scrubbed.
 - EXPD: The vdisk is being expanded.
 - INIT: The vdisk is being initialized.
 - RCON: The vdisk is being reconstructed.
 - VRFY: The vdisk is being verified.
 - VRSC: The vdisk is being scrubbed.
- Transfer Rate. The data transfer rate in Gbit/s.

 **NOTE:** Some 6-Gbit/s disks might not consistently support a 6-Gbit/s transfer rate. If this happens, the controller automatically adjusts transfers to those disks to 3 Gbit/s, increasing reliability and reducing error messages with little impact on system performance. This rate adjustment persists until the controller is restarted or power-cycled.

Power supply properties

When you select a PSU, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

When you select a PSU, a table shows:

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

Controller module properties

When you select a controller module, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Fault
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

Controller module: network port properties

When you select a network port, a table shows the following health fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK. The port is operating normally.
 -  Degraded. The port's operation is degraded.
- Health Reason. If Health is not OK, this field shows the reason for the health state.

Controller module: host port properties

When you select a host port, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  N/A
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Status.

Controller module: expansion port properties

When you select an expansion (Out) port, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  N/A
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

Controller module: CompactFlash properties

When you select a CompactFlash card, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

When you select a CompactFlash card in the Rear Tabular view, a table shows:

- Health.
 -  OK
 -  Fault
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

Drive enclosure: I/O module properties

When you select an IOM, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Status.

I/O modules: In port properties

When you select an In port, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  N/A
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

I/O modules: Out port properties

When you select an Out port, a table shows the following health and status fields; other fields that display are described in the *AssuredSAN 4000 Series RAIDar User Guide*.

- Health.
 -  OK
 -  Degraded
 -  Fault
 -  N/A
 -  Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.

Viewing the system event log

 **NOTE:** If you are having a problem with the system or a vdisk, review events as described below before calling technical support. Event information might enable you to resolve the problem.

In the Configuration View panel, right-click the system and select **View > Event Log**. The System Events panel shows the 100 most recent events that have been logged by either controller. All events are logged, regardless of event-notification settings. Click the buttons above the table to view all events, or only critical, warning, or informational events.

The event log table shows the following information:

- Severity.
 -  **Critical.** A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.
 -  **Error.** A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
 -  **Warning.** A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.
 -  **Informational.** A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.

- Time. Date and time when the event occurred, shown as *year-month-day hour.minutes.seconds*. Time stamps have one-second granularity.
- Event ID. An identifier for the event. The prefix A or B identifies the controller that logged the event.
- Code. An event code that helps you and support personnel diagnose problems. For event-code descriptions and recommended actions, see [Event descriptions](#).
- Message. Brief information about the event. Click the message to show or hide additional information and recommended actions.

When reviewing events, do the following:

1. For any critical, error, or warning events, click the message to view additional information and recommended actions. This information also appears in the [Event descriptions](#).
Identify the primary events and any that might be the cause of the primary event. For example, an over-temperature event could cause a disk failure.
2. View the event log and locate other critical/error/warning events in the sequence for the controller that reported the event.
Repeat this step for the other controller if necessary.
3. Review the events that occurred before and after the primary event.
During this review you are looking for any events that might indicate the cause of the critical/error/warning event. You are also looking for events that resulted from the critical/error/warning event, known as secondary events.
4. Review the events following the primary and secondary events.
You are looking for any actions that might have already been taken to resolve the problems reported by the events.

Clearing disk metadata

△ CAUTION:

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

Each disk in a vdisk has metadata that identifies the owning vdisk, the other members of the vdisk, and the last time data was written to the vdisk. The following situations cause a disk to become a *leftover*:

- Vdisk members' timestamps do not match so the system designates members having an older timestamp as leftovers.
- A disk is not detected during a rescan, then is subsequently detected.

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

- The disk's health becomes Degraded and its How Used state becomes LEFTOVR.
- The disk is automatically excluded from the vdisk, causing the vdisk's health to become Degraded or Fault, depending on the RAID level.
- The disk's Fault LED is illuminated amber.

If spares are available, and the health of the vdisk is Degraded, the vdisk will use them to start reconstruction. When reconstruction is complete, you can clear the leftover disk's metadata. Clearing the metadata will change the disk's health to OK and its How Used state to AVAIL, making the disk available for use in a new vdisk or as a spare.

If spares are not available to begin reconstruction, or reconstruction has not completed, keep the leftover disk so that you'll have an opportunity to recover its data.

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

To clear metadata from leftover disks

1. In the Configuration View panel, right-click the system and then select **Tools > Clear Disk Metadata**.
2. In the main panel, select leftover disks to clear metadata from. To select or clear all leftover disks, toggle the checkbox in the heading row.
3. Click **Clear Metadata**. When processing is complete a success dialog appears.
4. Click **OK**.

Isolating faulty disk drives

When a drive fault occurs, basic troubleshooting actions are:

- Identify the faulty drive
- Review the drive error statistics
- Review the event log
- Replace the faulty drive
- Reconstruct the associated vdisk

Identifying a faulty disk drive

The ID of a faulty disk drive involves confirming the drive fault and identifying the physical location of the drive.

To confirm a drive fault, use the basic troubleshooting steps in on page 19. You can also right-click on the System and select **View > Event Log**. Look for any notifications pertaining to a disk drive fault.

When you have confirmed a drive fault, record the drive's enclosure number and slot number.

To identify the physical location of a faulty drive:

1. Select Physical in the Configuration View.
2. Select the Enclosure indicated in the drive fault error.
3. Click the Front Graphical tab in the Enclosure Overview.

This displays a graphical view of the enclosure. The faulty disk drive is indicated with the appropriate health icon as described in [Viewing information about all vdisks](#) on page 20.

A disk having the status FAILED cannot be reused in the storage system and must be replaced.

For more information about viewing disk information, see the *AssuredSAN 4000 Series RAIDar User Guide*.

Reviewing the event logs

If all the steps in [Identifying a faulty disk drive](#) on page 27 have been performed, you have determined the following:

- A disk drive has encountered a fault
- The location of the disk drive
- What fault occurred

The next step is to review the event logs to determine if there were any events that led to the fault. If you skip this step, you could replace the faulty drive and then encounter another fault.

To view the event logs from any page, right-click the system and select **View > Event Log**. See [Viewing the system event log](#) on page 25 for more information about the Event Log.

Reconstructing a vdisk

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

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

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

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

RAID6 reconstruction behaves as follows:

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

When a disk fails, its Fault LED illuminates amber. When a spare is used as a reconstruction target, its Activity LED blinks green. For details about LED states, see [System LEDs](#).

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

Using recovery utilities

This section describes recovering data from a vdisk that is quarantined or offline (failed).

Quarantining vdisks

The system will automatically quarantine a vdisk having a fault-tolerant RAID level if one or more of its disks becomes inaccessible, or to prevent invalid ("stale") data that may exist in the controller from being written to the vdisk. Quarantine will not occur if a known-failed disk becomes inaccessible or if a disk becomes inaccessible after failover or recovery. The system will automatically quarantine an NRAID or RAID0 vdisk to prevent invalid data from being written to the vdisk. If quarantine occurs because of an

inaccessible disk, event 172 is logged. If quarantine occurs to prevent writing invalid data, event 485 is logged.

Examples of when quarantine can occur are:

- At system power-up, a vdisk has fewer disks online than at the previous power-up. This may happen because a disk is slow to spin up or because an enclosure is not powered up. The vdisk will be automatically dequarantined if the inaccessible disks come online and the vdisk status becomes FTOL (fault-tolerant and online), or if after 60 seconds the vdisk status is QTCR or QTDN.
- During system operation, a vdisk loses redundancy plus one more disk; for example, three disks are inaccessible in a RAID6 vdisk or two disks are inaccessible for other fault-tolerant RAID levels. The vdisk will be automatically dequarantined if after 60 seconds the vdisk status is FTOL, FTDN, or CRIT.

Quarantine isolates the vdisk from host access and prevents the system from changing the vdisk status to OFFL (offline). The number of inaccessible disks determines the quarantine status; from least to most severe:

- QTDN (quarantined with down disks): The vdisk is degraded or online with at least one inaccessible disk. The vdisk remains fault tolerant. For example, one disk is inaccessible in a RAID6 vdisk.
- QTCR (quarantined critical): The vdisk is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID6 vdisk or one disk is inaccessible for other fault-tolerant RAID levels.
- QTOF (quarantined offline): The vdisk is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID0 vdisk.

When a vdisk is quarantined, its disks become write-locked, its volumes become inaccessible, and it is not available to hosts until it is dequarantined. If there are interdependencies between the quarantined vdisk's volumes and volumes in other vdisks, quarantine may temporarily impact operation of those other volumes. Depending on the operation, the length of the outage, and the settings associated with the operation, the operation may automatically resume when the vdisk is dequarantined or may require manual intervention. A vdisk can remain quarantined indefinitely without risk of data loss.

 **NOTE:** The only tasks allowed for a quarantined vdisk are Dequarantine Vdisk and Delete Vdisk. If you delete a quarantined vdisk and its inaccessible disks later come online, the vdisk will reappear as quarantined or offline and you must delete it again (to clear those disks).

Removing a vdisk from quarantine

A vdisk is dequarantined when it is brought back online, which can occur in three ways:

- If the inaccessible disks come online, making the vdisk FTOL, the vdisk is automatically dequarantined.
- If after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined. The inaccessible disks are marked as failed and the vdisk status changes to CRIT (critical) or FTDN (fault tolerant with down disks). If the inaccessible disks later come online, they are marked as LEFTOVR (leftover).
- The dequarantine command is used to manually dequarantine the vdisk. If the inaccessible disks later come online, they are marked as LEFTOVR (leftover). If event 485 was logged, use the dequarantine command only as specified by the event's recommended-action text to avoid data corruption or loss.

A quarantined vdisk can be fully recovered if the inaccessible disks are restored. Make sure that all disks are properly seated, that no disks have been inadvertently removed, and that no cables have been unplugged. Sometimes not all disks in the vdisk power up. Check that all enclosures have restarted after a power failure. If these problems are found and then fixed, the vdisk recovers and no data is lost.

If the inaccessible disks cannot be restored (for example, they failed), and the vdisk's status is FTDN or CRIT, and compatible spares are available, reconstruction will automatically begin.

If a replacement disk (reconstruct target) is inaccessible at power up, the vdisk becomes quarantined; when the disk is found, the vdisk is dequarantined and reconstruction starts. If reconstruction was in process, it continues where it left off.

△ **CAUTION:** If a vdisk is removed from quarantine and does not have enough disks to continue operation, its status will change to OFFL and its data cannot be recovered. To continue operation, a RAID3 or RAID5 vdisk can have only one inaccessible disk; a RAID6 vdisk can have only one or two inaccessible disks; a RAID10 or RAID50 vdisk can have only one inaccessible disk per sub-vdisk. For example, a 16-disk RAID10 vdisk can remain online (critical) with 8 inaccessible disks if one disk per mirror is inaccessible.

To remove a vdisk from quarantine

1. In the Configuration View panel, right-click a quarantined vdisk and select **Tools > Dequarantine Vdisk**.
2. Click **Dequarantine Vdisk**. Depending on the number of disks that remain active in the vdisk, its health might change to Degraded (RAID6 only) and its status changes to FTOL, CRIT, or FTDN. For status descriptions, see [Vdisk properties](#) on page 20.

Correcting enclosure IDs

When installing a system with enclosures attached, the enclosure IDs might differ from the physical cabling order. This is because the controller might have been previously attached to some of the same enclosures and it attempts to preserve the previous enclosure IDs if possible. To correct this condition, you can perform a rescan.

To rescan disk channels

1. Verify that both controllers are operating normally.
2. In the Configuration View panel, right-click the system and select **Tools > Rescan Disk Channels**.
3. Click **Rescan**.

Problems after power-on or restart

After powering on the storage system or restarting the MC or SC, the processors take about 45 seconds to boot up, and the system takes an additional minute or more to become fully functional and able to process commands from RAIDar or the CLI. The time to become fully functional depends on many factors such as the number of enclosures, the number of disk drives, the number of vdisks, and the amount of I/O running at the time of the restart. During this time, some RAIDar or CLI commands might fail and some RAIDar pages may not be available. If this occurs, wait a few minutes and try again.

Problems with performance degradation

You can view performance statistics for both disks and vdisks. For more information, see the *AssuredSAN 4000 Series RAIDar User Guide*

- To view performance statistics for vdisks, select the Vdisk component and select the **Performance** tab. The Performance Statistics panel shows three graphs of historical performance statistics for the vdisk: Data Transferred (GB), Data Throughput (MB/s), and Average Response Time (ms). Data samples are taken every quarter hour and the graphs represent up to 50 samples.
- To view performance statistics for disks, select a disk and click the **Performance** tab.

A table shows eight graphs of historical performance statistics for the disk. Data samples are taken every quarter hour and the graphs represent up to 50 samples. By default, the graphs show the newest 50 samples.

Several factors can negatively impact vdisk and/or disk performance. [Table 4](#) lists the factors, their impact, and recommendations for improving performance.

Table 4 Solutions to performance degradation

Feature	Impact	Recommendations for minimizing impact
Managed logs	The managed logs function collects information at least once every 12 hours. While collecting information, the system might experience increased I/O response time and/or I/O time-outs.	Disable managed logs through RAIDar.
Active RAIDar, CLI, SMI-S, and SNMP sessions	Active RAIDar, CLI, SMI-S, and SNMP sessions collect information up to 4 times per hour. While collecting information, the system might experience increased I/O response time and/or I/O time-outs.  NOTE: Use of SMI-S and SNMP traps does not affect performance.	Use RAIDar, the CLI, SMI-S, and SNMP during non-peak hours.
Background and manual scrubs	<ul style="list-style-type: none"> • A background scrub affects performance up to 5%. • A manual scrub affects performance 25 - 60%. 	<ul style="list-style-type: none"> • Disable background scrubs through RAIDar. <p> CAUTION: If you disable background scrubs, run a manual scrub at least once per month.</p> <ul style="list-style-type: none"> • Run a manual scrub during non-peak hours. • Set the Utility priority for manual scrubs to low through RAIDar.
Reconstruction and copyback	<ul style="list-style-type: none"> • Reconstruction affects performance 5 - 50%. • Copyback affects performance up to 15%. 	<ul style="list-style-type: none"> • Set the Utility priority for reconstruction to low through RAIDar. • Replace failed disks during non-peak hours <p> CAUTION: It is recommended that failed disks are replaced immediately.</p>

3 Troubleshooting using the CLI

Isolating data path faults

When isolating data path faults, you must first isolate the fault to an internal data path or an external data path. This will help to target your troubleshooting efforts.

Internal data paths include the following:

- Controller to disk connectivity
- Controller to controller connectivity
- Controller ingress (incoming signals from drive enclosures)
- Controller egress (outgoing signals to drive enclosures)

External data paths consist of the connections between the storage system and data hosts.

Changing fault isolation settings

The EC in each IOM performs fault-isolation analysis of SAS expander PHY statistics. When one or more error counters for a specific PHY exceed the built-in thresholds, the PHY is disabled to maintain storage system operation.

Use the following information to help isolate PHY errors.

Resetting expander error counters

You can clear the counters and status for SAS expander lanes. Use the [clear expander-status](#) command on page 40 to reset error counters.

△ **CAUTION:** For use by or with direction from a service technician.

Disabling or enabling a PHY

If a PHY continues to accumulate errors you can disable it. Use the [set expander-phy](#) command on page 53 to disable or enable a specific PHY.

△ **CAUTION:** For use by or with direction from a service technician.

Disabling or enabling PHY isolation

You can change an expander's PHY Isolation setting to enable or disable fault monitoring and isolation for all PHYs in that expander. While troubleshooting a storage system problem, use the [set expander-fault-isolation](#) command on page 52 to temporarily disable fault isolation for a specific EC in a specific enclosure.

△ **CAUTION:** For use by or with direction from a service technician.

Isolating internal data path faults

Fault isolation firmware monitors hardware PHYs for problems.

PHYs are tested and verified before shipment as part of the manufacturing and qualification process.

Subsequent problems in a PHY cause symptoms such as:

- A host or controller continually rescans drives.
This can disrupt I/O or cause I/O errors. I/O errors can result in a failed drive, causing a vdisk to become critical or causing complete loss of a vdisk if more than one fails.
- Bad cables connecting enclosures, damaged controller connectors, and other physical damage.
This can cause continual errors, which the fault isolation firmware can often trace to a single problematic PHY. The fault isolation firmware recognizes the large number and rapid rate of these errors and disables this PHY without user intervention. This disabling, sometimes referred to as PHY fencing, eliminates the I/O errors and enables the system to continue operation without suffering performance degradation. To avoid these problems, problem PHYs are identified and disabled, if necessary, and status information is transmitted to the controller so that each action can be reported in the event log. Problem PHY ID and status information is reported in RAIDar, but disabled PHYs are only reported through event messages.
- PHY errors when powering on an enclosure, when removing or inserting a controller, and when connecting or disconnecting an enclosure.
An incompletely connected or disturbed cable might also generate a PHY error. These errors are usually not significant enough to disable a PHY, so the fault isolation firmware analyzes the number of errors and the error rate. If errors for a particular PHY increase at a slow rate, the PHY is usually not disabled. Instead the errors are accumulated and reported.

The firmware recognizes large number and rapid rate of these errors and disables the indicated PHY without user intervention. This disabling eliminates the I/O errors and enables the system to continue operation.

If a PHY becomes disabled, the event log entry helps to determine which enclosure or enclosures and which controller (or controllers) are affected. [Troubleshooting using event logs](#) on page 87 for more information about view and interpreting logs.

To enable a disabled PHY, reset the affected controller or power cycle the enclosure. Before doing so, it may be necessary to replace a defective cable or FRU. See [Troubleshooting and replacing FRUs](#) on page 103 for more information about replacing defective FRUs.

Checking PHY status

PHY status can be checked from the CLI. See [show expander-status](#) on page 66 for more information about how to check the PHY lanes.

△ **CAUTION:** For use by or with direction from a service technician.

Resolving PHY faults

1. Ensure that the cables are securely connected. If they are not, tighten the connectors.
2. Reset the affected controller or power-cycle the enclosure.
3. If the problem persists, replace the affected FRU or enclosure.
4. Periodically run the [show expander-status](#) to see if the fault isolation firmware disables the same PHY again. If it does:
 - a. Replace the appropriate cable.
 - b. Reset the affected controller or power-cycle the enclosure.

Isolating external data path faults

To troubleshoot external data path faults, perform the following steps:

1. Use the [show host-parameters](#) command as described on page 71 to display information about host port status.
2. To target the cause of the link failure, review the detail as output.

The details include:

- Port information. Selected controller and port number
- Media. Host link type
- Target ID.
- Status. Condition of the link, Up or Disconnected.

In Fibre Channel storage systems

- Topology. Port connection type
- Speed. Both actual and configured link speed, 2 Gbit/s, 4 Gbit/s, 8 Gbit/s, or Auto
- Primary ID.

Resolving external data path faults

Review the output for host ports with a status of Disconnected. This can be caused by one or more of the following conditions:

- A faulty HBA in the host
- A faulty cable
- A disconnected cable
- A faulty port in the host interface module

Resetting a host channel on an FC storage system

For an FC system using loop topology, you might need to reset a host port (channel) to fix a host connection or configuration problem.

Use the [reset host-link](#) command on page 44 to reset a host port.

Problems with performance degradation

You can view performance statistics for controllers, disks, host ports, vdisks, and volumes in the CLI. For more information, see the *AssuredSAN 4000 Series CLI Reference Guide*

- To view performance statistics for a controller, run the [show controller-statistics](#) command.
- To view performance statistics for a disk, run the [show disk-statistics](#) command.
- To view performance statistics for a host port, run the [show host-port-statistics](#) command.
- To view performance statistics for a vdisk, run the [show vdisk-statistics](#) command.
- To view performance statistics for a volume, run the [show volume-statistics](#) command.

Several factors can negatively impact performance. [Table 5](#) lists the factors, their impact, and recommendations for improving performance.

Table 5 Solutions to performance degradation

Feature	Impact	Recommendations for minimizing impact
Managed logs	The managed logs function collects information at least once every 12 hours. While collecting information, the system might experience increased I/O response time and/or I/O time-outs.	Disable managed logs through the CLI by running the set advanced-settings command.
Active RAIDar, CLI, SMI-S, and SNMP sessions	Active RAIDar, CLI, SMI-S, and SNMP sessions collect information up to 4 times per hour. While collecting information, the system might experience increased I/O response time and/or I/O time-outs.  NOTE: Use of SMI-S and SNMP traps does not affect performance.	Use RAIDar, the CLI, SMI-S, and SNMP during non-peak hours.
Background and manual scrubs	<ul style="list-style-type: none"> • A background scrub affects performance up to 5%. • A manual scrub affects performance 25 - 60%. 	<ul style="list-style-type: none"> • Disable background scrubs through the CLI by running the set advanced-settings command. <p> CAUTION: If you disable background scrubs, run a manual scrub at least once per month.</p> <ul style="list-style-type: none"> • Run a manual scrub during non-peak hours by running the scrub vdisk command. • Set the Utility priority for manual scrubs to low through the CLI by running the set advanced-settings command.
Reconstruction and copyback	<ul style="list-style-type: none"> • Reconstruction affects performance 5 - 50%. • Copyback affects performance up to 15%. 	<ul style="list-style-type: none"> • Set the Utility priority for reconstruction to low through the CLI by running the set advanced-settings command. • Replace failed disks during non-peak hours <p> CAUTION: It is recommended that failed disks are replaced immediately.</p>

Problems scheduling tasks

There are two parts to scheduling tasks: you must first create the task and then create the schedule to run the task.

- To create a task, run the [create task](#) command.
- To create a schedule, run the [create schedule](#) command.

If your task does not run at the times you specified, check the schedule specifications. It is possible to create conflicting specifications.

Errors associated with scheduling tasks

The following table describes error messages associated with scheduling tasks.

Table 6 Errors associated with scheduling tasks in the CLI

Error Message	Solution
Task Already Exists	Select a different name for the task.
Unknown Task Type	The task type is misspelled. Verify the task type is spelled correctly.
Schedule Already Exists	Select a different name for the schedule.
Expected one of START, EVERY, BETWEEN, ONLY, COUNT, EXPIRES	There might be a comma at the end of the expression. Ensure there is no comma at the end of the expression.
Invalid syntax for Nth suffix	The suffix must match the number. 1st, 2nd, 3rd, etc.
Specified start time must be at least a minute later than the current system time	Change the start time.
Memory Allocation Error	Contact the system's administrator for assistance.

Deleting schedules and tasks

Deleting a task will delete any schedules using that task. Deleting a schedule does not affect tasks.

- To delete a task, run the [delete task](#) command.
- To delete a schedule, run the [delete schedule](#) command.

Command reference

This section provides information about CLI commands commonly used for debugging and includes syntax, parameters, and usage examples. This list is not inclusive of all CLI commands. Additional information about commands and command syntax can be found in the *AssuredSAN 4000 Series CLI Reference Guide*.

Command references that include a See Also section include two types of references. Commands in blue with a page number are commands referenced in this guide. All other references, in black, can be found in the *AssuredSAN 4000 Series CLI Reference Guide*.

See [Related documentation](#) on page 13 for information about additional reference material.

Viewing help

To view brief descriptions of all commands that are available to the user level you logged in as, enter:

```
help
```

To view help for a command and then return to the command prompt, enter:

```
help command-name
```

To view information about command syntax, enter:

```
help syntax
```

To view information about command completion, editing, and history, enter:

```
help help
```

Missing parameter data error

If you try to use a command that has a name parameter and the CLI displays "Error: The command is missing parameter data" then the name value you specified might have been interpreted as the keyword of an optional parameter.

For example, this problem would occur if you tried to create a vdisk named A or a without specifying the `assigned-to` parameter.

To use a name that the CLI could interpret as an optional parameter, you must specify that parameter before the name parameter.

abort scrub

Description Aborts the `scrub vdisk` operation for specified vdisks.

Syntax `abort scrub vdisk vdisks`

Parameters `vdisk vdisks`
Names or serial numbers of the vdisks to stop scrubbing. For `vdisk` syntax, see *Command Syntax* in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

Example Abort scrubbing vdisk `vd1`:

```
# abort scrub vdisk vd1
Info: Scrub was aborted on vdisk vd1. (vd1)
Success: Command completed successfully. (2012-01-20 15:42:08)
```

See also

- [scrub vdisk](#) on page 46
- `show vdisks`

clear cache

Description Clears unwritable cache data from both controllers. This data cannot be written to disk because it 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.

You can clear unwritable cache data for one or more volumes.

When there are several volumes' worth of unwritable data, running the `clear cache` command will clear only the first volume's unwritable data. Therefore, it might become necessary to run the `clear cache` command multiple times to remove all cache data. Use the following process to ensure all cache data has been cleared.

1. Run the `show unwritable-cache` command to view the percent of unwritable cache in each controller.
2. Run the `clear cache` command.
3. Run the `show unwritable-cache` command to view the percent of unwritable cache in each controller. If the value is not 0, repeat steps 1 - 3 until the value is 0.

Syntax `clear cache [volume volume]`

Parameters `volume volume`
Optional. Name or serial number of the volume whose cache data should be cleared. For `volume` syntax, see *Command Syntax* in the *AssuredSAN 4000 Series CLI Reference Guide*. If this parameter is omitted, the command clears any unneeded orphaned data for volumes that are no longer online or that no longer exist.

Example Clear unwritable cache data for volume `V1` from both controllers:

```
# clear cache volume V1
Success: Command completed successfully - If unwritable cache data
existed, it has been cleared. (2012-01-18 14:21:11)
```

See also `show unwritable-cache`

clear disk-metadata

Description Clears metadata from leftover disks.

△ CAUTION:

- Only use this command when all vdisks are online and leftover disks exist. Improper use of this command may result in data loss.
 - Do not use this command when a vdisk is offline and one or more leftover disks exist.
-

If you are uncertain whether to use this command, contact technical support for further assistance.

Each disk in a vdisk has metadata that identifies the owning vdisk, the other members of the vdisk, and the last time data was written to the vdisk. The following situations cause a disk to become a leftover:

- Vdisk members' timestamps do not match so the system designates members having an older timestamp as leftovers.
- A disk is not detected during a rescan, then is subsequently detected.

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

- The disk's health becomes `Degraded` and its How Used state becomes `LEFTOVR`.
- The disk is automatically excluded from the vdisk, causing the vdisk's health to become `Degraded` or `Fault`, depending on the RAID level.
- The disk's Fault LED is illuminated amber.

If spares are available, and the health of the vdisk is `Degraded`, the vdisk will use them to start reconstruction. When reconstruction is complete, you can clear the leftover disk's metadata. Clearing the metadata will change the disk's health to `OK` and its How Used state to `AVAIL`, making the disk available for use in a new vdisk or as a spare.

If spares are not available to begin reconstruction, or reconstruction has not completed, keep the leftover disk so that you'll have an opportunity to recover its data.

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

Syntax `clear disk-metadata disks`

Parameters `disks`
IDs of the leftover disks to clear metadata from. For disk syntax, see *Command Syntax in the AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

Example Show disk usage:

```
# show disks
Location ... How Used ...
-----
1.1      ... LEFTOVR  ...
1.2      ... VDISK    ...
...
```

Clear metadata from a leftover disk:

```
# clear disk-metadata 1.1
Info: Updating disk list...
Info: Disk disk_1.1 metadata was cleared. (2012-01-18 10:35:39)

Success: Command completed successfully. - Metadata was cleared.
(2012-01-18 10:35:39)
```

Try to clear metadata from a disk that is not leftover:

```
# clear disk-metadata 1.2
Error: The specified disk is not a leftover disk. (1.2) - Metadata was
not cleared for one or more disks. (2012-01-18 10:32:59)
```

clear events

△ **CAUTION:** For use by or with direction from a service technician.

Description Clears the event log for controller A, B, or both.

Syntax `clear events [a|b|both]`

Parameters `a|b|both`
Optional. The controller event log to clear. If this parameter is omitted, both event logs are cleared.

Example Clear the event log for controller A:

```
# clear events a
Success: Command completed successfully. - The event log was
successfully cleared. (2012-01-18 10:40:13)
```

See also • [show events](#) on page 63

clear expander-status

△ **CAUTION:** For use by or with direction from a service technician.

Description Clears the counters and status for SAS expander lanes. Counters and status can be reset to a good state for all enclosures, or for a specific enclosure whose status is `Error` as shown by the [show expander-status](#) command.

 **NOTE:** If a rescan is in progress, the clear operation will fail with an error message saying that an EMP does exist. Wait for the rescan to complete and then retry the clear operation.

Syntax `clear expander-status [enclosure ID]`

Parameters `enclosure ID`
Optional. The enclosure number.

Example Clear the expander status for the first enclosure:

```
# clear expander-status enclosure 0
Success: Command completed successfully. - Expander status was cleared.
(2012-01-18 14:18:53)
```

See also • [show expander-status](#) on page 66

create schedule

Description Schedules a task to run automatically.

Syntax `create schedule
schedule-specification "specification"
task-name task-name
schedule-name`

Parameters `schedule-specification "specification"`
Defines when the task will first run, and optionally when it will recur and expire. You can use a comma to separate optional conditions. Dates cannot be in the past. For times, if neither AM nor PM is specified, a 24-hour clock is used.

- `start yyyy-mm-dd hh:mm [AM|PM]`
Specifies a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
- `[every # minutes|hours|days|weeks|months|years]`
Specifies the interval at which the task will run.
- `[between hh:mm [AM|PM] and hh:mm [AM|PM]]`
Constrains the time range during which the task is permitted to run. Ensure that the start time is within the specified time range.
- `[only any|first|second|third|fourth|fifth|last|#st|#nd|#rd|#th weekday|weekendday|Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday of year|month|January|February|March|April|May|June|July|August|September|October|November|December]`
Constrains the days or months when the task is permitted to run. Ensure that this constraint includes the start date.
- `[count #]`
Constrains the number of times the task is permitted to run.
- `[expires yyyy-mm-dd hh:mm [AM|PM]]`
Specifies when the schedule expires, after which the task will no longer run.

`task-name task-name`

The task to run. The name is case sensitive.

`schedule-name`

A name for the new schedule. The name is case sensitive; cannot include a comma, double quote, angle bracket, or backslash; and can have a maximum of 32 bytes. A name that includes a space must be enclosed in double quotes.

Example Create schedule Sched1 that runs Task1 for the first time on March 1, 2012; runs daily between midnight and 1:00 AM; and runs for the last time in the morning of January 1, 2013:

```
# create schedule schedule-specification "start 2012-03-01 00:01, every  
1 days, between 12:00 AM and 1:00 AM, expires 2013-01-01 1:00 AM"  
task-name Task1 Sched1  
Success: Command completed successfully. (Sched1) - The schedule was  
created. (2012-01-20 15:48:01)
```

Create schedule Sched2 that runs Task2 for the first time on March 1, 2012, and on the first weekday of each month, with no expiration:

```
# create schedule schedule-specification "start 2012-03-01 00:01 only  
first weekday of month" task-name Task2 Sched2  
Success: Command completed successfully. (Sched2) - The schedule was  
created. (2012-01-20 15:46:16)
```

Try to create Sched3 with a start time outside the “between” range:

```
# create schedule schedule-specification "start 2012-01-14 4:15 PM
between 12:00 AM and 12:00 PM" task-name Task3 Sched3
Error: create schedule: (Sched3) - The specified start time must be
within the range specified with the 'between' parameter. (2012-01-20
15:46:08)
```

- See also**
- [delete schedule](#)
 - [set schedule](#)
 - [show schedule-details](#)
 - [show schedules](#)
 - [show task-details](#)
 - [show tasks](#)

create task

Description Creates a task that can be scheduled. You can create a task to enable or disable DSD.

Syntax To create a task to enable spin down for all disks:

```
create task type EnableDSD taskDSDresume
```

To create a task to disable spin down for all disks:

```
create task type DisableDSD taskDSDsuspend
```

Parameters type EnableDSD|DisableDSD

The task type:

- **EnableDSD:** Enables spin down for all vdisks. You can use this to enable or resume spin down during hours of infrequent activity.
- **DisableDSD:** Disables spin down for all vdisks. You can use this to disable or suspend spin down during hours of frequent activity.

name

A name for the new task. The name is case sensitive; cannot include a comma, double quote, angle bracket, or backslash; and can have a maximum of 32 bytes. A name that includes a space must be enclosed in double quotes.

Example Create a task named `taskDSDresume` to enable or resume spin down:

```
# create task type EnableDSD taskDSDresume
Success: Command completed successfully. (taskDSDresume) - The task was
created. (2012-01-19 15:47:04)
```

Create a task named `taskDSDsuspend` to disable or suspend spin down:

```
# create task type DisableDSD taskDSDsuspend
Success: Command completed successfully. (taskDSDsuspend) - The task
was created. (2012-01-19 15:47:15)
```

- See also**
- [create schedule](#)
 - [show task-details](#)
 - [show tasks](#)
 - [show volumes](#)

delete schedule

Description Deletes a task schedule.

Syntax `delete schedule schedule`

Parameters *schedule*
The schedule to delete.

Example Delete schedule Sched1:

```
# delete schedule Sched1
Success: Command completed successfully. (Sched1) - The schedule was
deleted. (2012-01-21 17:05:15)
```

See also

- [create schedule](#)
- [show schedule-details](#)
- [show schedules](#)

delete task

Description Deletes a task. If the task is scheduled, a confirmation prompt will ask whether you want to delete the task and its schedules. Reply yes to delete both, or no to cancel the command.

Syntax `delete task task`

Parameters *task*
The task to delete.

Example Delete task Task1:

```
# delete task Task1
Success: Command completed successfully. (Task1) - The task was deleted.
(2012-01-21 17:05:46)
```

See also

- [create task](#)
- [delete schedule](#)
- [show schedule-details](#)
- [show schedules](#)
- [show task-details](#)
- [show tasks](#)

rescan

Description This command forces rediscovery of attached disks and enclosures. If both SCs are online and able to communicate with both expansion modules in each connected enclosure, this command also reassigns enclosure IDs based on controller A's enclosure cabling order. A manual rescan may be needed after system power-up to display enclosures in the proper order.

A manual rescan is not required to detect when disks are inserted or removed; the controllers do this automatically. When disks are inserted they are detected after a short delay, which allows the disks to spin up.

When you perform a manual rescan, it temporarily pauses all I/O processes, then resumes normal operation.

Syntax `rescan`

Example Scan for device changes and re-evaluate enclosure IDs:

```
# rescan
Success: Command completed successfully. (2012-01-21 12:20:57)
```

reset host-link

Description Resets specified controller host ports (channels).

For an FC host port configured to use FC-AL topology, a LIP is issued.

For SAS, resetting a host port issues a COMINIT/COMRESET sequence and might reset other ports.

Syntax `reset host-link
ports ports
[controller a|b]`

Parameters port *ports*

A controller host port ID, a comma-separated list of IDs, a hyphenated range of IDs, or a combination of these. A port ID is a controller ID and port number, and is not case sensitive. Do not mix controller IDs in a range.

controller a|b

Optional. The controller ID, either A or B.

Example Reset the host link on port A1:

```
# reset host-link ports A1
```

```
Success: Command completed successfully. - Reset Host Link(s) on port(s)  
A1 from current controller. (2012-01-21 11:36:28)
```

See also • show ports

restart

Description Restarts the SC or MC in a controller module.

If you restart an SC, 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 MC is not restarted so it can provide status information to external interfaces.

If you restart an MC, communication with it is lost until it successfully restarts. If the restart fails, the partner MC remains active with full ownership of operations and configuration information.

△ **CAUTION:** If you restart both controller modules, users lose access to the system and its data until the restart is complete.

 **NOTE:** When an SC is restarted, live performance statistics that it recorded will be reset; historical performance statistics are not affected. Disk statistics may be reduced but will not be reset to zero, because disk statistics are summed between the two controllers. For more information, see help for commands that show statistics.

Syntax `restart
sc|mc
[a|b|both]
[noprompt]`

Parameters `sc|mc`

The controller to restart:

- `sc`: SC
- `mc`: MC

`a|b|both`

Optional. The controller module containing the controller to restart. If this parameter is omitted, the command affects the controller being accessed.

`noprompt`

Optional in console format; required for XML API format. Suppresses the confirmation prompt, which requires a yes or no response. Specifying this parameter allows the command to proceed without user interaction.

Example Restart the MC in controller A, which you are logged in to:

```
# restart mc a
```

During the restart process you will briefly lose communication with the specified Management Controller(s).

Continue? **yes**

Info: Restarting the local MC (A)...

Success: Command completed successfully. (2012-01-21 11:38:47)

From controller A, restart the SC in controller B:

```
# restart sc b
```

Success: Command completed successfully. - SC B was restarted.
(2012-01-21 11:42:10)

Restart both SCs:

```
# restart sc both
```

Restarting both controllers can cause a temporary loss of data availability.

Do you want to continue? **yes**

Success: Command completed successfully. - Both SCs were restarted.
(2012-01-21 13:09:52)

See also • `shutdown`

restore defaults

△ **CAUTION:** For use by or with direction from a service technician.

Description Restores the default configuration to the controllers. For details about which settings are restored see the *AssuredSAN 4000 Series CLI Reference Guide*.

△ **CAUTION:** This command changes how the system operates and might require some reconfiguration to restore host access to volumes.

Syntax `restore defaults`
`[noprompt]`
`[prompt yes|no]`

Parameters `noprompt`

Optional in console format; required for XML API format. Suppresses the confirmation prompt, which requires a yes or no response. Specifying this parameter allows the command to proceed without user interaction.

prompt yes|no

Optional. Specifies an automatic response to the confirmation prompt:

- `yes`: Allow the command to proceed.
- `no`: Cancel the command.

If this parameter is omitted, you must manually reply to the prompt.

Example Restore the controllers' default configuration:

```
# restore defaults
WARNING: The configuration of the array controller will be re-set to
default settings. The Management Controller will restart once this is
completed. Are you sure? yes
Success: Command completed successfully. - Device default configuration
was restored.
```

See also • [restart](#) on page 44

scrub vdisk

Description Analyzes specified vdisks to find and fix disk errors. This command acts on disks that are associated with a vdisk and are neither dedicated spares nor leftovers. This command will fix parity mismatches for RAID 3, 5, 6, and 50; mirror mismatches for RAID 1 and 10; and media errors for all RAID levels.

Vdisk scrub can last over an hour, depending on vdisk size, utility priority, and amount of I/O activity. However, a "foreground" scrub performed with this command is typically faster than a background scrub enabled with the `set job-parameters` command. You can use a vdisk while it is being scrubbed. To check the progress of a vdisk scrub (VRSC) job, use the `show vdisks` command.

When a scrub is complete, event 207 is logged and specifies whether errors were found and whether user action is required.

Syntax `scrub vdisk vdisks`

Parameters *vdisks*

Names or serial numbers of the vdisks to scrub. For vdisk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

Example Start scrubbing vdisk vd1:

```
# scrub vdisk vd1
Info: Scrub was started on vdisk vd1. (vd1)
Success: Command completed successfully. (2012-01-20 15:41:38)
```

See also • [abort scrub](#) on page 38
• [set advanced-settings](#) on page 47
• `set job-parameters`
• `show vdisks`

set advanced-settings

Description Sets advanced system configuration options.

Syntax `set advanced-settings`
[auto-write-back enabled|disabled|on|off]
[background-disk-scrub enabled|disabled|on|off]
[background-scrub enabled|disabled|on|off]
[background-scrub-interval *interval*]
[compact-flash-failure enabled|disabled|on|off]
[controller-failure enabled|disabled|on|off]
[dynamic-spares enabled|disabled|on|off]
[emp-poll-rate *rate*]
[fan-failure enabled|disabled|on|off]
[host-cache-control enabled|disabled|on|off]
[independent-cache enabled|disabled|on|off]
[managed-logs enabled|disabled|on|off]
[missing-lun-response notready|illegal]
[partner-firmware-upgrade enabled|disabled|on|off]
[partner-notify enabled|disabled|on|off]
[power-supply-failure enabled|disabled|on|off]
[smart enabled|disabled|on|off|detect-only]
[super-cap-failure enabled|disabled|on|off]
[sync-cache-mode immediate|flush]
[temperature-exceeded enabled|disabled|on|off]
[utility-priority low|medium|high]
[spin-down enabled|disabled|on|off]
[spin-down-delay *delay*]

Parameters `auto-write-back enabled|disabled|on|off`
Optional. Sets whether the cache mode will change from write-through to write-back when the trigger condition is cleared.

- disabled or off: Auto-write-back is disabled.
- enabled or on: Auto-write-back is enabled.

`background-disk-scrub enabled|disabled|on|off`
Optional. Sets whether disks that are not in vdisks are automatically checked for disk defects to ensure system health. The interval between background disk scrub finishing and starting again is 24 hours.

- disabled or off: Background disk scrub is disabled.
- enabled or on: Background disk scrub is enabled.

`background-scrub enabled|disabled|on|off`
Optional. Sets whether disks in vdisks are automatically checked for disk defects to ensure system health. The interval between background vdisk scrub finishing and starting again is specified by the `background-scrub-interval` parameter.

- disabled or off: Background vdisk scrub is disabled.
- enabled or on: Background vdisk scrub is enabled.

`background-scrub-interval interval`
Optional. Sets the interval in hours between background vdisk scrub finishing and starting again, from 1–360 hours.

`compact-flash-failure` `enabled|disabled|on|off`

Optional. Sets whether the cache policy will change from write-back to write-through when CompactFlash memory is not detected during POST, fails during POST, or fails during controller operation.

- `disabled` or `off`: The CompactFlash failure trigger is disabled.
- `enabled` or `on`: The CompactFlash failure trigger is enabled.

`controller-failure` `enabled|disabled|on|off`

Optional. Sets whether the cache policy will change from write-back to write-through when a controller fails.

- `disabled` or `off`: The controller failure trigger is disabled.
- `enabled` or `on`: The controller failure trigger is enabled.

`dynamic-spare` `enabled|disabled|on|off`

Optional. Sets whether the storage system will automatically designate an available compatible disk as a spare to replace a failed disk in a vdisk. A compatible disk has enough capacity to replace the failed disk and is the same type (SAS SSD, enterprise SAS, or midline SAS).

- `disabled` or `off`: The dynamic spares feature is disabled.
- `enabled` or `on`: The dynamic spares feature is enabled.

`emp-poll-rate` *rate*

Optional. Sets the interval at which the storage system will poll each enclosure's EMP for status changes, from 5–3600 seconds.

`fan-failure` `enabled|disabled|on|off`

Optional. Sets whether the cache policy will change from write-back to write-through when a fan fails.

- `disabled` or `off`: The fan failure trigger is disabled.
- `enabled` or `on`: The fan failure trigger is enabled.

`host-cache-control` `enabled|disabled|on|off`

Optional. Sets whether hosts are allowed to use the `SCSI MODE SELECT` command to change the storage system's write-back cache setting.

- `disabled` or `off`: Host control of caching is disabled.
- `enabled` or `on`: Host control of caching is enabled.

`independent-cache` `enabled|disabled|on|off`

Optional. Sets the cache redundancy mode for a dual-controller storage system.

For the change to take effect, the user must restart both SCs.

- `disabled` or `off`: Controller failover is enabled and data in a controller's write-back cache is mirrored to the partner controller.
- `enabled` or `on`: The controllers use Independent Cache Performance Mode, in which controller failover is disabled and data in a controller's write-back cache is not mirrored to the partner controller. This improves write performance at the risk of losing unwritten data if a controller failure occurs while there is data in controller cache.

`managed-logs` `enabled|disabled|on|off`

Optional. Enables or disables the managed logs feature, which allows log files to be transferred from the storage system to a log collection system to avoid losing diagnostic data.

- `disabled` or `off`: The managed logs feature is disabled.
- `enabled` or `on`: The managed logs feature is enabled.

`missing-lun-response` `notready|illegal`

Optional. Sets whether host drivers may probe for LUNs until the host drivers reach the LUN to which they have access.

- `notready`: Sends a reply that there is a LUN where a gap has been created but that it is "not ready." Sense data returned is sensekey = 2, code = 4, qualifier = 3.
- `illegal`: Sends a reply that there is a LUN but that the request is "illegal." Sense data returned is sensekey = 5, code = 25h, qualifier = 0. If the system is used in a VMware environment, use this option.

`partner-firmware-upgrade` `enabled|disabled|on|off`

Optional. Sets whether component firmware versions are monitored and will be automatically updated on the partner controller.

- `disabled` or `off`: PFU is disabled.
- `enabled` or `on`: PFU is enabled.

`partner-notify` `enabled|disabled|on|off`

Optional. Sets whether to notify the partner controller that a trigger condition occurred. Enable this option to have the partner also change to write-through mode for better data protection. Disable this option to allow the partner continue using its current caching mode for better performance.

- `disabled` or `off`: Notification is disabled.
- `enabled` or `on`: Notification is enabled.

`power-supply-failure` `enabled|disabled|on|off`

Optional. Sets whether the cache policy automatically changes to write-through when a PSU fails.

- `disabled` or `off`: The power-supply failure trigger is disabled.
- `enabled` or `on`: The power-supply failure trigger is enabled.

`smart` `enabled|disabled|on|off|detect-only`

Optional. Enables or disables SMART monitoring for all disks in the storage system.

- `disabled` or `off`: Disables SMART for all disks in the system and for all disks added to the system.
- `enabled` or `on`: Enables SMART for all disks in the system and for all disks added to the system.
- `detect-only`: Detects but does not change the SMART setting of each disk in the system, and for each new disk added to the system.

`super-cap-failure` `enabled|disabled|on|off`

Optional. Sets whether the cache policy will change from write-back to write-through when the supercapacitor that provides backup power for cache is not fully charged or fails.

- `disabled` or `off`: The supercapacitor failure trigger is disabled.
- `enabled` or `on`: The supercapacitor failure trigger is enabled.

`sync-cache-mode` `immediate|flush`

Optional. Sets how the SCSI `SYNCHRONIZE CACHE` command is handled.

- `immediate`: Good status is returned immediately and cache content is unchanged.
- `flush`: Good status is returned only after all write-back data for the specified volume is flushed to disk.

`temperature-exceeded` `enabled|disabled|on|off`

Optional. Sets whether the system will shut down a controller when its temperature exceeds the critical operating range.

- `disabled` or `off`: The over-temperature trigger is disabled.
- `enabled` or `on`: The over-temperature trigger is enabled.

`utility-priority` `low|medium|high`

Optional. Sets the priority at which data-redundancy utilities, such as `vdisk verify` and `reconstruct`, run with respect to I/O operations competing for the system's processors. (This does not affect `vdisk background scrub`, which always runs at "background" priority.)

- `high`: Utilities have higher priority than host I/O. Use when your highest priority is to return the system to a fully fault-tolerant state. This can cause heavy I/O to be slower than normal.
- `medium`: Utility performance is balanced with host I/O performance.
- `low`: Utilities run at a slower rate with minimal effect on host I/O. Use when streaming data without interruption, such as for a web server, is more important than data redundancy.

`spin-down` `enabled|disabled|on|off`

Optional. Sets whether available disks and global spares will spin down after a period of inactivity shown by the `spin-down-delay` parameter.

- `disabled` or `off`: DSD for available disks and global spares is disabled.
- `enabled` or `on`: DSD for available disks and global spares is enabled.

`spin-down-delay` *delay*

Optional. Sets the period of inactivity after which available disks and global spares will spin down. Setting the delay to 1–360 minutes will enable spin down; setting the delay to 0 will disable spin down.

Example Enable PFU:

```
# set advanced-settings partner-firmware-upgrade enabled
Success: Command completed successfully. - The settings were changed
successfully. (2012-01-20 11:57:01)
```

Enable managed logs:

```
# set advanced-settings managed-logs enabled
Success: Command completed successfully. - The settings were changed
successfully. (2012-01-21 16:25:58)
```

- See also**
- [scrub vdisk](#) on page 46
 - `set job-parameters`
 - `set spares`
 - `show advanced-settings`

set debug-log-parameters

△ **CAUTION:** For use by or with direction from a service technician.

Description Sets the types of debug messages to include in the SC debug log.

Syntax `set debug-log-parameters message-type+|- [...]`

Parameters `message-type+|-`

One of the following message types, followed by a plus (+) to enable or a minus (-) to disable inclusion in the log:

- `awt`: Auto-write-through cache triggers debug messages.
- `bkcfg`: Internal configuration debug messages.
- `cache`: Cache debug messages.
- `capi`: Internal CAPI debug messages.
- `capi2`: Internal CAPI tracing debug messages.
- `disk`: Disk interface debug messages.
- `emp`: EMP debug messages.
- `fo`: Failover and recovery debug messages.
- `fruid`: FRU ID debug messages.
- `hb`: Not used.
- `host` or `host-dbg`: Host interface debug messages.
- `init`: Not used.
- `ioa`: I/O interface driver debug messages (standard).
- `iob`: I/O interface driver debug messages (resource counts).
- `ioc`: I/O interface driver debug messages (upper layer, verbose).
- `iod`: I/O interface driver debug messages (lower layer, verbose).
- `mem`: Internal memory debug messages.
- `misc`: Internal debug messages.
- `msg`: Inter-controller message debug messages.
- `mui`: Internal service interface debug messages.
- `ps`: Not used.
- `raid`: RAID debug messages.
- `rcm`: Removable-component manager debug messages.
- `res2`: Internal debug messages.
- `resmgr`: Reservation Manager debug messages.

Example Include RAID and cache messages, exclude EMP messages, and leave other message types unchanged:

```
# set debug-log-parameters raid+ cache+ emp-
```

```
Success: Command completed successfully. - Debug-log parameters were changed. (2012-01-21 11:58:38)
```

See also • [show debug-log-parameters](#) on page 58

set expander-fault-isolation

△ **CAUTION:** For use by or with direction from a service technician.

Description The EC in each IOM performs fault-isolation analysis of SAS expander PHY statistics. When one or more error counters for a specific PHY exceed the built-in thresholds, the PHY is disabled to maintain storage system operation.

While troubleshooting a storage system problem, a service technician can use this command to temporarily disable fault isolation for a specific EC in a specific enclosure.

 **NOTE:** If fault isolation is disabled, be sure to re-enable it before placing the system back into service. Serious problems can result if fault isolation is disabled and a PHY failure occurs.

Syntax `set expander-fault-isolation`
 `[wwn wwn]`
 `encl enclosure-ID`
 `controller a|b|both`
 `enabled|disabled|on|off`

Parameters `wwn wwn`
Optional. The WWN of the enclosure containing the PHY. Specify either this parameter or the `encl` parameter.

`encl enclosure-ID`
The enclosure ID of the enclosure containing the PHY. Specify either this parameter or the `wwn` parameter.

`controller a|b|both`
The IOM containing the EC whose setting you want to change: A, B, or both.

`enabled|disabled|on|off`
Whether to enable or disable PHY fault isolation.

Example Disable PHY fault isolation for EC A in an enclosure:

```
# set expander-fault-isolation encl 0 controller a disabled
Success: Command completed successfully. - Expander fault isolation was
disabled. (2012-01-21 12:05:41)
```

Re-enable PHY fault isolation for EC A in the same enclosure:

```
# set expander-fault-isolation encl 0 controller a enabled
Success: Command completed successfully. - Expander fault isolation was
enabled. (2012-01-21 12:05:51)
```

See also

- [set expander-phy](#) on page 53
- [show enclosures](#)
- [show expander-status](#) on page 66

set expander-phy

△ **CAUTION:** For use by or with direction from a service technician.

Description Disables or enables a specific PHY.

Syntax set expander-phy
[encl *enclosure-ID*]
controller a|b|both
[type
drive|inter-exp|sc|sc-0|sc-1|ingress|ingress-0|ingress-1|egress
|egress-0|egress-1]
[phy *phy-ID*]
enabled|disabled|on|off
[wnn *wnn*]

Parameters encl *enclosure-ID*
Optional. The enclosure ID of the enclosure containing the PHY. Specify either this parameter or the wnn parameter.

controller a|b|both

The IOM containing the PHY to enable or disable: A, B, or both.

type drive|inter-exp|sc|sc-0|sc-1|ingress|ingress-0|ingress-1|egress
|egress-0|egress-0]

Optional. The PHY type:

- drive: PHY connected to a disk drive.
- inter-exp: PHY in an expansion module that communicates between its expander and the expander in the partner expansion module.
- sc: PHY in the ingress bus to the SC.
- sc-0: PHY in the ingress bus to the local SC.
- sc-1: PHY in the ingress bus to the partner SC.
- ingress: PHY in an ingress port.
- ingress-0: PHY in an ingress port.
- ingress-1: PHY in an ingress port.
- egress: PHY in an egress port.
- egress-0: PHY in an egress port.
- egress-1: PHY in an egress port.

phy *phy-ID*

Optional. The logical PHY number.

```
set expander-phy
  [encl enclosure-ID]
  controller a|b|both
  [type
  drive|inter-exp|sc|sc-0|sc-1|ingress|ingress-0|ingress-1|egress
  |egress-0|egress-1]
  [phy phy-ID]
  enabled|disabled|on|off
  [wnn wnn]
```

enabled|disabled|on|off

Whether to enable or disable the specified PHY.

wnn *wnn*

Optional. The WWN of the PHY. Specify either this parameter or the encl parameter.

Example Disable the first egress PHY in controller A, and check the resulting status:

```
# set expander-phy encl 0 controller a type egress phy 0 disabled
Success: Command completed successfully. - Disabled PHY 0 on controller
a in enclosure 0. (PHY type: egress) (2012-01-21 12:07:36)
```

```
# show expander-status
Encl  Ctlr  Phy  Type      Status      Elem Status  Disabled  Reason
-----
...
0      A      0    Egress  Disabled  Disabled    Disabled  PHY control
-----
Success: Command completed successfully. (2012-01-21 12:03:42)
```

Enable the PHY for disk 5 in controller B, and check the resulting status:

```
# set expander-phy encl 0 controller b type drive phy 5 enabled
Success: Command completed successfully. - Enabled PHY 5 on controller b
in enclosure 0. (PHY type: drive) (2012-01-21 12:07:50)
```

```
# show expander-status
Encl  Ctlr  Phy  Type      Status      Elem Status  Disabled  Reason
-----
...
0      B      5    Drive    Enabled-Healthy  OK          Enabled
-----
Success: Command completed successfully. (2012-01-21 12:03:42)
```

- See also**
- [set expander-fault-isolation](#) on page 52
 - [show enclosures](#)
 - [show expander-status](#) on page 66

set led

Description Changes the state of the ID LED on a specified disk or enclosure. For a disk this affects the fault LED. For an enclosure this affects the unit locator LED. LEDs are described in [System LEDs](#) on page 197.

Syntax To set a disk LED:

```
set led
    disk ID
        enable|disable|on|off
```

To set an enclosure LED:

```
set led
    enclosure ID
        enable|disable|on|off
```

Parameters *disk ID*
The disk to locate. For disk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

enclosure ID
The enclosure to locate.

`enable|disable|on|off`
Specifies to set or unset the LED.

Example Identify disk 5 in the first enclosure:

```
# set led disk 0.5 on
Success: Command completed successfully. - Enabling identification LED
for disk 0.5... (2012-01-21 12:23:18)
```

Stop identifying the first enclosure:

```
# set led enclosure 0 off
Success: Disabling identification LED for enclosure 0... (2012-01-21
12:24:03)
```

set protocols

Description Enables or disables management services and protocols.

Syntax set protocols
[debug enabled|disabled|on|off]
[ftp enabled|disabled|on|off]
[http enabled|disabled|on|off]
[https enabled|disabled|on|off]
[ses enabled|disabled|on|off]
[smis enabled|disabled|on|off]
[snmp enabled|disabled|on|off]
[ssh enabled|disabled|on|off]
[telnet enabled|disabled|on|off]
[usmis enabled|disabled|on|off]

Parameters debug enabled|disabled|on|off
Optional. Enables or disables the Telnet debug port.

ftp enabled|disabled|on|off
Optional. Enables or disables the expert interface for updating firmware.

http enabled|disabled|on|off
Optional. Enables or disables the standard RAIDar web server.

https enabled|disabled|on|off
Optional. Enables or disables the secure RAIDar web server.

ses enabled|disabled|on|off
Optional. Enables or disables the in-band SES interface.

smis enabled|disabled|on|off
Optional. Enables or disables the secure SMI-S interface. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTPS port 5989. HTTPS port 5989 and HTTP port 5988 cannot be enabled at the same time, so enabling this option will disable port 5988.

snmp enabled|disabled|on|off
Optional. Enables or disables the SNMP interface. Disabling this option disables all SNMP requests to the MIB and disables SNMP traps. To configure SNMP traps use the set snmp-parameters command.

ssh enabled|disabled|on|off
Optional. Enables or disables the SSH CLI.

telnet enabled|disabled|on|off
Optional. Enables or disables the standard CLI.

usmis enabled|disabled|on|off

Optional. Enables or disables the unsecure SMI-S interface. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTP port 5988. HTTP port 5988 and HTTPS port 5989 cannot be enabled at the same time, so enabling this option will disable port 5989.

Example Disable unsecure HTTP connections and enable FTP:

```
# set protocols http disabled ftp enabled
Success: Command completed successfully. (2012-01-21 14:46:55)
```

See also • [show protocols](#) on page 74

show controller-statistics

Description Shows live performance statistics for controller A, B, or both.

Properties shown only in XML API format are described in the *AssuredSAN 4000 Series CLI Reference Guide*.

Syntax show controller-statistics [a|b|both]

Parameters a|b|both

Optional. Specifies whether to show information for controller A, B, or both. If this parameter is omitted, information is shown for both controllers.

Output Durable ID
Controller ID in the form `controller_ID`.

CPU Load
Percentage of time the processor is busy, from 0–100.

Power On Time (Secs)
Number of seconds since the controller was restarted.

Bytes per second
Data transfer rate calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

IOPS
IOPS calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

Number of Reads
Number of read operations since these statistics were last reset or since the controller was restarted.

Number of Writes
Number of write operations since these statistics were last reset or since the controller was restarted.

Data Read
Amount of data read since these statistics were last reset or since the controller was restarted.

Data Written
Amount of data written since these statistics were last reset or since the controller was restarted.

Num Forwarded Cmds
The current count of commands that are being forwarded or are queued to be forwarded to the partner controller for processing. This value will be zero if no commands are being forwarded or are queued to be forwarded.

Reset Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when these statistics were last reset, either by a user or by a controller restart.

Total Power On Hours

The total amount of hours the controller has been powered on in its life time.

Example Show statistics for controller A:

```
# show controller-statistics a
Durable ID      CPU Load  Power On Time (Secs)  Bytes per second  IOPS
Number of Reads Number of Writes  Data Read  Data Written
Num  Forwarded Cmds  Reset Time                Total Power On Hours
-----
controller_A  5          437034                5596.6KB          406
235196190    331183103          6922.3GB    7999.1GB
0            2012-01-18 10:14:50  127449.88
-----
Success: Command completed successfully. (2012-01-18 11:34:41)
```

- See also**
- `reset all-statistics`
 - `reset controller-statistics`
 - [show disk-statistics](#) on page 59
 - [show host-port-statistics](#) on page 72
 - [show vdisk-statistics](#) on page 79
 - [show volume-statistics](#) on page 83

show debug-log-parameters

△ **CAUTION:** For use by or with direction from a service technician.

Description Shows which debug message types are enabled (`On`) or disabled (`Off`) for inclusion in the SC debug log.

Syntax `show debug-log-parameters`

Output

- `host`: Host interface debug messages.
- `disk`: Disk interface debug messages.
- `mem`: Internal memory debug messages.
- `fo`: Failover and recovery debug messages.
- `msg`: Inter-controller message debug messages.
- `ioa`: I/O interface driver debug messages (standard).
- `iob`: I/O interface driver debug messages (resource counts).
- `ioc`: I/O interface driver debug messages (upper layer, verbose).
- `iod`: I/O interface driver debug messages (lower layer, verbose).
- `misc`: Internal debug messages.
- `rcm`: Removable-component manager debug messages.
- `raid`: RAID debug messages.
- `cache`: Cache debug messages.
- `emp`: EMP debug messages.
- `capi`: Internal CAPI debug messages.
- `mui`: Internal service interface debug messages.
- `bkcfg`: Internal configuration debug messages.
- `awt`: Auto-write-through cache triggers debug messages.
- `res2`: Internal debug messages.
- `capi2`: Internal CAPI tracing debug messages.
- `fruid`: FRU ID debug messages.
- `resmgr`: Reservation Manager debug messages.
- `init`: Not used.
- `ps`: Not used.
- `hb`: Not used.

Example Show debug log parameters:

```
# show debug-log-parameters
Debug Log Parameters
-----
host: On
disk: On
mem: Off
...

Success: Command completed successfully. (2012-01-18 14:59:52)
```

See also • [set debug-log-parameters](#) on page 51

show disk-statistics

Description Shows live or historical performance statistics for disks. You can view live statistics for all or specified disks, or historical statistics for a specified disk. The system samples disk-performance statistics every quarter hour and retains performance data for 6 months.

The historical option allows you to specify a time range or a number (count) of data samples to include. It is not recommended to specify both the `time-range` and `count` parameters; if both parameters are specified, and more samples exist for the specified time range, the samples' values will be aggregated to show the required number of samples.

Properties shown only in XML API format are described in the *AssuredSAN 4000 Series CLI Reference Guide*.

Syntax To show live statistics:

```
show disk-statistics [disks]
```

To show historical statistics:

```
show disk-statistics
    disk
    historical
    [time-range "date/time-range"]
    [count number-of-data-samples]
    [all]
```

Parameters *disks*

Optional. Identifies one or more disks to show live statistics for. If this parameter is omitted, statistics will be shown for all disks. For disk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

disk

Identifies one disk to show historical statistics for. For disk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

historical

Optional. Specifies to show historical statistics. If this parameter is omitted, live statistics will be shown.

time-range "*date/time-range*"

Optional. Specifies the date/time range of historical statistics to show, in the format "`start yyyy-mm-dd hh:mm [AM|PM] end yyyy-mm-dd hh:mm [AM|PM]`". If the start date/time is specified but no end date/time is specified, the current date/time will be used as the end date/time. The system will return the oldest sample taken after the start time and the latest sample taken before the end time. If the specified start date/time is earlier than the oldest sample, that sample will be used as the start date/time. If you specify this parameter, do not specify the `count` parameter. If this parameter is omitted, the most recent 100 data samples will be displayed.

count *number-of-data-samples*

Optional. Specifies the number of data samples to display, from 1–100. Each sample will be shown as a separate row in the command output. If this parameter is omitted, 100 samples will be shown. If you specify this parameter, do not specify the `time-range` parameter.

all

Optional. Specifies to show the full set of performance metrics. If this parameter is omitted, the default set of performance metrics will be shown.

Output Durable ID

(Live) Disk ID in the form `disk_enclosure-number.disk-number`.

Serial Number
Disk serial number.

Bytes per second
Data transfer rate calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

IOPS
IOPS calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

Number of Reads
Number of read operations since these statistics were last reset or since the controller was restarted.

Number of Writes
Number of write operations since these statistics were last reset or since the controller was restarted.

Data Read
Amount of data read since these statistics were last reset or since the controller was restarted.

Data Written
Amount of data written since these statistics were last reset or since the controller was restarted.

Reset Time
Date and time, in the format *year-month-day hour:minutes:seconds*, when these statistics were last reset, either by a user or by a controller restart.

**Output
(Historical)**

Durable ID
Disk ID in the form *disk_enclosure-number.disk-number*.

Serial Number
Disk serial number.

Total I/Os
Total number of read and write operations since the last sampling time.

Data Transferred
Total amount of data read and written since the last sampling time.

Total IOPS
Total number of read and write operations per second since the last sampling time.

Total B/s
Total data transfer rate, in bytes/s, since the last sampling time.

I/O Resp Time
Average response time, in microseconds, for read and write operations since the last sampling time.

Sample Time
Date and time, in the format *year-month-day hour:minutes:seconds*, when the data sample was taken.

**Output
(Historical,
all)**

Durable ID
Disk ID in the form *disk_enclosure-number.disk-number*.

Serial Number
Disk serial number.

Total I/Os
Total number of read and write operations since the last sampling time.

Number of Reads

Shown by the `all` parameter. Number of read operations since the last sampling time.

Number of Writes

Shown by the `all` parameter. Number of write operations since the last sampling time.

Data Transferred

Total amount of data read and written since the last sampling time.

Data Read

Shown by the `all` parameter. Amount of data read since the last sampling time.

Data Written

Shown by the `all` parameter. Amount of data written since the last sampling time.

Total IOPS

Total number of read and write operations per second since the last sampling time.

Read IOPS

Shown by the `all` parameter. Number of read operations per second since the last sampling time.

Write IOPS

Shown by the `all` parameter. Number of write operations per second since the last sampling time.

Total B/s

Total data transfer rate, in bytes/s, since the last sampling time.

Read B/s

Shown by the `all` parameter. Data transfer rate, in bytes/s, for read operations since the last sampling time.

Write B/s

Shown by the `all` parameter. Data transfer rate, in bytes/s, for write operations since the last sampling time.

Queue Depth

Shown by the `all` parameter. Average number of pending read and write operations being serviced since the last sampling time. This value represents periods of activity only and excludes periods of inactivity.

I/O Resp Time

Average response time, in microseconds, for read and write operations since the last sampling time.

Read Resp Time

Shown by the `all` parameter. Average response time, in microseconds, for read operations since the last sampling time.

Write Resp Time

Shown by the `all` parameter. Average response time, in microseconds, for write operations since the last sampling time.

Average I/O Size

Shown by the `all` parameter. Average data size of read and write operations since the last sampling time.

Average Read I/O Size

Shown by the `all` parameter. Average data size of read operations since the last sampling time.

Average Write I/O Size

Shown by the `all` parameter. Average data size of write operations since the last sampling time.

Number of Disk Errors

Shown by the `all` parameter. Total number of disk errors detected since the last sampling time. Error types include: number of SMART events; number of timeouts accessing the disk; number of times the disk did not respond; number of attempts by the storage system to spin-up the disk; media errors generated by the disk as specified by its manufacturer; non-media errors (generated by the storage system, or by the disk and not categorized as media errors); number of bad-block reassignments.

Sample Time

Date and time, in the format `year-month-day hour:minutes:seconds`, when the data sample was taken.

Example Show live statistics for disks 1.1 and 2.1:

```
# show disk-statistics 1.1,2.1
Durable ID  Serial Number  Bytes per second  IOPS  Number of Reads
  Number of Writes  Data Read  Data Written  Reset Time
-----
disk_1.1    SN                3936.2KB          67    23241330
14457080    1309.8GB  857.1GB          2012-01-17 19:22:54
disk_2.1    SN                4972.0KB          85    33941798
14529518    1935.5GB  846.1GB          2012-01-17 21:01:20
-----
Success: Command completed successfully. (2012-01-18 12:53:55)
```

Show historical statistics from a specified date and time range for disk 1.5:

```
# show disk-statistics 1.5 historical time-range "start 2011-12-05 4:40
PM end 2011-12-05 5:00 PM"
Durable ID          Serial Number
-----
disk_1.5            SN

      Total I/Os  Data Transferred  Total IOPS  Total B/s  I/O Resp Time
      Sample Time
-----
183018    11.9GB          203        13.3MB    222
2011-12-05 17:00:00
1961773    128.5GB         2179       142.8MB    240
2011-12-05 16:45:00
-----
Success: Command completed successfully. (2012-01-18 12:39:11)
```

Show all samples of historical statistics for disk 1.5:

```
# show disk-statistics 1.5 historical all
Durable ID          Serial Number
-----
disk_1.5            SN

Total I/Os   Number of Reads   Number of Writes   Data Transferred
Data Read   Data Written   Total IOPS   Read IOPS   Write IOPS
Total B/s   Read B/s   Write B/s   Queue Depth   I/O Resp Time
Read Resp Time   Write Resp Time   Average I/O Size
Average Read I/O Size   Average Write I/O Size
Number of Disk Errors   Sample Time
-----
121174          60588          60586          5800.5MB
2900.3MB   2900.1MB          134          67          67
6445.0KB   3222.5KB   3222.0KB   709072   13062
12759          13366          47.6KB
47.6KB          47.6KB
0          2012-01-18 12:30:00
...
-----
Success: Command completed successfully. (2012-01-18 12:39:27)
```

- See also**
- [reset all-statistics](#)
 - [reset disk-error-statistics](#)
 - [reset disk-statistics](#)
 - [show controller-statistics](#) on page 56
 - [show disks](#)
 - [show host-port-statistics](#) on page 72
 - [show vdisk-statistics](#) on page 79
 - [show volume-statistics](#) on page 83

show events

Description Shows events logged by each controller in the storage system. A separate set of event numbers is maintained for each controller. Each event number is prefixed with a letter identifying the controller that logged the event.

Events are listed from newest to oldest, based on a timestamp with one-second granularity; therefore the event log sequence matches the actual event sequence within about one second.

For further information about diagnosing and resolving problems, see:

- [Troubleshooting using system LEDs](#) on page 91
- [System LEDs](#) on page 197
- [Verifying component failure](#) on page 106

Syntax To show a certain number of events:

```
show events
  [detail]
  [last #]
  [a|b|both|error]
```

To show events by time:

```
show events
  [detail]
  [from timestamp]
  [to timestamp]
  [a|b|both|error]
```

To show events by ID:

```
show events
  [detail]
  [from-event event-ID]
  [to-event event-ID]
  [a|b|both|error]
```

Parameters *detail*

Optional. Shows additional information and recommended actions for displayed events. This information is also in [Troubleshooting using system LEDs](#) on page 91 and [Event descriptions](#) on page 149.

last #

Optional. Shows the latest specified number of events. If this parameter is omitted, all events are shown.

from timestamp

Optional. Shows events including and after a timestamp specified with the format *MMDDYYhhmmss*. For example, 043011235900 represents April 30 2011 at 11:59:00 p.m. This parameter can be used with the *to* parameter or the *to-event* parameter.

to timestamp

Optional. Shows events before and including a timestamp specified with the format *MMDDYYhhmmss*. For example, 043011235900 represents April 30 2011 at 11:59:00 p.m. This parameter can be used with the *from* parameter or the *from-event* parameter.

from-event event-ID

Optional. Shows events including and after the specified event ID. If this number is smaller than the ID of the oldest event, events are shown from the oldest available event. Events are shown only for the controller that the event ID specifies (A or B). This parameter can be used with the *to* parameter or the *to-event* parameter.

to-event event-ID

Optional. Shows events before and including the specified event ID. If this number is larger than the ID of the oldest event, events are shown up to the latest event. Events are shown only for the controller that the event ID specifies (A or B). This parameter can be used with the *from* parameter or the *from-event* parameter.

a|b|both|error

Optional. Specifies to filter the event listing:

- *a*: Shows events from controller A only. Do not use this parameter with the *from-event* parameter or the *to-event* parameter.
- *b*: Shows events from controller B only. Do not use this parameter with the *from-event* parameter or the *to-event* parameter.
- *both*: Shows events from both controllers. Do not use this parameter with the *from-event* parameter or the *to-event* parameter.
- *error*: Shows Warning, Error, and Critical events.

- Output**
- Date and time when the event was logged
 - Event code identifying the type of event to help diagnose problems; for example, [181]
 - Event ID prefixed by A or B, indicating which controller logged the event; for example, #A123
 - Model, serial number, and ID of the controller module that logged the event
 - Severity:
 - **CRITICAL:** A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.
 - **ERROR:** A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
 - **WARNING:** A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.
 - **INFORMATIONAL:** A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.
 - Event-specific message giving details about the event

Example Show the last two events:

```
# show events last 2
```

Show the last three non-Informational events:

```
# show events last 3 error
```

Show all events from April 30 2011 at 11:59:00 p.m. through May 2 2011 at 11:59:00 a.m.:

```
# show events from 043011235900 to 050211115900
```

Show a range of events logged by controller A:

```
# show events from-event a100 to-event a123
```

Show detailed output for a specific event:

```
# show events from-event A2264 to-event A2264 detail
```

- See also**
- [clear events](#) on page 40
 - [set snmp-parameters](#)
 - [show snmp-parameters](#)

show expander-status

△ **CAUTION:** For use by or with direction from a service technician.

Description Shows diagnostic information relating to SAS EC physical channels, known as PHY lanes. For each enclosure, this command shows status information for PHYs in IOM A and then IOM B.

Syntax `show expander-status`

Output `Encl`
Enclosure that contains the SAS expander.

`Ctlr`
IOM that contains the SAS expander.

`Phy`
Identifies a PHY's logical location within a group based on the PHY type. Logical IDs are 0–23 for drive PHYs; 0–1 for SC PHYs; and 0–3 for other PHYs. If the PHY's controller module or expansion module is not installed, this field shows "--".

`Type`

- `Drive`: 1-lane PHY that communicates between the expander and a disk drive.
- `Egress`: 4-lane PHY that communicates between the expander and an expansion port or SAS Out port.
- `SC-1`: (Controller module only) 2-lane PHY that communicates between the expander and the partner's expander.
- `SC-0`: (Controller module only) 4-lane PHY that communicates between the expander and the SC.
- `Ingress`: (Expansion module only) 4-lane PHY that communicates between the expander and an expansion port.
- `Inter-Exp`: (Expansion module only) Communicates between the expander and the partner's expander.
- `Undefined`: No status information is available.
- `Unused`: The PHY exists in the expander but is not connected, by design.

`Status`

- `Enabled - Healthy`: The PHY is enabled and healthy.
- `Enabled - Degraded`: The PHY is enabled but degraded.
- `Disabled`: The PHY has been disabled by a user or by the system.

Elem Status

A standard SES status for the element:

- **Disabled:** Critical condition is detected.
- **Error:** Unrecoverable condition is detected. Appears only if there is a firmware problem related to PHY definition data.
- **Non-critical:** Non-critical condition is detected.
- **Not Used:** Element is not installed in enclosure.
- **OK:** Element is installed and no error conditions are known.
- **Unknown:** Either:
 - Sensor has failed or element status is not available. Appears only if an IOM indicates it has fewer PHYs than the reporting IOM, in which case all additional PHYs are reported as unknown.
 - Element is installed with no known errors, but the element has not been turned on or set into operation.

Disabled

- **Enabled:** PHY is enabled.
- **Disabled:** PHY is disabled.

Reason

- **Blank if Elem Status is OK.**
- **Error count interrupts:** PHY disabled because of error-count interrupts.
- **Phy control:** PHY disabled by a SES control page as a result of action by an SC or user.
- **Not ready:** PHY is enabled but not ready. Appears for SC-1 PHYs when the partner IOM is not installed. Appears for Drive, SC-1, or Ingress PHYs when a connection problem exists such as a broken connector.
- **Drive removed:** PHY disabled because drive slot is empty.
- **Unused - disabled by default:** PHY is disabled by default because it is not used.
- **Excessive Phy changes:** PHY is disabled because of excessive PHY change counts.

Example Show expander status with an empty disk slot:

```
# show expander-status
Encl  Ctlr  Phy  Type  Status          Elem Status  Disabled
Reason
-----
0     A     0    Drive  Enabled - Healthy  OK           Enabled
0     A     1    Drive  Enabled - Degraded Non-critical  Enabled
Not ready
...
0     A     23   Drive  Disabled          OK           Disabled
Drive removed
0     A     0    SC-1   Enabled - Healthy  OK           Enabled
0     A     1    SC-1   Enabled - Healthy  OK           Enabled
0     A     0    SC-0   Enabled - Healthy  OK           Enabled
...
0     A     3    SC-0   Enabled - Healthy  OK           Enabled
0     A     0    Egress Enabled - Healthy  OK           Enabled
...
0     A     3    Egress Enabled - Healthy  OK           Enabled
-----
Success: Command completed successfully. (2012-01-18 15:02:13)
Encl  Ctlr  Phy  Type  Status          Elem Status  Disabled
Reason
-----
0     B     0    Drive  Enabled - Healthy  OK           Enabled
0     B     1    Drive  Enabled - Degraded Non-critical  Enabled
Not ready
...
0     B     23   Drive  Disabled          OK           Disabled
Drive removed
0     B     0    SC-1   Enabled - Healthy  OK           Enabled
0     B     1    SC-1   Enabled - Healthy  OK           Enabled
0     B     0    SC-0   Enabled - Healthy  OK           Enabled
...
0     B     0    Egress Enabled - Healthy  OK           Enabled
...
0     B     3    Egress Enabled - Healthy  OK           Enabled
-----
Success: Command completed successfully. (2012-01-18 15:02:13)
```

- See also**
- [clear expander-status](#) on page 40
 - [set expander-fault-isolation](#) on page 52
 - [set expander-phy](#) on page 53

show frus

Description Shows FRU information for the storage system. Some information is for use by service technicians.

Syntax `show frus`

Output **FRU fields:**

Name

- CHASSIS_MIDPLANE: 2U chassis and midplane circuit board
- RAID_IOM: Controller module
- IOM: Expansion module
- POWER_SUPPLY: PSU

Description

FRU description

Part Number

FRU part number

Serial Number

FRU serial number

Revision

Hardware revision level

Dash Level

FRU template revision number

FRU Shortname

Short description

Manufacturing Date

Date and time in the format *year-month-day hour.minutes.seconds* when a PCBA was programmed or a PSU was manufactured

Manufacturing Location

City, state/province, and country where the FRU was manufactured

Manufacturing Vendor ID

JEDEC ID of the manufacturer

FRU Location

Location of the FRU in the enclosure:

- MID-PLANE SLOT: Chassis midplane
- UPPER IOM SLOT: Controller module or expansion module A
- LOWER IOM SLOT: Controller module or expansion module B
- LEFT PSU SLOT: PSU on the left, as viewed from the rear
- RIGHT PSU SLOT: PSU on the right, as viewed from the rear

Configuration SN

Configuration serial number

FRU Status

- Absent: Component is not present
- Fault: One or more subcomponents has a fault
- OK: All subcomponents are operating normally
- Not Available: Status is not available

Enclosure ID
Enclosure number

Original SN
For a PSU, the original manufacturer serial number; otherwise, does not display.

Original PN
For a PSU, the original manufacturer part number; otherwise, does not display.

Original Rev
For a PSU, the original manufacturer hardware revision; otherwise, does not display.

Example Show FRUs

```
# show frus
FRU
---
Name: CHASSIS_MIDPLANE
Description: Box 2U12 Chass+Midplane 6 GB V2
Part Number: PN
Serial Number: SN
Revision: Rev
Dash Level:
FRU Shortname: Midplane/Chassis
Manufacturing Date: 2012-02-29 13:00:25
Manufacturing Location: Longhua, Schenzhen, CN
Manufacturing Vendor ID: ID
FRU Location: MID-PLANE SLOT
Configuration SN: SN
FRU Status: OK
Enclosure ID: 0

...

FRU
---
Name: POWER_SUPPLY
Description: FRU PSU 595W AC 2U
Part Number: PN
Serial Number: SN
Revision: Rev
Dash Level:
FRU Shortname: AC Power Supply
Manufacturing Date: 2012-02-18 07:45:09
Manufacturing Location: Zhongshan, Guangdong, CN
Manufacturing Vendor ID: ID
FRU Location: LEFT PSU SLOT
Configuration SN: SN
FRU Status: OK
Original SN: SN
Original PN: PN
Original Rev: Rev
Enclosure ID: 0

Success: Command completed successfully. (2012-01-18 15:02:52)
```

- See also**
- set host-parameters
 - show ports

show host-parameters

Description Shows information about host ports on both controllers. This command shows the same information as the `show ports` command.

Syntax `show host-parameters`

Output Ports
Controller ID and port number

Media

- FC (L): FC-AL (public or private)
- FC (P): FC Point-to-Point
- FC (-): FC disconnected
- SAS: SAS

Target ID

Port WWN

Status

- Up: Port is cabled and has an I/O link.
- Disconnected: Either no I/O link is detected or the port is not cabled.

Speed (A)

Actual link speed in Gbit/s. Blank if not applicable.

Speed (C)

Configured host-port link speed. Does not display for SAS.

- FC: Auto, 8Gb, 4Gb, or 2Gb (Gbit/s)
- Blank if not applicable

Health

- OK
- Degraded
- Fault
- N/A

Health Reason

If Health is not OK, this field shows the reason for the health state.

Health Recommendation

If Health is not OK, this field shows recommended actions to take to resolve the health issue.

Topo (C)

FC only. Configured topology.

Width

SAS only. Number of PHY lanes in the SAS port. Displays instead of PID.

PID

FC only. Primary ID, or blank if not applicable. Displays instead of Width.

Example Show port information for a system with two FC ports:

```
# show host-parameters
Ports Media Target ID Status Speed(A) Speed(C)
Health Health Reason Health Recommendation
-----
A0 FC(L) WWPN Up 8Gb Auto
OK

Topo(C) PID
-----
Loop 0

A1 FC(-) WWPN Disconnected Auto N/A
There is no host connection to this host port. - No action is
required.

Topo(C) PID
-----
Loop 0

-----
Success: Command completed successfully. (2012-01-18 15:03:24)
```

Example Show port information for a system with two SAS ports:

```
# show host-parameters
Ports Media Target ID Status Speed(A)
Health Health Reason Health Recommendation
-----
A0 SAS WWPN Up Auto
OK

Topo(C) Width
-----
Direct 0

A1 SAS WWPN Disconnected Auto N/A
There is no host connection to this host port. - No action is
required.

Topo(C) Width
-----
Loop 0

-----
Success: Command completed successfully. (2012-01-18 15:03:24)
```

See also

- set host-parameters
- show ports

show host-port-statistics

Description Shows live performance statistics for each controller host port. For each host port these statistics quantify I/O operations through the port between a host and a volume. For example, each time a host writes to a volume's cache, the host port's statistics are adjusted.

Syntax show host-port-statistics [ports *ports*]

Parameters `ports ports`
Optional. The controller ID and port number of ports to show information about. For port syntax, see the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command. If this parameter is omitted, information is shown for all host ports.

Output `Durable ID`
Host port ID in the form `hostport_controller-ID-and-port-number`.

`Bytes per second`
Data transfer rate calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

`IOPS`
IOPS calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

`Number of Reads`
Number of read operations since these statistics were last reset or since the controller was restarted.

`Number of Writes`
Number of write operations since these statistics were last reset or since the controller was restarted.

`Data Read`
Amount of data read since these statistics were last reset or since the controller was restarted.

`Data Written`
Amount of data written since these statistics were last reset or since the controller was restarted.

`Queue Depth`
Number of pending I/O operations being serviced.

`I/O Resp Time`
Average response time in microseconds for read and write operations, calculated over the interval since these statistics were last requested or reset.

`Read Resp Time`
Average response time in microseconds for all read operations, calculated over the interval since these statistics were last requested or reset.

`Write Resp Time`
Average response time in microseconds for all write operations, calculated over the interval since these statistics were last requested or reset.

`Reset Time`
Date and time, in the format *year-month-day hour:minutes:seconds*, when these statistics were last reset, either by a user or by a controller restart.

Example Show host-port statistics:

```
# show host-port-statistics
Durable ID   Bytes per second   IOPS   Number of Reads   Number of Writes
  Data Read   Data Written   Queue Depth   I/O Resp Time   Read Resp Time
  Write Resp Time   Reset Time
-----
hostport_A0  72.0MB           549    45372779          5020328
  5947.1GB    657.8GB         0        1517248          1106826
  5226569           2012-01-17 21:01:20
...
-----
Success: Command completed successfully. (2012-01-18 16:25:41)
```

- See also**
- `reset all-statistics`
 - `reset host-port-statistics`
 - [show controller-statistics](#) on page 56
 - [show disk-statistics](#) on page 59
 - `show ports`
 - [show vdisk-statistics](#) on page 79
 - [show volume-statistics](#) on page 83

show protocols

Description Shows which management services and protocols are enabled or disabled.

Syntax `show protocols`

Example Show the status of service and security protocols:

```
# show protocols
Service and Security Protocols
-----
Web Browser Interface (HTTP): Enabled
Secure Web Browser Interface (HTTPS): Enabled
Command Line Interface (Telnet): Enabled
Secure Command Line Interface (SSH): Enabled
Storage Management Initiative Specification (SMI-S): Enabled
Unsecure Storage Management Initiative Specification (SMI-S 5988):
  Disabled
File Transfer Protocol (FTP): Disabled
Simple Network Management Protocol (SNMP): Enabled
Service Debug (Debug): Disabled
In-band SES Management (SES): Enabled

Success: Command completed successfully. (2012-01-18 15:13:23)
```

- See also**
- [set protocols](#) on page 55

show redundancy-mode

Description Shows the redundancy status of the system.

Syntax `show redundancy-mode`

Output Controller Redundancy Mode

Shows the system's operating mode, also called the cache redundancy mode:

- **Independent Cache Performance Mode:** Controller failover is disabled and data in a controller's write-back cache is not mirrored to the partner controller. This improves write performance at the risk of losing unwritten data if a controller failure occurs while there is data in controller cache.
- **Active-Active ULP:** Both controllers are active using ULP. Data for volumes configured to use write-back cache is automatically mirrored between the two controllers to provide fault tolerance.
- **Fail Over:** Operation has failed over to one controller because its partner is not operational. The system has lost redundancy.
- **Down:** Both controllers are not operational.

Controller Redundancy Status

- **Redundant with independent cache:** Both controllers are operational but are not mirroring their cache data to each other.
- **Redundant:** Both controllers are operational.
- **Operational but not redundant:** In active-active mode, one controller is operational and the other is offline. In single-controller mode, the controller is operational.
- **Down:** This controller is not operational.
- **Unknown:** Status information is not available.

Controller *ID* Status

- **Operational:** The controller is operational.
- **Down:** The controller is installed but not operational.
- **Not Installed:** The controller is not installed.

Controller *ID* Serial Number

- **Controller module serial number**
- **Not Available:** The controller is down or not installed.

Other MC Status

The operational status of the partner MC.

- **Operational**
- **Not Operational**

Example From either controller, show the redundancy status where both controllers are operating:

```
# show redundancy-mode
System Redundancy
-----
Controller Redundancy Mode: Active-Active ULP
Controller Redundancy Status: Redundant
Controller A Status: Operational
Controller A Serial Number: SN
Controller B Status: Operational
Controller B Serial Number: SN
Other MC Status: Operational

Success: Command completed successfully. (2012-01-18 11:02:36)
```

From either controller, show the redundancy status where controller B is down:

```
# show redundancy-mode
System Redundancy
-----
Controller Redundancy Mode: Fail Over
Controller Redundancy Status: Operational but not redundant
Controller A Status: Operational
Controller A Serial Number: SN
Controller B Status: Down
Controller B Serial Number: SN
Other MC Status: Not Operational

Success: Command completed successfully. (2012-02-01 11:03:39)
```

From either controller, show the redundancy status where both controllers are down:

```
# show redundancy-mode
System Redundancy
-----
Controller Redundancy Mode: Down
Controller Redundancy Status: Down
Controller A Status: Down
Controller A Serial Number: SN
Controller B Status: Down
Controller B Serial Number: SN
Other MC Status: Not Operational

Success: Command completed successfully. (2012-02-01 11:03:39)
```

show sensor-status

Description Shows the status of each environmental sensor in each enclosure.

Information shown only for a controller enclosure: on-board temperature, disk controller temperature, memory controller temperature, supercapacitor voltage and charge, overall unit (enclosure) status.

Information shown for all enclosures: temperature, voltage, and current for each IOM (controller module or expansion module); temperature, voltage, and current for each PSU.

Normal and error ranges for temperature and voltage are specified in the *AssuredSAN 4000 Series Setup Guide*.

Syntax show sensor-status

Output Encl
Enclosure number.

Sensor Name
Sensor name and location.

Value

- For a sensor, its value.
- For overall unit status, one of the status values below.

Status

- **OK:** The sensor is present and detects no error condition.
- **Warning:** The sensor detected a non-critical error condition. Temperature, voltage, or current is between the warning and critical thresholds.
- **Error:** The sensor detected a critical error condition. Temperature, voltage, or current exceeds the critical threshold.
- **Unavailable:** The sensor is present with no known errors, but has not been turned on or set into operation because it is initializing. This typically occurs during controller startup.
- **Unrecoverable:** The EMP cannot communicate with the sensor.
- **Unknown:** The sensor is present but status is not available.
- **Not Installed:** The sensor is not present.
- **Unsupported:** Status detection is not implemented.

Example Show sensor status for a system that includes a controller enclosure and a drive enclosure:

```
# show sensor-status
Encl  Sensor Name                               Value      Status
-----
0     On-Board Temperature 1-Ctrlr A              55 C      OK
0     On-Board Temperature 1-Ctrlr B              54 C      OK
0     On-Board Temperature 2-Ctrlr A              76 C      OK
0     On-Board Temperature 2-Ctrlr B              69 C      OK
0     On-Board Temperature 3-Ctrlr A              53 C      OK
0     On-Board Temperature 3-Ctrlr B              55 C      OK
0     Disk Controller Temp-Ctrlr A                31 C      OK
0     Disk Controller Temp-Ctrlr B                30 C      OK
0     Memory Controller Temp-Ctrlr A              71 C      OK
0     Memory Controller Temp-Ctrlr B              76 C      OK
0     Capacitor Pack Voltage-Ctrlr A              8.20      OK
0     Capacitor Pack Voltage-Ctrlr B              8.12      OK
0     Capacitor Cell 1 Voltage-Ctrlr A            2.04      OK
0     Capacitor Cell 1 Voltage-Ctrlr B            2.02      OK
0     Capacitor Cell 2 Voltage-Ctrlr A            2.04      OK
0     Capacitor Cell 2 Voltage-Ctrlr B            2.08      OK
0     Capacitor Cell 3 Voltage-Ctrlr A            2.03      OK
0     Capacitor Cell 3 Voltage-Ctrlr B            2.02      OK
0     Capacitor Cell 4 Voltage-Ctrlr A            2.08      OK
0     Capacitor Cell 4 Voltage-Ctrlr B            2.00      OK
0     Capacitor Charge-Ctrlr A                    100%      OK
0     Capacitor Charge-Ctrlr B                    100%      OK
0     Overall Unit Status                         OK        OK
0     Temperature Loc: upper-IOM A                42 C      OK
0     Temperature Loc: lower-IOM B                38 C      OK
0     Temperature Loc: left-PSU                   33 C      OK
0     Temperature Loc: right-PSU                  36 C      OK
0     Voltage 12V Loc: upper-IOM A                11.92     OK
0     Voltage 5V Loc: upper-IOM A                 5.08      OK
0     Voltage 12V Loc: lower-IOM B                11.86     OK
0     Voltage 5V Loc: lower-IOM B                 5.08      OK
0     Voltage 12V Loc: left-PSU                   11.93     OK
0     Voltage 5V Loc: left-PSU                     5.11      OK
0     Voltage 3.3V Loc: left-PSU                   3.48      OK
0     Voltage 12V Loc: right-PSU                  12.04     OK
0     Voltage 5V Loc: right-PSU                     5.13      OK
0     Voltage 3.3V Loc: right-PSU                  3.49      OK
0     Current 12V Loc: upper-IOM A                 4.33      OK
0     Current 12V Loc: lower-IOM B                 4.42      OK
0     Current 12V Loc: left-PSU                     5.17      OK
0     Current 5V Loc: left-PSU                       7.24      OK
0     Current 12V Loc: right-PSU                    5.80      OK
0     Current 5V Loc: right-PSU                     7.15      OK
-----
Success: Command completed successfully. (2011-10-10 15:26:37)
```

show vdisk-statistics

Description Shows live or historical performance statistics for vdisks. You can view live statistics for all or specified vdisks, or historical statistics for a specified vdisk. The system samples disk-performance statistics every quarter hour and retains performance data for 6 months.

The historical option allows you to specify a time range or a number (count) of data samples to include. It is not recommended to specify both the `time-range` and `count` parameters; if both parameters are specified, and more samples exist for the specified time range, the samples' values will be aggregated to show the required number of samples.

For each vdisk these statistics quantify destages, read-aheads, and host reads that are cache misses. For example, each time data is written from a volume's cache to disks in the vdisk that contains the volume, the vdisk's statistics are adjusted.

Properties shown only in XML API format are described in the *AssuredSAN 4000 Series CLI Reference Guide*.

Syntax To show live statistics:

```
show vdisk-statistics [vdisks]
```

To show historical statistics:

```
show vdisk-statistics
    vdisk
    historical
    [time-range "date/time-range"]
    [count number-of-data-samples]
    [all]
```

Parameters *vdisks*

Optional. Identifies one or more vdisks to show live statistics for. If this parameter is omitted, statistics will be shown for all vdisks. For vdisk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

vdisk

Identifies one vdisk to show historical statistics for. For vdisk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

historical

Optional. Specifies to show historical statistics. If this parameter is omitted, live statistics will be shown.

time-range "date/time-range"

Optional. Specifies the date/time range of historical statistics to show, in the format "`start yyyy-mm-dd hh:mm [AM|PM] end yyyy-mm-dd hh:mm [AM|PM]`". If the start date/time is specified but no end date/time is specified, the current date/time will be used as the end date/time. The system will return the oldest sample taken after the start time and the latest sample taken before the end time. If the specified start date/time is earlier than the oldest sample, that sample will be used as the start date/time. If you specify this parameter, do not specify the `count` parameter. If this parameter is omitted, the most recent 100 data samples will be displayed.

count number-of-data-samples

Optional. Specifies the number of data samples to display, from 1–100. Each sample will be shown as a separate row in the command output. If this parameter is omitted, 100 samples will be shown. If you specify this parameter, do not specify the `time-range` parameter.

all

Optional. Specifies to show the full set of performance metrics. If this parameter is omitted, the default set of performance metrics will be shown.

Output

Name

Vdisk name.

Serial Number

Vdisk serial number.

Bytes per second

Data transfer rate calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

IOPS

IOPS, calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

Number of Reads

Number of read operations since these statistics were last reset or since the controller was restarted.

Number of Writes

Number of write operations since these statistics were last reset or since the controller was restarted.

Data Read

Amount of data read since these statistics were last reset or since the controller was restarted.

Data Written

Amount of data written since these statistics were last reset or since the controller was restarted.

I/O Resp Time

Average response time in microseconds for read and write operations, calculated over the interval since these statistics were last requested or reset.

Read Resp Time

Average response time in microseconds for all read operations, calculated over the interval since these statistics were last requested or reset.

Write Resp Time

Average response time in microseconds for all write operations, calculated over the interval since these statistics were last requested or reset.

Reset Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when these statistics were last reset, either by a user or by a controller restart.

Name

Vdisk name.

Serial Number

Vdisk serial number.

Data Transferred

Total amount of data read and written since the last sampling time.

Data Read

Shown by the all parameter. Amount of data read since the last sampling time.

Data Written

Shown by the all parameter. Amount of data written since the last sampling time.

Total B/s

Data transfer rate, in bytes per second, since the last sampling time. This is the sum of Read B/s and Write B/s.

Read B/s

Shown by the `all` parameter. Data transfer rate, in bytes per second, for read operations since the last sampling time.

Write B/s

Shown by the `all` parameter. Data transfer rate, in bytes per second, for write operations since the last sampling time.

Sample Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when the data sample was taken.

**Output
(Historical)**

Name

Vdisk name.

Serial Number

Vdisk serial number.

Data Transferred

Total amount of data read and written since the last sampling time.

Total B/s

Data transfer rate, in bytes/s, since the last sampling time. This is the sum of Read B/s and Write B/s.

Sample Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when the data sample was taken.

**Output
(Historical,
all)**

Name

Vdisk name.

Serial Number

Vdisk serial number.

Data Transferred

Total amount of data read and written since the last sampling time.

Data Read

Shown by the `all` parameter. Amount of data read since the last sampling time.

Data Written

Shown by the `all` parameter. Amount of data written since the last sampling time.

Total B/s

Data transfer rate, in bytes/s, since the last sampling time. This is the sum of Read B/s and Write B/s.

Read B/s

Shown by the `all` parameter. Data transfer rate, in bytes/s, for read operations since the last sampling time.

Write B/s

Shown by the `all` parameter. Data transfer rate, in bytes/s, for write operations since the last sampling time.

Sample Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when the data sample was taken.

Example Show live statistics for vdisks VD1 and MyVdisk:

```
# show vdisk-statistics VD1,MyVdisk
Name      Serial Number  Bytes per second  IOPS  Number of Reads
          Number of Writes  Data Read  Data Written  I/O Resp Time
          Read Resp Time  Write Resp Time  Reset Time
-----
VD1      SN
          22.0MB
          82      6179839
10507038  478.8GB  1024.4GB  156240
12699     240665   2011-01-17 08:15:01
MyVdisk  SN
          22.1MB
          78      4872260
9913102   539.3GB  1044.1GB  79033
16405     109815   2012-01-17 21:01:20
-----
```

Success: Command completed successfully. (2012-01-19 16:25:26)

Show historical statistics from a specified date and time range for vdisk VD2:

```
# show vdisk-statistics VD2 historical time-range "start 2012-01-18
4:40 PM
end 2011-01-18 5:00 PM"
Name  Serial Number
-----
```

```
VD2  SN

      Data Transferred  Total B/s      Sample Time
-----
      30.5GB            33.9MB         2012-01-18 17:00:00
      31.5GB            35.0MB         2012-01-18 16:45:00
-----
```

Success: Command completed successfully. (2012-01-19 12:32:51)

Show all historical statistics (the latest 100 samples) for vdisk VD2:

```
# show vdisk-statistics VD2 historical all
Name  Serial Number
-----
VD2  SN

      Data Transferred  Data Read  Data Written  Total B/s  Read B/s
      Write B/s  Sample Time
-----
      44.8GB            22.4GB     22.4GB       49.8MB     24.9MB
      24.9MB            2012-01-19 11:30:00
      ...
-----
```

Success: Command completed successfully. (2012-01-19 12:35:06)

- See also**
- reset all-statistics
 - reset vdisk-statistics
 - [show controller-statistics](#) on page 56
 - [show disk-statistics](#) on page 59
 - [show host-port-statistics](#) on page 72
 - show vdisks
 - [show volume-statistics](#) on page 83

show volume-statistics

Description Shows live performance statistics for all or specified volumes. For each volume these statistics quantify I/O operations between hosts and the volume. For example, each time a host writes to a volume's cache, the volume's statistics are adjusted.

Properties shown only in XML API format are described in the *AssuredSAN 4000 Series CLI Reference Guide*.

Syntax `show volume-statistics [volumes]`

Parameters *volumes*

Optional. Names or serial numbers of the volumes to show information about. For volume syntax, see the *AssuredSAN 4000 Series CLI Reference Guide*. If this parameter is omitted, information is shown for all volumes.

Output Name

Volume name.

Serial Number

Volume serial number.

Bytes per second

Data transfer rate calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

IOPS

IOPS, calculated over the interval since these statistics were last requested or reset. This value will be zero if it has not been requested or reset since a controller restart.

Number of Reads

Number of read operations since these statistics were last reset or since the controller was restarted.

Number of Writes

Number of write operations since these statistics were last reset or since the controller was restarted.

Data Read

Amount of data read since these statistics were last reset or since the controller was restarted.

Data Written

Amount of data written since these statistics were last reset or since the controller was restarted.

Reset Time

Date and time, in the format *year-month-day hour:minutes:seconds*, when these statistics were last reset, either by a user or by a controller restart.

Example Show statistics for volume `vd1_v0001`:

```
# show volume-statistics vd1_v0001
Name          Serial Number  Bytes per second  IOPS  Number of Reads
  Number of Writes  Data Read  Data Written  Reset Time
-----
vd1_v0001  SN                5696.0KB           236  44091454
  60342344          1133.0GB   1378.9GB         2012-01-20 10:14:54
-----
Success: Command completed successfully. (2012-01-20 12:44:50)
```

- See also**
- reset all-statistics
 - reset volume-statistics
 - [show controller-statistics](#) on page 56
 - [show disk-statistics](#) on page 59
 - [show host-port-statistics](#) on page 72
 - [show vdisk-statistics](#) on page 79
 - show volumes

trust

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

Description Enables an offline vdisk to be brought online for emergency data recovery. This command must be enabled before each use. If used improperly this command can cause unstable operation and data loss; before use, carefully read the cautions and procedures below.

The trust command resynchronizes the time and date stamp and any other metadata on a bad disk. This makes the disk an active member of the vdisk again. You might need to do this when a vdisk is offline because a disk is failing, you have no data backup, and you want to try to recover the data from the vdisk. In this case, trust may work, but only as long as the failing disk continues to operate. Trust is only able to recover data already reconstructed on a target disk at the time the other disk failed.

When the “trusted” vdisk is back online, back up its data and audit the data to make sure that it is intact. Then delete that vdisk, create a new vdisk, and restore data from the backup to the new vdisk. Using a trusted vdisk is only a disaster-recovery measure; the vdisk has no tolerance for any additional failures.

△ **CAUTION:**

1. Do not use the trust command when the storage system is unstable; for example, if there are many power or topology-change events.
 2. The trust command cannot be run on a quarantined vdisk.
 3. Never update controller-module, expansion-module, or disk firmware when the vdisk is offline.
 4. Never clear unwritten data cache when a vdisk is offline.
 5. Do not use the trust command on a vdisk that went offline during vdisk expansion.
 6. Do not use the trust command on a vdisk with status CRIT. Instead, add spares and let the system reconstruct the vdisk.
-

Steps for running the trust command

1. Disable background scrub.
2. Identify the cause for the vdisk going offline.
3. If an external issue (power, cabling, and so forth) caused the vdisk to go offline, fix the external issue before continuing to the next step.
4. Disable host access to the offline vdisk.
 - a. Determine the owning controller of the offline vdisk.
 - b. For all online vdisks owned by that controller, change ownership to the partner controller.
 - c. Remove the host-port cables of the owning controller of the offline vdisk.

5. Note the order in which the disks failed.
6. If the disks went `LEFTOVR`/failed at different times, before running the `trust` command, physically remove all disks that were members of the vdisk that were not in use or available when the vdisk was last in the critical state. This includes disks added for reconstruction of the vdisk.
 - a. For a RAID5 vdisk, remove the first failed disk of the offline vdisk, according to the logs.
 - b. For a RAID6 vdisk, remove the first two failed disks of the offline vdisk, according to the logs.
 - c. For a RAID50 vdisk, remove the first failed disk of each failed RAID5 sub-vdisk, according to the logs.
7. If the vdisk went offline in the middle of reconstruction, remove the disk being used as the reconstruction target.
8. Unseat the spare disks associated with the vdisk to prevent reconstruction.

△ **CAUTION:** It is recommended to avoid reconstruction after using the `trust` command. Reconstruction causes heavy usage of disks that were already reporting errors. This usage could cause the disks to fail during reconstruction, which can cause data to be unrecoverable.

9. Reseat the remaining affected disks.
10. Enable the `trust` command.
11. Run the `trust` command on the vdisk.

After running the `trust` command

1. Perform a complete backup of the vdisk.
2. Delete the vdisk.
3. Replace disks, if necessary.
4. Re-create the vdisk.
5. Restore the data from the backup performed in step 1.
6. Run `verify vdisk vdisk-name fix no` to verify that the correct disk was used in the `trust` command.
7. Restore original vdisk ownership and reinsert host-port cables.
8. Re-enable background scrub.

Syntax To enable the `trust` command:

```
trust enable
```

To trust a vdisk:

```
trust vdisk vdisk
```

Parameters `enable`
Enables the `trust` command before use.

```
vdisk vdisk
```

Name or serial number of the vdisk to trust. For vdisk syntax, see Command Syntax in the *AssuredSAN 4000 Series CLI Reference Guide* or run the `help syntax` command.

Example Enable the `trust` command and then trust vdisk VD1:

```
# trust enable
Success: Command completed successfully.

# trust vdisk VD1
Success: Command completed successfully.
```

See also • [show vdisks](#)

4 Troubleshooting using event logs

Events and event messages

When an event occurs in a storage system, an event message is recorded in the system's event log and, depending on the system's event notification on settings, may also be sent to users (via email) and host-based applications (via SNMP or SMI-S).

Each event has a numeric code that identifies the type of event that occurred, and has one of the following severities:

-  **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. In this guide, this severity is abbreviated as "Info."

An event message may specify an associated error code or reason code, which provides additional detail for technical support. See [Event descriptions](#) for information about these codes.

Reviewing events

Whether viewing the events in the CLI, RAIDar, or saved log file, do the following when reviewing events:

1. For any critical, error, or warning events, click the message to view additional information and recommended actions. This information also appears in [Event descriptions](#).
Identify the primary events and any that might be the cause of the primary event. For example, an over-temperature event could cause a disk failure.
2. View the event log and locate other critical/error/warning events in the sequence for the controller that reported the event.
Repeat this step for the other controller if necessary.
3. Review the events that occurred before and after the primary event.
During this review you are looking for any events that might indicate the cause of the critical/error/warning event. You are also looking for events that resulted from the critical/error/warning event, known as secondary events.
4. Review the events following the primary and secondary events.
You are looking for any actions that might have already been taken to resolve the problems reported by the events.

Viewing the event log in the CLI

Use the `show event` command to view the event log in the CLI. The events will be listed in reverse chronological order (most recent messages are at the top of the list). See [show events](#) for more information.

If any component has a problem, the system health will be Degraded, Fault, or Unknown, and those components will be listed as Unhealthy Components. Follow the recommended actions in the component Health Recommendation field to resolve the problem. See [show events](#) for more information.

Viewing the event log in RAIDar

In the Configuration View panel, right-click the system and select **View > Event Log**. The System Events panel shows the 100 most recent events that have been logged by either controller, in reverse chronological order (most recent messages are at the top of the list). All events are logged, regardless of

event-notification settings. Click the buttons above the table to view all events, or only critical, warning, or informational events.

The event log table shows the following information:

- Severity.
 - ❌ Critical. A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.
 - ⚠️ Error. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
 - ⚠️ Warning. A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.
 - 1 Informational. A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.
- Time. Date and time when the event occurred, shown as *year-month-day hour.minutes.seconds*. Time stamps have one-second granularity.
- Event ID. An identifier for the event. The prefix A or B identifies the controller that logged the event.
- Code. An event code that helps you and support personnel diagnose problems. For event-code descriptions and recommended actions, see [Event descriptions](#).
- Message. Brief information about the event. Click the message to show or hide additional information and recommended actions.

 **NOTE:** If you are having a problem with the system or a vdisk, check the event log before calling technical support. Event messages might enable you to resolve the problem.

Saving log information to a file

To help service personnel diagnose a system problem, you might be asked to provide system log data. Using RAIDar, you can save log data to a compressed zip file. The file will contain the following data:

- Device status summary, which includes basic status and configuration data for the system
- Each controller's event log
- Each controller's debug log
- Each controller's boot log, which shows the startup sequence
- Critical error dumps from each controller, if critical errors have occurred
- CAPI traces from each controller

 **NOTE:** The controllers share one memory buffer for gathering log data and for loading firmware. Do not try to perform more than one save-logs operation at a time, or to perform a firmware-update operation while performing a save-logs operation.

To save logs

1. In the Configuration View panel, right-click the system and select **Tools > Save Logs**.
2. In the main panel:
 - a. Enter your name, email address, and phone number so support personnel will know who provided the log data.
 - b. 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 be 500 bytes long.
3. Click **Save Logs**.

 **NOTE:** In Microsoft Internet Explorer if the download is blocked by a security bar, select its **Download File** option. If the download does not succeed the first time, return to the Save Logs panel and retry the save operation.

Log data is collected, which takes several minutes.

4. When prompted to open or save the file, click **Save**.

- If you are using Firefox and have a download directory set, the file `store.zip` is saved there.
- Otherwise, you are prompted to specify the file location and name. The default file name is `store.zip`. Change the name to identify the system, controller, and date.

 **NOTE:** Because the file is compressed, you must uncompress it before you can view the files it contains. To examine diagnostic data, first view `store_yyyy_mm_dd_hh_mm_ss.logs`.

Viewing an event log saved from RAIDar

You can save event log data to a file on your network as described in [Saving log information to a file on page 88](#).

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

- SC debug-log records. Contain date/time stamps of the form `mm/dd hh:mm:ss`.
- SC crash logs (diagnostic dumps). 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.
- EC debug logs. 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.

The file lists up to 400 events for both controllers. The events are listed in chronological order; that is, the most recent event is at the bottom of a section. In the event log sections, the following information appears:

- Event ID – Event Serial Number. The prefix (A or B) indicates which controller logged the event. This corresponds to the Event Serial Number column in RAIDar.
- Date/Time – Year, month, day, and time when the event occurred.
- Code – Event code that assists service personnel when diagnosing problems. This corresponds to the Event Code column in RAIDar.
- Severity – Informational; Warning; Error; Critical. This corresponds to the Severity Level column in RAIDar.
- Message – Information about the event. This corresponds to the Message column in RAIDar.

For example:

Event SN	Date/Time	Code	Severity	Controller	Description
A29856	08-06	33	I	A	Time/date has been changed
A29809	09:35:07	65	C	A	Uncorrectable ECC error in buffer memory address 0x0 on bootup
	08-04				
	12:12:05				

5 Troubleshooting using system LEDs

Check the controller enclosure status LEDs periodically, or after you have received an error notification. If an LED is illuminated amber, the enclosure has experienced a fault or failure.

More than one LED may display a fault condition at the same time. For example, if a disk drive failed due to an exceedingly high ambient temperature, both the Temperature Fault and Fault/Service Required LEDs indicate the fault. This functionality can help you determine the cause of a fault in a FRU.

For descriptions of LED statuses, see the component diagram and table in the [System LEDs](#) section that pertains to your specific enclosure model.

Using enclosure status LEDs – front panel

Enclosure status LEDs are located on the front of the controller enclosure. See [24-disk enclosure front panel LEDs](#) on page 197 or [12-disk enclosure front panel LEDs](#) on page 198 for the enclosure front view pertaining to your model.

Normal operation

During normal operation, the FRU OK and Temperature Fault LEDs are green, and the other status LEDs are off.

Other LED behaviors

- If the FRU OK LED is off, the enclosure is not powered on.
If the enclosure should be powered on, verify that its PSUs are properly cabled to active power sources of the proper type – AC or DC – see [Connecting a power cable](#) on page 133. For unit with a power switch, verify that the two PSUs are switched on (see [Installing a PSU](#) on page 132).
- If the Fault/Service Required LED is amber, an enclosure-level fault occurred, and service action is required. See [Diagnostic steps](#) on page 94.
- If the Temperature Fault LED is amber, the enclosure temperature is above threshold.

Using disk drive module LEDs – front panel

- Disk drive module LEDs are located on the front of the controller enclosure.
- See [Disk drive LEDs](#) on page 199 for the disk drive type used by your controller enclosure model.

Normal operation

During normal operation, the OK to Remove LED is off and the Power/Activity/Fault LED is green (steady or blinking).

Other LED behaviors

- If the Power/Activity LED is off, the disk drive is not powered on.
 - If the disk drive should be powered on, verify that it is fully inserted and latched in place, and that the enclosure is powered on.
- If the Power/Activity LED is blinking green, one of the following conditions exist. See [Diagnostic steps](#) on page 94.
 - The disk drive module is initializing.
 - The disk drive module is active and processing I/O.
 - The disk drive module is performing a media scan.
 - The associated vdisk is initializing or reconstructing.
- If the Fault LED is blinking amber, the drive has been physically identified using RAIDar or the CLI.
- If the Fault LED is steady amber, one of the following conditions exist. See [Diagnostic steps](#) on page 94.
 - The disk has experienced a fault or has failed.
 - The disk is a leftover.
 - The associated vdisk is critical.

△ **CAUTION:** Do not remove a disk drive that is reconstructing. Doing so may terminate the current operation and cause data loss.

Using controller module host port LEDs – rear panel

Normal operation

- When a controller module host port is connected to a data host, the port's host Link Status LED and host Link Activity LEDs are green.
- If there is I/O activity, the host Activity LED blinks green.
- See the host port LED descriptions pertaining to your controller enclosure model(s) in [System LEDs](#) for more information.

Other LED behaviors

- If hosts are having trouble accessing the storage system, check the following:
In RAIDar's Configuration View panel, right-click on the system, and select **Configuration > System Settings > Host Interfaces**. Verify the settings and modify them if necessary.
- If a connected host port's link status LED is off, the link is down.
 - In RAIDar, select **View > Event Log**. The System Events table displays. Review the event logs for indicators of a specific fault in a host data path component.
 - If you cannot locate a specific fault, or you cannot access the event logs, see [Diagnostic steps](#) on page 94 to isolate the fault.
- For further troubleshooting, see [Isolating a host-side connection fault on page 98](#).

Using the controller module expansion port status LED – rear panel

Normal operation

When a controller module's expansion port is connected to another enclosure, the expansion port status LED is green. See the Expansion Port Status LED description pertaining to your enclosure model in [System LEDs](#) for more information.

Other LED behaviors

- If the connected port's LED is off, the link is down.
 - In RAIDar, select **View > Event Log**. The System Events table displays. Review the event logs for indicators of a specific fault.
 - If you cannot locate a specific fault, or you cannot access the event logs, see [Diagnostic steps](#) on page 94 to isolate the fault.
- For further troubleshooting, see [Isolating a controller module expansion port connection fault on page 100](#).

Using controller module network port LEDs – rear panel

Normal operation

- When a controller module's network port is connected, its Ethernet Link Status LED is green.
- If there is I/O activity, the Ethernet Activity LED blinks green. See the Network Port LED descriptions pertaining to your enclosure model in [System LEDs](#) for more information.

Other LED behaviors

If a connected port's Ethernet Link Status LED is off, the link is down. Use standard networking troubleshooting procedures to isolate faults on the network.

Using controller module status LEDs – rear panel

Normal operation

- The FRU OK LED is green; the Cache Status LED can be green, blinking, or off; and the other controller module status LEDs (Unit Locator, OK to Remove, Fault/Service Required) are off.
- See the OK to Remove, Unit Locator, FRU OK, Fault/Service Required, and Cache Status LED descriptions pertaining to your enclosure model in [System LEDs](#) for more information.

Other LED behaviors

- If the FRU OK LED is off, either:
 - The controller module is not powered on. If it should be powered on, verify that it is fully inserted and latched in place, and that the controller enclosure is powered on.
 - The controller module has failed. In RAIDar, select **View > Event Log**. The System Events table displays. Review the event logs for indicators of a specific fault.
- If the Cache Status LED is blinking green, a CompactFlash flush or cache self-refresh is in progress, indicating cache activity. No action is required. (See also [Diagnostic steps](#) on page 94).
 - If the LED is blinking evenly, a cache flush is in progress. When a controller module loses power and write cache is dirty (contains data that has not been written to disk), the supercapacitor pack provides backup power to flush (copy) data from write cache to CompactFlash memory. When cache flush is complete, the cache transitions into self-refresh mode.
 - If the LED is blinking momentarily slowly, the cache is in a self-refresh mode. In self-refresh mode, if primary power is restored before the backup power is depleted (3 – 30 minutes, depending on various factors), the system boots, finds data preserved in cache, and writes it to disk. This means the system can be operational within 30 seconds, and before the typical host I/O time-out of 60 seconds, at which point system failure would cause host-application failure. If primary power is restored after the backup power is depleted, the system boots and restores data to cache from CompactFlash, which can take about 90 seconds.

CAUTION: If the Cache Status LED is solid green, the controller should be shut-down from the user interface so unwritten data can be flushed to the CompactFlash.

NOTE: The cache flush and self-refresh mechanism is an important data protection feature; essentially four copies of user data are preserved: one in each controller's cache and one in each controller's CompactFlash.

- If the Fault/Service Required LED is steady amber, a fault occurred or a service action is required. See [Diagnostic steps](#) on page 94.
- If the Fault/Service Required LED is blinking amber, one of the following errors occurred. See [Diagnostic steps](#) on page 94.
 - Hardware-controlled power up error
 - Cache flush error
 - Cache self-refresh error
- If the OK to Remove LED is blue, the controller module is prepared for removal.
- If the controller has failed or does not start, see [Diagnostic steps](#) on page 94.

Using PSU LEDs – rear panel

Normal operation

- The Input Source Power Good LED is green.
- See [PSU LEDs](#) on page 204 for PSU descriptions, and refer to the PSU (AC or DC) included with your controller enclosure.

Other LED behaviors

- If the AC Power Good LED is off, the module is not receiving adequate power. Verify that the power cable is properly connected, and check the power source it is connected to (see [Connecting a power cable](#) on page 133).
- If the DC Voltage/Fan Fault/Service Required LED is amber, either the PSU or a fan is operating at an unacceptable voltage or r/min level, or has failed. When isolating faults in a PSU, remember that the fans in both modules receive power through a common bus on the midplane, so if a PSU fails, the fans continue to operate normally.

Using expansion module LEDs – rear panel

Normal operation

- When the expansion module is connected to a controller module or host, the SAS In port status LED is green.
- If the SAS Out port is connected to another module, the SAS Out port status LED is also green.
- The FRU OK LED is green and the other expansion module status LEDs (Unit Locator, OK to Remove, Fault/Service Required) are off.
- See the LED descriptions pertaining to your enclosure model(s) in [System LEDs](#) for more information.

Other LED behaviors

- If a connected port's status LED is off, the link is down. In RAIDar, select **View > Event Log**. The System Events table displays. Review the event logs for indicators of a specific fault in a host data path component.
- If the FRU OK LED is off, one of the following conditions exists. See [Is the controller rear panel "FRU OK" LED lit?](#) on page 95.
 - The expansion module is not powered on. If it should be powered on, verify that it is fully inserted and latched in place, and that the enclosure is powered on.
 - The expansion module has failed. In RAIDar, select **View > Event Log**. The System Events table displays. Review the event logs for indicators of a specific fault.
- If the Fault/Service Required LED is steady amber, a fault occurred or a service action is required. See [Is the controller rear panel "Fault/Service Required" LED amber?](#) on page 95.
- If the Fault/Service Required LED is blinking amber, one of the following errors occurred.
 - Hardware-controlled power up error.
 - Cache flush error.
 - Cache self-refresh error.See [Is the controller rear panel "Fault/Service Required" LED amber?](#) on page 95.
- If the OK to Remove LED is blue, the controller module is prepared for removal.

Diagnostic steps

This section describes possible reasons and actions to take when an LED indicates a fault condition during initial system setup.

As previously discussed, in addition to monitoring LEDs via line-of-sight observation of the racked hardware components when performing diagnostic steps, you can also monitor the health of the system and its components using management interfaces. Bear this in mind when reviewing the Actions column in the following diagnostics tables, and when reviewing the step procedures provided later in this chapter.

Is the enclosure front panel “Fault/Service Required” LED amber?

Table 7 Diagnostic LED status: Front panel “Fault/Service Required”

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	A fault condition exists/occurred. If installing an IOM FRU, the module has gone online and likely failed its self-test.	<ul style="list-style-type: none"> Check the LEDs on the rear of the controller to narrow the fault to a FRU, connection, or both. Check the event log for specific information regarding the fault; follow any Recommended Actions. If installing an IOM FRU, try removing and reinstalling the new IOM, and check the event log for errors. If the above actions do not resolve the fault, isolate the fault and contact an authorized service provider for assistance. Replacement may be necessary.

Is the controller rear panel “FRU OK” LED lit?

Table 8 Diagnostic LED status: Rear panel “FRU OK”

Answer	Possible reasons	Actions
Yes (blinking)	System functioning properly. System is booting.	No action required. Wait for system to boot.
No	The controller module is not powered on. The controller module has failed.	<ul style="list-style-type: none"> Check that the controller module is fully inserted and latched in place, and that the enclosure is powered on. Check the event log for specific information regarding the failure.

Is the controller rear panel “Fault/Service Required” LED amber?

Table 9 Diagnostic LED status: Rear panel “Fault/Service Required”

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes (blinking)	One of the following errors occurred: <ul style="list-style-type: none"> Hardware-controlled power-up error Cache flush error Cache self-refresh error 	<ul style="list-style-type: none"> Restart this controller from the other controller using RAIDar or the CLI. If the above action does not resolve the fault, remove the controller and reinsert it. If the above action does not resolve the fault, contact an authorized service provider for assistance. It may be necessary to replace the controller.

Are both disk drive module LEDs off?

Table 10 Diagnostic LED status: Disk drive module

Answer	Possible reasons	Actions
Yes	<ul style="list-style-type: none"> There is no power The disk is offline 	Check that the disk is fully inserted and latched in place, and that the enclosure is powered on.

Is the disk drive module “Fault” LED amber?

Table 11 Diagnostic LED status: Disk drive “Fault” LED (LFF and SFF modules)

Answer	Possible reasons	Actions
Yes, and the online/activity LED is off .	The disk is offline. An event message may have been received for this device.	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance.
Yes, and the online/activity LED is blinking .	The disk has been identified using RAIDar or the CLI.	Clear the locator LED using either RAIDar or the CLI. <ul style="list-style-type: none"> • In the CLI, use the <code>set led</code> command. • In RAIDar, select another component or sign out using the Sign Out screen near the top of the RAIDar window. Do not close the browser window without signing out. Doing so will cause the LED to remain lit.
	The disk is active, but an event message may have been received for this device.	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance.

Is a connected host port’s “Host Link Status” LED lit?

Table 12 Diagnostic LED status: Rear panel “Host Link Status”

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The link is down.	See also Isolating a host-side connection fault on page 98 . <ul style="list-style-type: none"> • Check cable connections and reset if necessary. • If the above action does not resolve the fault, inspect cable for damage. Replace cable if necessary • If the above action does not resolve the fault, swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. • If the above action does not resolve the fault, verify that the switch, if any, is operating properly. If possible, test with another port. • If the above action does not resolve the fault, verify that the HBA is fully seated, and that the PCI slot is powered on and operational. • If the above action does not resolve the fault, review event logs for indicators of a specific fault in a host data path component. • If the above action does not resolve the fault, contact an authorized service provider for assistance.

Is a connected port's "Expansion Port Status" LED lit?

Table 13 Diagnostic LED status: Rear panel "Expansion Port Status"

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The link is down.	<p>See also Using controller module network port LEDs – rear panel on page 92.</p> <ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • If the above action does not resolve the fault, inspect cable for damage. Replace cable if necessary • If the above action does not resolve the fault, swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. • If the above action does not resolve the fault, verify that the switch, if any, is operating properly. If possible, test with another port. • If the above action does not resolve the fault, verify that the HBA is fully seated, and that the PCI slot is powered on and operational. • If the above action does not resolve the fault, review event logs for indicators of a specific fault in a host data path component. • If the above action does not resolve the fault, contact an authorized service provider for assistance.

Is a connected port's "Network Port Link Status" LED lit?

Table 14 Diagnostic LED status: Rear panel "Network Port Link Status"

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The link is down.	<ul style="list-style-type: none"> • Swap cables between the A and B controllers to isolate the fault. • Use standard networking troubleshooting procedures to isolate faults on the network.

Is the PSU's "Input Power Source" LED lit?

Table 15 Diagnostic LED status: Rear panel PSU "Input Power Source"

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The PSU is not receiving adequate power.	<ul style="list-style-type: none"> • Verify that the power cord is properly connected, and check the power source to which it connects. • If the above action does not resolve the fault, check that the PSU FRU is firmly locked into position. • If the above action does not resolve the fault, check the event log for specific information regarding the fault. • If the above action does not resolve the fault, isolate the fault and contact an authorized service provider for assistance.

Is the “Voltage/Fan Fault/Service Required” LED amber?

Table 16 Diagnostic LED status: Rear panel PSU “Voltage/Fan Fault/Service Required”

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The PSU or a fan is operating at an unacceptable voltage or r/min level, or has failed.	<p>When isolating faults in the PSU, remember that the fans in both modules receive power through a common bus on the midplane, so if a PSU fails, the fans continue to operate normally.</p> <ul style="list-style-type: none">• Verify that the PSU FRU is firmly locked into position.• If the above action does not resolve the fault, verify that the power cable is connected to a power source.• If the above action does not resolve the fault, verify that the power cable is connected to the enclosure’s PSU.• If the above action does not resolve the fault, FRU replacement may be necessary; see Troubleshooting and replacing FRUs.

Isolating a host-side connection fault

During normal operation, when a controller module host port is connected to a data host, the port’s host link status LED and host link activity LED are green. If there is I/O activity, the host activity LED blinks green. If data hosts are having trouble accessing the storage system, and you cannot locate a specific fault or cannot access the event logs, use the following procedure.

This procedure requires scheduled downtime.

 **IMPORTANT:** Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

Host-side connection troubleshooting featuring FC host ports

The procedure below pertains to AssuredSAN 4000 Series controller enclosures employing SFP transceiver connectors in 2/4/8 Gbit FC host interface ports.

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 106).
2. Check the host activity LED.

If there is activity, halt all applications that access the storage system.

3. Check the Cache Status LED to verify that the controller’s cached data is flushed to the disk drives.
 - Solid – Cache is dirty (contains unwritten data) and is not writing to disk.
 - Blinking – Data is still being written to disk.
 - Off – Cache is clean (no unwritten data).
4. Inspect the cable for damage.
5. Reseat the SFP and host cable.

Is the host link status LED on?

- Yes – Monitor the status to ensure that there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
- No – Proceed to the next step.

6. Move the SFP and host cable to a port with a known good link status.
This step isolates the problem to the external data path (SFP, host cable, and host-side devices) or to the controller module port.
Is the host link status LED on?
 - Yes – You now know that the SFP, host cable, and host-side devices are functioning properly. Return the SFP and cable to the original port. If the link status LED remains off, you have isolated the fault to the controller module's port. Replace the controller module.
 - No – Proceed to the next step.
7. Swap the SFP with a known good one.
Is the host link status LED on?
 - Yes – You have isolated the fault to the SFP. Replace the SFP.
 - No – Proceed to the next step.
8. Re-insert the original SFP and swap the cable with a known good one.
Is the host link status LED on?
 - Yes – You have isolated the fault to the cable. Replace the cable.
 - No – Proceed to the next step.
9. Verify that the switch, if any, is operating properly. If possible, test with another port.
10. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
11. Replace the HBA with a known good HBA, or move the host side cable and SFP to a known good HBA.
Is the host link status LED on?
 - Yes – You have isolated the fault to the HBA. Replace the HBA.
 - No – It is likely that the controller module needs to be replaced.
12. Move the cable and SFP back to its original port.
Is the host link status LED on?
 - No – The controller module's port has failed. Replace the controller module.
 - Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with SFPs, damaged cables, and HBAs.

Host-side connection troubleshooting featuring SAS host ports

The procedure below applies to AssuredSAN 4000 Series controller enclosures configured with 6 Gbit SFF miniSAS host interface ports.

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 106).
2. Check the host activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller's cached data is flushed to the disk drives.
 - Solid – Cache is dirty (contains unwritten data) and is not writing to disk.
 - Blinking – Data is still being written to disk.
 - Off – Cache is clean (no unwritten data).
4. Inspect the cable for damage.
5. Reseat the cable.
Is the host link status LED on?
 - Yes – Monitor the status to ensure that there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.

6. Move the cable to a port with a known good link status.

This step isolates the problem to the external data path (host cable and host-side devices) or to the controller module port.

Is the host link status LED on?

- Yes – You now know that the host cable and host-side devices are functioning properly. Return the cable to the original port. If the link status LED remains off, you have isolated the fault to the controller module's port. Replace the controller module.
- No – Proceed to the next step.

7. Verify that the switch, if any, is operating properly. If possible, test with another port.

8. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.

9. Replace the HBA with a known good HBA, or move the host side cable to a known good HBA.

Is the host link status LED on?

- Yes – You have isolated the fault to the HBA. Replace the HBA.
- No – It is likely that the controller module needs to be replaced.

10. Move the cable back to its original port.

Is the host link status LED on?

- No – The controller module's port has failed. Replace the controller module.
- Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with damaged cables and HBAs.

Isolating a controller module expansion port connection fault

During normal operation, when a controller module's expansion port is connected to a drive enclosure, the expansion port status LED is green. If the connected port's expansion port LED is off, the link is down. Use the following procedure to isolate the fault.

This procedure requires scheduled downtime.

 **NOTE:** Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 106).

2. Check the host activity LED.

If there is activity, halt all applications that access the storage system.

3. Check the Cache Status LED to verify that the controller's cached data is flushed to the disk drives.

- Solid – Cache is dirty (contains unwritten data) and is not writing to disk.
- Blinking – Data is still being written to disk.
- Off – Cache is clean (no unwritten data).

4. Reseat the expansion cable, and inspect it for damage.

Is the expansion port status LED on?

- Yes – Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
- No – Proceed to the next step.

5. Move the expansion cable to a port on the controller enclosure with a known good link status.

This step isolates the problem to the expansion cable or to the controller module's expansion port.

Is the expansion port status LED on?

- Yes – You now know that the expansion cable is good. Return the cable to the original port. If the expansion port status LED remains off, you have isolated the fault to the controller module's expansion port. Replace the controller module.
- No – Proceed to the next step.

6. Move the expansion cable back to the original port on the controller enclosure.

7. Move the expansion cable on the drive enclosure to a known good expansion port on the drive enclosure.

Is the expansion port status LED on?

- Yes – You have isolated the problem to the drive enclosure's port. Replace the expansion module.
- No – Proceed to the next step.

8. Replace the cable with a known good cable, ensuring the cable is attached to the original ports used by the previous cable.

Is the host link status LED on?

- Yes – Replace the original cable. The fault has been isolated.
- No – It is likely that the controller module must be replaced.

6 Troubleshooting and replacing FRUs

This chapter provides procedures for replacing FRUs, including precautions, removal instructions, installation instructions, and verification of successful installation. Each procedure addresses a specific task. Certain procedures refer to related documentation. See [Available FRUs](#) for figures and lists of FRUs.

ESD

Before you begin *any* of the procedures, consider the following precautions and preventive measures.

Preventing ESD

To prevent ESD from damaging the system, be aware of the precautions to consider when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

△ **CAUTION:** Parts can be damaged by ESD. Follow these precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
 - Keep electrostatic-sensitive parts in their containers until they arrive at static-protected workstations.
 - Place parts in a static-protected area before removing them from their containers.
 - Avoid touching pins, leads, or circuitry.
 - Always be properly grounded when touching a static-sensitive component or assembly.
 - Remove clutter (plastic, vinyl, foam) from the static-protected workstation.
-

Grounding methods to prevent ESD

Several methods are used for grounding. Adhere to the following precautions when handling or installing electrostatic-sensitive parts.

△ **CAUTION:** Parts can be damaged by ESD. Use proper anti-static protection:

- Keep the replacement FRU in the ESD bag until needed; and when removing a FRU from the enclosure, immediately place it in the ESD bag and anti-static packaging.
 - Wear an ESD wrist strap connected by a ground cord to a grounded workstation or unpainted surface of the computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm (± 10 percent) resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
 - If an ESD wrist strap is unavailable, touch an unpainted surface of the chassis before handling the component.
 - Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
 - Use conductive field service tools.
 - Use a portable field service kit with a folding static-dissipating work mat.
-

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information on static electricity or assistance with product installation, contact an authorized reseller.

Replacing chassis FRU components

The chassis FRU replaces a damaged chassis or chassis components. A fully functional chassis requires successful installation of the following components:

- One or two controller modules of the same model (for a given controller enclosure)*
See [Replacing a controller module or expansion module](#) on page 104 for more information.
- All disk drives and air management modules
See [Replacing a disk drive module](#) on page 121 for more information.
- Two PSUs of the same type (AC or DC)
See [Replacing a PSU](#) on page 128 for more information.
- Two ear bezels (complementary left and right ear kits)
See [Replacing ear bezels](#) on page 135 for more information.

 **NOTE:** Some product models use an enclosure bezel instead of ear covers. If your model is equipped with a bezel instead of ear covers, see the enclosure bezel kit installation document provided in your product's ship kit.

- See [Figure 33](#) on page 210 for 2U24 enclosure bezel alignment.
- See [Figure 38](#) on page 213 for 2U12 enclosure bezel alignment.

-
- One or two expansion modules of the same model (per optional drive enclosure)*
[Replacing a controller enclosure chassis](#) on page 139 for more information.

*For enclosures equipped with a single IOM, the lower IOM slot within the chassis is empty, and must be covered with an IOM blank to allow optimum airflow through the enclosure during operation.

In addition to the FRUs identified above, replacement procedures are provided to address specific interface protocols and replacement of the enclosure chassis:

- Removal and installation of an FC transceiver
See [Replacing an FC transceiver](#) on page 137 for more information.
- Removal and installation of a controller enclosure chassis
See [Replacing a controller enclosure chassis](#) on page 139 for more information.

 **NOTE:** AssuredSAN 4000 Series controller enclosures support hot-plug replacement of redundant controller modules, fans, power supplies, and IOMs. Hot-add of drive enclosures is also supported. The term "hot" means components can be replaced, swapped, or added without halting I/O to the vdisks or powering off the enclosure.

 **TIP:** Many procedures refer to component LEDs and LED status. See [System LEDs](#) for descriptions of model-specific front panel and rear panel LEDs.

Replacing a controller module or expansion module

Controller and expansion modules are hot-swappable, which means you can replace one module without halting I/O to vdisks, or powering off the enclosure. In this case, the second module takes over operation of the storage system until you install the new module.

 **IMPORTANT:** When swapping controllers in the same enclosure, special precautions must be taken to ensure the vdisks do not enter quarantine status. See [Swapping controllers in the same enclosure](#) on page 110.

You may need to replace a controller or expansion module when:

- The Fault/Service Required LED is illuminated
- Events in RAIDar indicate a problem with the module
- Troubleshooting indicates a problem with the module

Before you begin

Removing a controller or expansion module from an operational enclosure significantly changes air flow within the enclosure. Openings must be populated for the enclosure to cool properly. Leave modules in the enclosure until ready to install a replacement. If you are replacing both controllers use RAIDar to record configuration settings before installing the new controller modules. See [Removing a controller module](#) on page 108, and [Installing a controller module or expansion module](#) on page 108 for instructions on installing an additional controller module.

△ CAUTION: When replacing a controller module, ensure that less than 10 seconds elapse between inserting it into a slot and fully latching it in place. Failing to do so might cause the controller to fail. If it is not latched within 10 seconds, remove the controller module from the slot, and repeat the process.

Configuring PFU

If PFU is enabled, when you update firmware on one controller, the system automatically updates the partner controller. Disable PFU only if requested by a service technician.

Use RAIDar or the CLI to change the PFU setting.

Using RAIDar

1. Sign-in to RAIDar using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Firmware**.
3. Select (enable) the **Partner Firmware Upgrade** option.
4. Click **Apply**.

 **NOTE:** See the *AssuredSAN 4000 Series RAIDar User Guide* for additional information.

Using the CLI

1. Log-in to the CLI using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. To verify that PFU is enabled, run the following command:

```
show advanced-settings
```
3. If PFU is disabled, enable it by running the following command:

```
set advanced-settings partner-firmware-upgrade enabled
```

 **NOTE:** See *AssuredSAN 4000 Series CLI Reference Guide* for additional information.

Verifying component failure

Select from the following methods to verify component failure:

- Use RAIDar to check the health icons/values of the system and its components to either ensure that everything is okay, or to drill down to a problem component. RAIDar uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. If you discover a problem component, follow the actions in its Health Recommendations field to resolve the problem.
- As an alternative to using RAIDar, you can run the `show system` command in the CLI to view the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. If you discover a problem component, follow the actions in its Health Recommendations field to resolve the problem.
- Monitor event notification — With event notification configured and enabled, use RAIDar to view the event log, or use the CLI to run the `show events detail` command to see details for events.
- Check Fault/Service Required LED (rear of enclosure). If the LED is amber, a fault condition exists.
- Check that the FRU OK LED (rear of enclosure) is off.

Stopping I/O

When troubleshooting drive and connectivity faults, ensure you have a current full backup of the data. As an additional data protection precaution, stop all I/O to the affected vdisks.

 **IMPORTANT:** Stopping I/O to a vdisk is a host-side task, and falls outside the scope of this document.

You can verify that there is no I/O activity by briefly monitoring the system LEDs; however, when accessing the storage system remotely, this is not possible. To determine if input and output has stopped, perform the steps below:

1. Using the CLI, run the `show vdisk-statistics` command.
The `Number of Reads` and `Number of Writes` outputs show the number of these operations that have occurred since the statistic was last requested. Record the numbers displayed.
2. Run the `show vdisk-statistics` command a second time.
This provides you a specific window of time (the interval between requesting the statistics) to determine if data is being written to or read from the disk. Record the numbers displayed.
3. To determine if any reads or writes occur during this interval, subtract the set of numbers you recorded in [step 1](#) from the numbers you recorded in [step 2](#).
 - If the resulting difference is zero, I/O has stopped.
 - If the resulting difference is not zero, a host is still reading from or writing to this vdisk. Continue to stop IOPS from hosts, and repeat [step 1](#) and [step 2](#) until the difference in [step 3](#) is zero.

 **NOTE:** See *AssuredSAN 4000 Series CLI Reference Guide* for additional information.

Shutting down a controller module

Shutting down the SC in a controller module ensures that a proper failover sequence is used, which includes stopping all I/O operations and writing any data in write cache to disk. If the SC in both controller modules is shut down, hosts cannot access the system's data. Perform a shut down before removing a controller module or powering down the system.

 **CAUTION:** You can continue to use the CLI when either or both SCs are shut down, but information shown might be invalid.

Use RAIDar or the CLI to perform a shut down.

Using RAIDar

1. Sign-in to RAIDar using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. In the Configuration View panel, right-click the system and select **Tools > Shut Down or Restart Controller**.
3. In the main panel, set the options:
 - In the Operation field, select **Shut down**.
 - In the Controller type field, select **Storage**.
 - In the Controller field, select whether to shut down the processor in controller A, B, or both.
4. Click **Shut down now**. A confirmation dialog appears.
5. Click **Yes** to continue; otherwise click **No**. If you click Yes, a second confirmation dialog appears.
6. Click **Yes** to continue; otherwise click **No**. If you click Yes, a message describes shutdown activity.

 **NOTE:** See the *AssuredSAN 4000 Series RAIDar User Guide* for additional information.

Using the CLI

1. Log-in to the CLI using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. Verify that the partner controller is online by running the `show redundancy-mode` command.
3. Shut down the failed controller — A or B — by running the `shutdown a` or `shutdown b` command.
The blue OK to Remove LED (rear of enclosure) illuminates to indicate that the controller module can be safely removed.
4. Illuminate the ID LED of the enclosure that contains the controller module to remove by running the `set led enclosure 0 on` command.

 **NOTE:** See the *AssuredSAN 4000 Series CLI Reference Guide* for additional information.

Removing a controller module or expansion module

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

 **IMPORTANT:** You may hot-replace a controller module in an operational enclosure, provided you first shut down the faulty controller using either RAIDar or the CLI.

 **NOTE:** Within these procedures, illustrations featuring controller module face plates are generic. They do not show host ports, and they pertain to all 4000 Series controller module models. For illustrations of model-specific controller face plates, see the *AssuredSAN 4000 Series Setup Guide*.

1. Verify that you have successfully shut down the controller module using RAIDar or the CLI. See [Stopping I/O](#) on page 106.
2. Locate the enclosure whose Unit Locator LED (front right ear) is illuminated, and within the enclosure, locate the controller module whose OK to Remove LED is blue (rear panel).
3. Disconnect any cables connected to the controller.
Label each cable to facilitate re-connection.
4. Turn the thumbscrews counterclockwise until they disengage from the controller (see [Figure 1](#)).

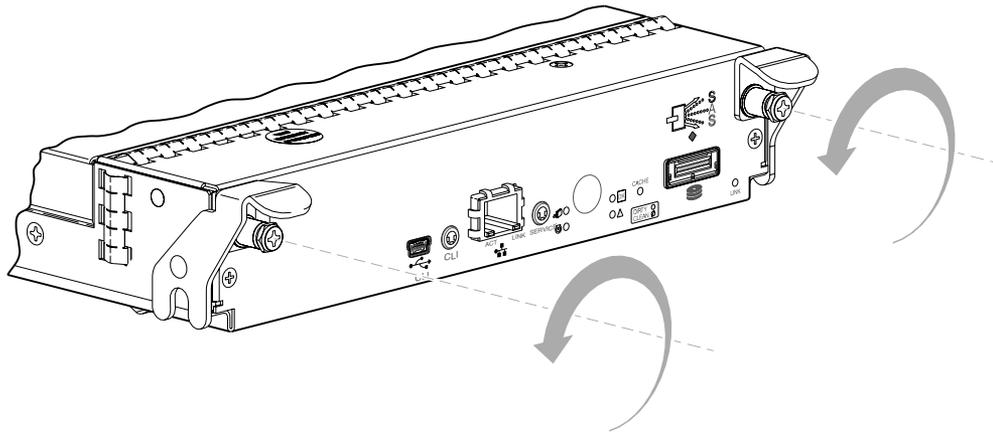


Figure 1 Disengaging a controller module

5. Press both latches downward to disconnect the controller module from the midplane (see [Figure 2](#)).

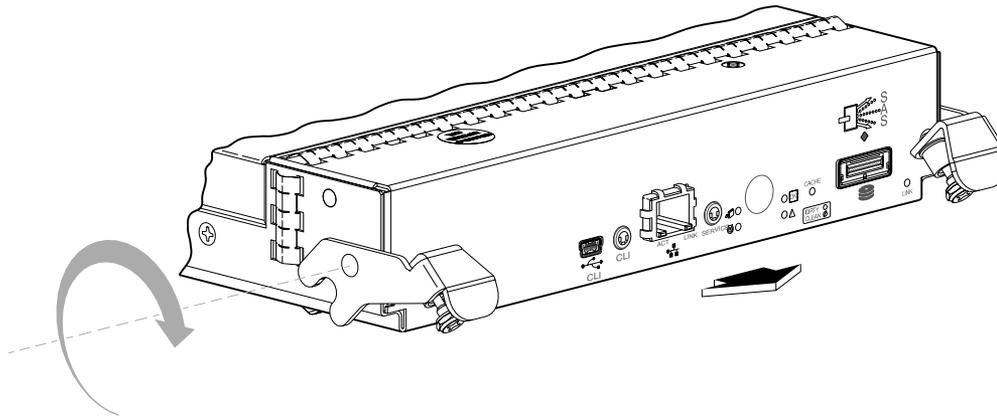


Figure 2 Disconnecting a controller module

6. Pull the controller module straight out of the enclosure (see [Figure 3](#)).

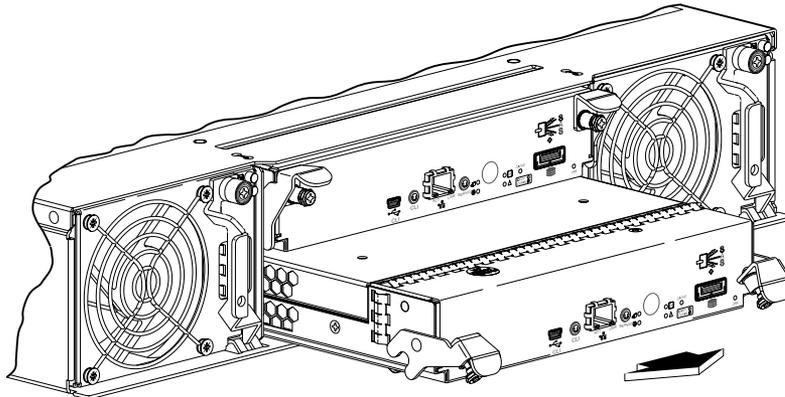


Figure 3 Removing a controller module

Installing a controller module or expansion module

TIP: You can install a controller module into an enclosure that is powered on, provided you wait 60 seconds after removing the old controller module. Check controller and midplane power connectors before inserting the new controller module into the enclosure.

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

1. Loosen the thumbscrews; press the latches downward (see [Figure 4](#)).

2. Slide the controller module into the enclosure as far as it will go (1).

A controller module that is only partially-seated will prevent optimal performance of the controller enclosure. Verify that the controller module is fully-seated before continuing.

3. Press the latches upward to engage the controller module (2); turn the thumbscrews clockwise until finger-tight.

4. Reconnect the cables.

 **NOTE:** See the *AssuredSAN 4000 Series Setup Guide* for cabling information.

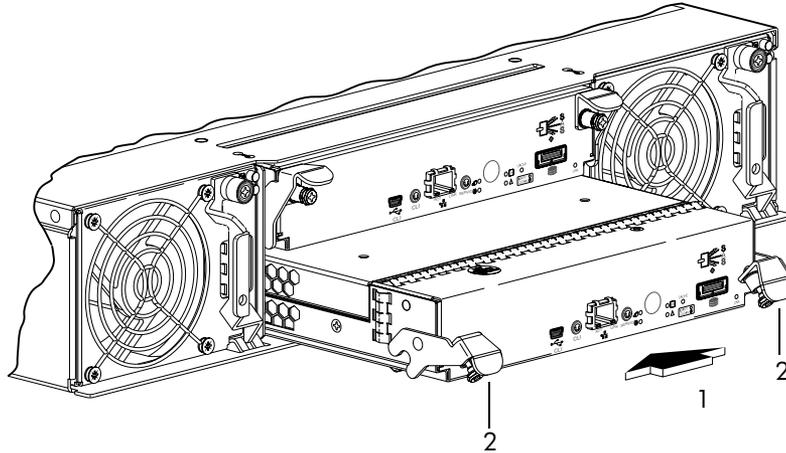


Figure 4 Inserting a controller module

 **IMPORTANT:** If PFU is enabled, when you update firmware on one controller, the system automatically updates the partner controller. Do not power off the system during a firmware upgrade. Doing so might cause irreparable damage to the controllers.

Fault/Service Required LED error status

If the Fault/Service Required LED is illuminated amber, the IOM is not online, and likely failed its self-test. See [Shutting down a controller module](#) on page 106 to try to successfully restart the IOM and bring it online. Also, check the event log for errors.

Boot handshake error

If a boot handshake error occurs during IOM power on, power off the enclosure for two seconds, and then power it on again. If this action does not correct the error, see [Removing a controller module or expansion module on page 107](#), and follow the procedure provided.

Setting the internal clock

When the serviced controller module is reinserted into the enclosure, the controller's date and time are automatically updated to match the date and time of the partner controller.

To set the clock using the CLI, run the `set controller-date` command.

Persistent IP address

The IP address for each controller is stored in a EEPROM on the midplane. The IP address is persistent. When you replace a controller module, the new controller will have the same IP address as the old controller.

Verifying component operation

After replacing the controller module, verify that the FRU OK LED (rear panel) illuminates green, indicating that the controller has completed initializing, and is online/operating normally. It may take two to five minutes for the replacement controller to become ready. If you are replacing either controller module, and PFU is enabled, you may need to wait 30 minutes to ensure that the two controllers — with their respective ownership of the vdisks — have enough time to fully stabilize.

Use RAIDar or the CLI to perform a restart only if necessary.

Using RAIDar

1. Sign-in to RAIDar using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. In the Configuration View panel, right-click the system and select **Tools > Shut Down or Restart Controller**.
3. In the main panel, set the options:
 - In the Operation field, select **Restart**.
 - In the Controller type field, select **Storage**.
 - In the Controller field, select whether to restart the processor in controller A, B, or both.
4. Click **Restart now**. A confirmation dialog appears.
5. Click **Yes** to continue; otherwise click **No**. If you click Yes, a second confirmation dialog appears.
6. Click **Yes** to continue; otherwise click **No**. If you click Yes, a message describes restart activity.

Using the CLI

1. Sign-in to the CLI using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. View the enclosure LEDs.
 - If the enclosure's Unit Locator LED is on, run the `set led enclosure 0 off` command to turn it off.
 - If the Fault/Service Required LED is amber, the controller module has not gone online, and likely failed its self-test. Put the module online by restarting the controller, or by checking the event log for errors.

To restart the controller (A or B), run the `restart sc a` or `restart sc b` command.

 **TIP:** See [System LEDs](#) on page 197 for descriptions of model-specific LEDs.

Swapping controllers in the same enclosure

When swapping controllers in the same enclosure, special precautions must be taken to ensure the vdisks do not enter quarantine offline status. See [Quarantined vdisks](#) on page 111 for more information.

To ensure the cache is clean and data integrity is maintained, perform the following steps:

1. Check for unwritable cache data.
 - If unwritable cache data is found, and the unwritable cache data is for a volume that has been deleted, use the CLI `clear cache` command to clear the unwritable cache data from the system. See [clear cache](#) on page 38 for information on using this command.
 - If the unwritable cache data is for a volume that is offline for other reasons, do not clear the unwritable cache data and do not proceed with the controller swap. Determine the cause for the presences of the unwritable cache data and resolve the issue before performing the controller swap.
2. Perform a shutdown of both controllers. See [Shutting down a controller module](#) on page 106.

Quarantined vdisks

When unwritable cache data is present or if a clean shutdown of both controllers is not performed, vdisks will be quarantined offline (QTOF) and event 485 will be logged for each affected vdisk. Data integrity is not guaranteed.

The vdisks can be dequarantined by shutting down and rebooting each controller separately. This ensures a proper failover sequence is followed. See [Shutting down a controller module](#) on page 106 for instructions.

Updating firmware

You can view the current versions of firmware in controller modules, expansion modules (in drive enclosures), and disks, and you can also install new firmware versions.

 **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 hosts 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.

A controller enclosure can contain one or two controller modules. Both controllers should 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 the PFU option is enabled, when you update one controller, the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller, you must log into the partner controller's IP address and perform the firmware update on that controller also.

 **NOTE:** If a vdisk is quarantined, firmware update is not permitted due to the risk of losing unwritten data that remains in cache for the vdisk volumes. Before you can update firmware, you must resolve the problem that is causing the vdisk to be quarantined, as described in the "Removing a vdisk from quarantine" topic in the *AssuredSAN 4000 Series RAIDar User Guide* or online help.

For best results, the storage system should be in a healthy state before starting firmware update.

Updating controller module firmware using RAIDar

A controller enclosure can contain one or two controller modules. Both controllers should 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 the PFU option is enabled, when you update one controller the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

 **NOTE:** For information about supported releases for firmware update, see the *AssuredSAN 4000 Series Release Notes*.

To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. Restart the MC in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers. For the procedure, see [Shutting down a controller module](#) on page 106.
3. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Controller Versions shows the currently installed versions.

4. Click **Browse** and select the firmware file to install.
5. Click **Install Controller-Module Firmware File**. A dialog box shows firmware-update progress.

The process starts by validating the firmware file:

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

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

Firmware update typically takes 10 minutes for a controller with current CPLD firmware, or 20 minutes for a controller with downlevel CPLD firmware. If the controller enclosure has attached enclosures, allow additional time for each expansion module's EMP to be updated. This typically takes 3 minutes for each EMP in a drive enclosure.

If the SC 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 controller will restart. Until the restart is complete, the RAIDar Sign In page will say that the system is currently unavailable. When this message is cleared, you may sign in.

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

6. Clear your web browser's cache, then sign in to RAIDar. If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

📄 **NOTE:** After firmware update has completed on both controllers, if the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

Updating controller module firmware using FTP

A controller enclosure contains two controller modules. Both controllers should 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 the PFU option is enabled, when you update one controller the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

📄 **NOTE:** For information about supported releases for firmware update, see the *AssuredSAN 4000 Series Release Notes*.

To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. In RAIDar, 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. Restart the MC in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers. For the procedure, see [Shutting down a controller module](#) on page 106.
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 CF100R01-01.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 attached drive enclosures, allow additional time for each EMP to be updated. This typically takes 3 minutes for an EMP in each drive enclosure.

NOTE: If you are using a Windows FTP client, during firmware update a client-side FTP application issue can cause the FTP session to be aborted. If this issue persists try using RAIDar to perform the update, use another client, or use another FTP application.

If the SC 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 RAIDar. If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

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

Updating expansion module firmware using RAIDar

A drive enclosure contains two expansion modules. Each expansion module contains an 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.

 **IMPORTANT:** Disable PFU before attempting to update the firmware. If PFU is not disabled, it will downgrade the firmware on the corresponding expansion module. If this occurs, restart each SC.

To update expansion-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Versions of All Expansion Modules (EMPs) shows the currently installed versions.
3. Select the expansion modules to update.
4. Click **Browse** and select the firmware file to install.
5. Click **Install Expansion-Module Firmware File**. A dialog box shows 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 a drive enclosure. Wait for a message that the code load has completed.

6. Verify that each updated expansion module has the correct firmware version.

Updating expansion module firmware using FTP

A drive enclosure contains two expansion modules. Each expansion module contains an 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.

 **IMPORTANT:** Disable PFU before attempting to update the firmware. If PFU is not disabled, it will downgrade the firmware on the corresponding expansion module. If this occurs, restart each SC.

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 RAIDar, determine the address of each expansion module to update:
 - a. In the Configuration View panel, select a drive enclosure.
 - b. In the enclosure properties table, note each EMP's bus ID and target ID values. For example, 0 and 63, and 1 and 63. Bus 0 is the bus that is native to a given controller, while bus 1 is an alternate path through the partner controller. It is recommended to perform update tasks consistently through one controller to avoid confusion.
3. In RAIDar, 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. 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. Either:

- To update all expansion modules, enter:

```
put firmware-file enc1
```

- To update specific expansion modules, enter:

```
put firmware-file enc1:EMP-bus-ID:EMP-target-ID
```

For example:

```
put S110R01.bin enc1:1:63
```

△ 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 1.5 minutes to update each EMP in a drive enclosure. Wait for a message that the code load has completed.

📄 NOTE: If the update fails, verify that you specified the correct firmware file and try the update a second time. If it fails again, contact technical support.

8. If you are updating specific expansion modules, repeat [step 7](#) for each remaining expansion module that needs to be updated.
9. Quit the FTP session.
10. Verify that each updated expansion module has the correct firmware version.

Identifying cable faults

When identifying cable faults, you must remember that there are two sides of the controller: the input/output to the host and the input/output to drive enclosures. It is also important to remember that identifying a cable fault can be difficult due to the multiple components that make up the data paths that cannot be overlooked as a cause of the fault.

Before beginning the troubleshooting analysis, review the cabling instructions for connecting hosts and drive enclosures (see the *AssuredSAN 4000 Series Setup Guide*) to verify proper cabling. Many faults can be eliminated by properly cabling the storage system.

Identifying cable faults on the host side

To identify a faulty cable on the host side, use the host link status LED and perform the troubleshooting procedure described in [Using controller module host port LEDs – rear panel](#) on page 92.

Identifying cable faults on the drive enclosure side

To identify a faulty cable on the drive enclosure side, use the expansion port status LED and perform the troubleshooting procedure described in [Using the controller module expansion port status LED – rear panel](#) on page 92.

Disconnecting and reconnecting SAS cables

The storage system supports disconnecting and reconnecting SAS cables between enclosures while the system is active. You might need to do this a part of replacing an IOM.

Follow these guidelines:

- If less than 15 seconds elapse between disconnecting and reconnecting a cable to the same port, no further action is required.
- If 15 or more seconds elapse between disconnecting a cable and connecting it to a different port on the same enclosure — or different enclosure — no further action is required.
- If less than 15 seconds elapse between disconnecting a cable and connecting it to a different port on the same enclosure — or different enclosure — you must perform a rescan.

Use RAIDar or the CLI to perform a rescan only if necessary.

Using RAIDar to perform a rescan

1. Sign-in to RAIDar using default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. In the Configuration View, right-click the system and select **View > Overview**. The System Overview panel appears. Within the System Redundancy table, verify that the status for controller A and controller B is set to **Operational**.
3. In the Configuration View, right-click the system and select **Tools > Rescan Disk Channels**.
4. Click **Rescan**.

Using the CLI to perform a rescan

1. Log-in to the CLI using default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. To perform a rescan, run the `rescan` command.

Identifying disk drive module faults

When identifying faults in disk drive modules, you must be able to:

- Understand disk-related errors.
- Determine whether the error is due to a faulty disk or a faulty disk channel.
- Identify which action the controller has taken to protect the vdisk after the fault occurred (e.g., reconstructing to a hot-spare).
- Identify disk drives in the enclosure.
- Understand the procedure for replacing a faulty disk drive module.

Understanding disk-related errors

The event log includes errors reported by the EMPs and disk drives in the storage system. Should you see such errors in the event log, the following information will help you better understand the errors.

Upon detecting a disk-related error, the disk drive returns a SCSI sense key. RAIDar records this key — and additional information if appropriate — in the event log. [Table 17](#) lists common SCSI sense key descriptions in hexadecimal format. [Table 18](#) lists the descriptions for the standard SCSI sense codes (ASC) and sense code qualifiers (ASCQ), all in hexadecimal. See the SCSI Primary Commands – (SPC-2, SPC-3, SPC-4) Specifications for a complete listing of ASC and ASCQ descriptions.

Table 17 Standard SCSI sense key descriptions

Sense key	Description
0h	No sense
1h	Recovered error
2h	Not Ready
3h	Medium error
4h	Hardware error
5h	Illegal request
6h	Unit attention
7h	Data protect
8h	Blank check
9h	Vendor-specific
Ah	Copy aborted
Bh	Aborted command
Ch	Obsolete
Dh	Volume overflow
Eh	Miscompare
Fh	Reserved

Table 18 Common ASC and ASCQ descriptions

ASC	ASCQ	Description
0C	02	Write error: Auto-reallocation failed
0C	03	Write error: Recommend reassignment
11	00	Unrecovered read error
11	01	Read retries exhausted
11	02	Error too long to correct
11	03	Multiple read errors
11	04	Unrecovered read error: Auto-reallocation failed
11	0B	Unrecovered read error: Recommend reassignment
11	0C	Unrecovered read error: Recommend rewrite the data
47	01h	Data phase CRC error detected

For example, the following error might be reported:

```
DISK DETECTED ERR 1.10 02, 04, 11.
```

This indicates the disk in drive slot No.10 of enclosure ID No.1 reported a sense key error of "2" (Not ready) and an ASCQ/ASC of "04/11" (Unrecovered read error — auto-reallocation failed).

Disk drive errors

In general, media errors (sense key 3), recovery errors (sense key 1), and SMART events (identified by SMART event text within event logs) indicate a problem with a specific disk drive. Other events, such as protocol errors and I/O timeouts might indicate disk drive problems, or they might indicate poorly-seated or faulty cables, or problems with particular drive slots. Each of these events may produce a warning or critical notification in the RAIDar event log.

Disk channel errors

Disk channel errors are similar to disk-detected errors, except they are detected by the controllers instead of the disk drive. Some disk channel errors are displayed as text strings. Others are displayed as hexadecimal codes.

In case of a critical error, see [Disk drive errors](#). Otherwise, [Table 19](#) lists the descriptions for disk channel errors. Most disk channel errors are informational because the storage system issues retries to correct any problem. Errors that cannot be corrected with retries result in another critical event describing the affected array (if any).

Table 19 Disk channel error codes

Error Code	Description
CRC Error	CRC error on data was received from a target
Dev Busy	Target reported busy status
Dn/Ov Run	Data overrun or underrun has been detected
IOTimeout	Array aborted an I/O request to this target because it timed out
Link Down	Link down while communication in progress
LIP	I/O request was aborted because of a channel rest
No Response	No response from target
Port Fail	Disk channel hardware failure. This may be the result of bad cabling
PrtColError	Array detected an unrecoverable protocol error on the part of the target
QueueFull	Target reported queue full status
Stat: 04	Data overrun or underrun occurred while getting sense data
Stat: 05	Request for sense data failed
Stat: 32	Target has been reserved by another initiator
Stat: 42	I/O request was aborted because of array's decision to reset the channel
Stat: 44	Array decided to abort I/O request for reasons other than bus or target reset
Stat: 45	I/O request was aborted because of target reset requested by array
Stat: 46	Target did not respond properly to abort sequence

Identifying faulty disk drive modules

To identify faulty disk drive modules, perform the following steps:

1. Does the fault involve a single disk?
 - If yes, perform step 2 through step 4.
 - If an entire enclosure of disk drives is faulty, check the cabling, and if necessary, perform the steps in [Identifying cable faults](#) on page 115.
2. Identify the suspected faulty disk drive using the LEDs.
3. Replace the faulty disk drive with a known good disk (a replacement disk drive module).
4. Does the replacement disk drive module correct the fault?
 - If yes, no further action is necessary.
 - Otherwise, continue to step 5.
5. The fault might be caused by a bad disk drive slot on the midplane. Investigate this possibility by powering off the storage system; moving a known functioning disk drive module into the suspected slot; and performing a system power up.

 **NOTE:** This step requires scheduled down time.

6. Does the disk fail when installed in the suspected slot?
 - If yes, replace the chassis with midplane FRU (the enclosure).
 - Otherwise, continue to step 7.
7. If the disk does not fail, move it back to the original disk drive slot, and re-insert the replacement disk drive module into the suspected slot, ensuring that the disk is fully inserted and secured into position.
8. To ensure that the controller detects all drives, power cycle the drive enclosure.

 **NOTE:** This step requires scheduled down time.

If the disk drive fails again, the midplane may have an intermittent fault, or the connector may be dirty. Replace the enclosure FRU.

Updating disk drive firmware

You can view the current versions of firmware in disks, and install new versions.

 **NOTE:** Disks of the same model in the storage system must have the same firmware revision.

 **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.

 **NOTE:** If a vdisk is quarantined, firmware update is not permitted due to the risk of losing unwritten data that remains in cache for the vdisk's volumes. Before you can update firmware, you must resolve the problem that is causing the vdisk to be quarantined, as described in the "Removing a disk from quarantine" topic in the *AssuredSAN 4000 Series RAIDar User Guide*.

Updating disk drive firmware using RAIDar

1. Obtain the appropriate firmware file and download it to your computer or network.
2. Check the disk manufacturer's documentation to determine whether disks must be power cycled after firmware update.
3. Stop I/O to the storage system. During the update all volumes will be temporarily inaccessible to hosts. If I/O is not stopped, mapped hosts will report I/O errors. Volume access is restored after the update completes.
4. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. A table titled Current Versions (Revisions) of All Disk Drives displays the currently installed versions.
5. Select the disks to update.
6. Click **Browse** and select the firmware file to install.
7. Click **Install Disk Firmware File**. A dialog box shows firmware-update progress.

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

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

8. If the updated disks must be power cycled:
 - a. Shut down both controllers; see [Shutting down a controller module](#) on page 106.
 - b. Power cycle all enclosures as described in the *AssuredSAN 4000 Series Setup Guide*.
9. Verify that each disk has the correct firmware revision.

Updating disk drive firmware using FTP

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 RAIDar, for each disk to update, determine the enclosure number and slot number of the disk.
4. In RAIDar, 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 RAIDar.
 - b. Power cycle all enclosures as described in the *AssuredSAN 4000 Series Setup Guide*.
8. Verify that each disk has the correct firmware revision.

Replacing a disk drive module

A disk drive module consists of a disk in a sled. Disk drive modules are hot-swappable, which means they can be replaced without halting I/O to the vdisks, or powering off the enclosure. The new disk drive module must be of the same type, and possess capacity equal to or greater than the smallest disk in the system. Otherwise, the storage system cannot use the new disk to reconstruct the vdisk (see “About vdisks” and “About disk failure and vdisk reconstruction” topics in the *AssuredSAN 4000 Series RAIDar User Guide*).

Air management modules

An air management module looks like a disk drive module; however, it is an empty box — also known as a blank — used to maintain optimum air flow for proper cooling within an enclosure. Air management modules are installed in slots missing disk drive modules. If you must remove a disk drive module, but cannot immediately replace it, you must either leave the faulty module in place, or insert an air management module in its place.

The blank is installed using the same procedure as [Installing a disk drive module on page 123](#). Similarly, the blank is removed using the same procedures as [Removing a disk drive module on page 122](#).

Before you begin

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

△ **CAUTION:** Removing either a disk drive module or blank impacts the airflow and cooling ability of the enclosure. If the internal temperature exceeds acceptable limits, the enclosure may overheat, and automatically shut down or restart. To avoid potential overheating, wait 20 seconds to allow the internal disks to stop spinning, then insert the new disk drive module or blank.

Verifying component failure

Before replacing a disk, perform the following steps to ensure that you have correctly identified the module requiring removal and replacement.

△ **CAUTION:** Failure to identify the correct disk drive module could result in data loss if the wrong disk is removed from the enclosure.

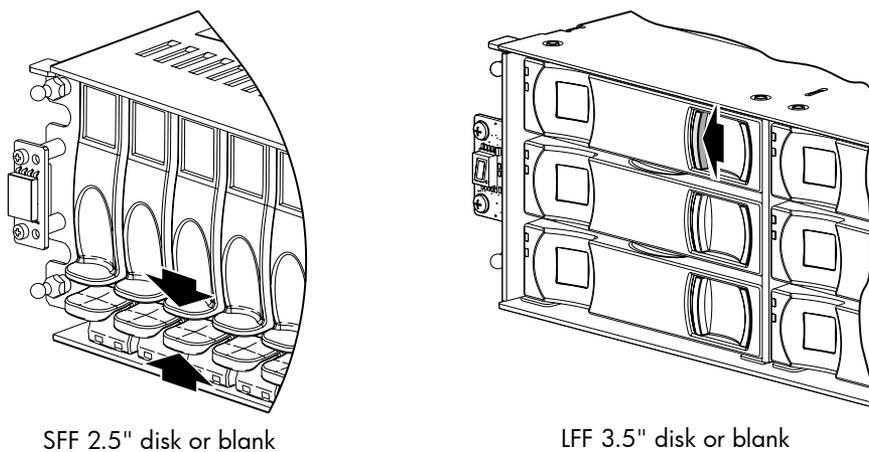
When a disk drive fault occurs, the failed disk's Fault Indicator LED, located on the enclosure's front panel, illuminates solid amber (see [System LEDs](#) for a description of LEDs and disk drive slot numbering for your enclosure). You can determine from visual inspection which disk in the enclosure is experiencing a fault/failure using the fault LED for your disk type. If necessary, use the `set led` command in the CLI to illuminate the disk locator LED.

Alternatively, you can observe disk component health using management interfaces to verify component failure or component operation (see [Using management interfaces](#) on page 142 for more information).

📄 **NOTE:** For enclosures equipped with a dust filtration bezel, you must remove the bezel to view the disk drive LEDs. Enclosure status LEDs are visible on the labeled bezel. See the enclosure bezel kit installation document in your product ship kit for information about removing and installing the bezel, or for instructions about servicing or replacing the bezel air filter.

Removing a disk drive module

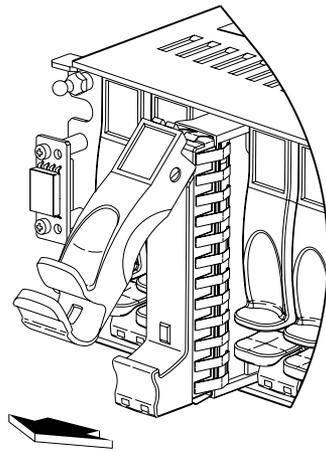
1. Disengage the disk drive module. See [Figure 5](#) on page 122.
 - SFF disk — Squeeze the latch release flanges together to disengage the disk drive module.
 - LFF disk — Slide the release latch to the left to disengage the disk drive module. Moving the latch to the left will provide a clicking sound and cause the spring to move its position inside the chassis, partially ejecting the disk from its installed position within the disk drive slot.



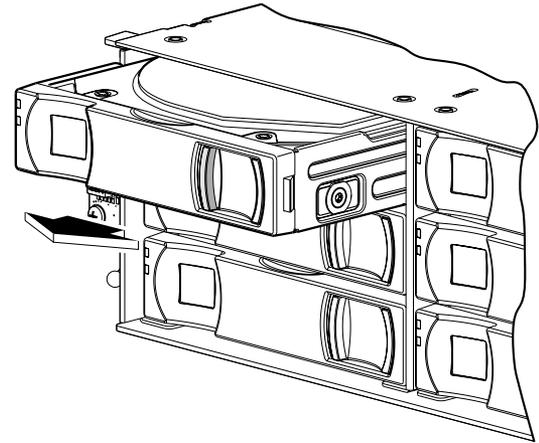
The enclosure bezel is removed in the illustrations above to show disks

Figure 5 Disengaging a disk drive module or blank

2. Wait 20 seconds for the internal disks to stop spinning.
3. Remove the disk drive module. See [Figure 6](#) on page 123.
 - SFF disk — Pull the disk drive module straight out of the chassis, taking care not to drop the module.
 - LFF disk — Once the disk drive module partially ejects from the slot, grasp the module firmly, and carefully pull it straight out of the chassis slot.



Extract SFF disk or blank

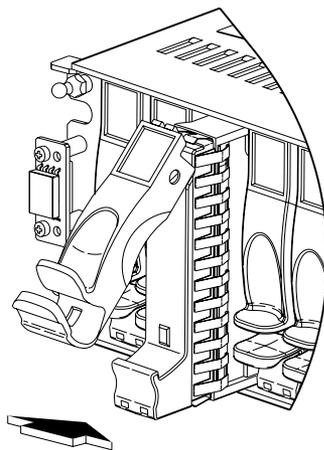


Eject and extract LFF disk or blank

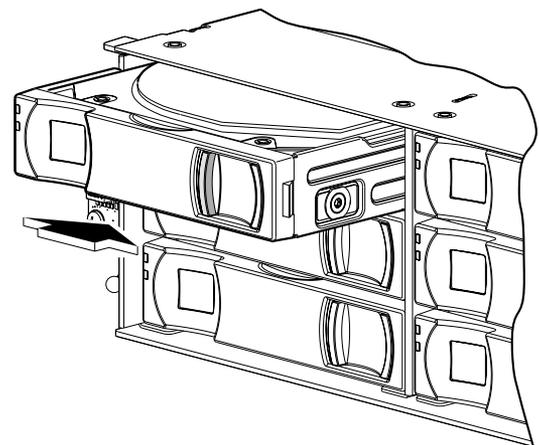
Figure 6 Removing a disk drive module or blank

Installing a disk drive module

1. If you have a SFF disk, prepare the slot for a disk drive module.
Squeeze the latch release flanges together, and then pull the latch, rotating it upward until it is fully open (see [Figure 5](#) on page 122).
2. Insert the disk drive module.
 - SFF disk — With the LEDs oriented to the bottom, slide the disk drive module into the drive slot as far as it will go (see upper left illustration in [Figure 7](#) on page 123).
 - LFF disk — With the LEDs oriented to the left, slide the disk drive module into the drive slot as far as it will go (see bottom illustration in [Figure 7](#) on page 123).



Insert SFF disk or blank



Insert LFF disk or blank

The enclosure bezel is removed in the illustrations above to show disks

Figure 7 Installing a disk drive module or blank

3. Secure the disk drive module in the slot.
 - SFF disk — Rotate the latch downward until it clicks closed to firmly seat the disk drive module in the enclosure midplane.
 - LFF disk — Verify that you have inserted the disk drive module into the slot as far as it will go, to ensure that the module is firmly seated in the enclosure midplane.

The installed disk drive module should now appear as shown in [Figure 5](#) on page 122.

 **NOTE:** Allow at least 30 seconds to elapse when jointly completing the “Removing a disk drive module” and “Installing a disk drive module” procedures.

Complete the procedure using either RAIDar or the CLI.

Using RAIDar:

1. Sign-in to RAIDar using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. View the System Overview panel to determine whether the health of the new disk is OK.
 - If the health is OK, then the disk drive module installation process is complete.
 - If the health is not OK, then in the Configuration View panel, select the enclosure that the new disk is in to display the Enclosure Overview panel, then select the disk and view details about it, such as Status and Health Recommendations.

Using the CLI:

1. Sign-in to the CLI using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. View information about disks by running the `show disks <disk-ID>` command.
Disks are specified by enclosure ID and slot number. Enclosure IDs increment from 0. Disk IDs increment from 0 in each enclosure (e.g., `show disks 0.7`). Entering the command shown above will display the disk health. If health is not OK, the command output will also display recommended actions.

Determine if a disk is missing

You can determine whether a disk is missing by using management interfaces.

Using RAIDar

1. Sign-in to RAIDar using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. In the Configuration View panel, right-click on the appropriate enclosure under **Physical**.
 - Select the **Front Graphical** tab to display a pictorial representation of disks within slots and the supporting enclosure table showing properties and values.
 - Select the **Front Tabular** tab to display the Enclosure’s Front View data table and supporting enclosure table showing properties and values.
3. Using the graphical and tabular views, look for gaps in the disk location sequence to determine if a disk is missing.

Using the CLI

1. Log-in to the CLI using the default user `manage` and password `!manage`.
If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the system defaults shown above.
2. To determine location of a missing or faulty drive, run the `show disks` command.
The command outputs a listing of detected disks’ properties by location. Review the information, and look for gaps in the disk location sequence to determine whether any disks are missing.

Installing an air management module

An air management module looks like a disk drive module; however, it is an empty box — also known as a blank — used to maintain optimum air flow and proper cooling within an enclosure. Air management modules are installed in slots missing drive modules. If you must remove a drive module, but cannot

immediately replace it, you must either leave the faulty drive module in place, or insert an air management module in its place.

The blank is installed using the same procedure as [Installing a disk drive module on page 123](#). Similarly, the blank is removed using the same procedures as [Removing a disk drive module on page 122](#).

Verifying component operation

Check that the Power/Activity LED — located on the front face of the disk drive's slot — is illuminated green. LEDs are shown in [Figure 7](#) on page 123.

TIP: See the [System LEDs](#) for descriptions of disk drive LEDs and other front panel LEDs pertaining to 2U12 and 2U24 controller enclosures.

Also see [Using management interfaces](#) on page 142 as an alternative to physically observing LEDs to verify component operation.

Disk error conditions

[Table 20](#) provides information about possible disk error conditions and recommended actions.

Table 20 Disk error conditions and recommended actions

Condition	Recommended actions
Event 8 reports that the RAID controller can no longer detect the disk.	<ul style="list-style-type: none"> Reinsert the disk or insert a replacement disk of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity as the one that was in the slot. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. If the disk then has a status of leftover (LEFTOVR), clear the metadata to reuse the disk. If the associated vdisk is offline or quarantined, contact technical support.
Event 8 reports a media error for the disk.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
Event 8 reports a hardware error for the disk.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
At the time a disk failed, the dynamic spares feature was enabled and a properly sized disk was available to use as a spare.	No action required; the system automatically uses that disk to reconstruct the vdisk.
At the time a disk failed, the dynamic spares feature was enabled but no properly sized disk was available to use as a spare.	Replace the disk so the system can automatically use the new disk to reconstruct the vdisk.
At the time a disk failed, the dynamic spares feature was disabled and no dedicated spare or properly sized global spare was available.	Replace the disk and use RAIDar to assign the new disk as a spare for the vdisk so the system can automatically use that disk to reconstruct the vdisk.

Table 20 Disk error conditions and recommended actions

Condition	Recommended actions
The status of the vdisk that originally had the failed disk status is FTOL. A global or vdisk (dedicated) spare has been successfully integrated into the vdisk and the replacement disk can be assigned as either a global spare or a vdisk spare.	Use RAIDar to assign the new disk as either a global spare or a vdisk spare.
The status of the disk just installed is LEFTOVR.	All of the member disks in a vdisk contain metadata in the first sectors. The storage system uses the metadata to identify vdisk members after restarting or replacing enclosures. See clear disk-metadata on page 39 for more information.
If the status of the vdisk that originally had the failed disk status is OFFL, one or more disks have failed in a RAID-0 vdisk; two or more disks have failed in a RAID-1, 3, or 5 vdisk; or three or more disks have failed in a RAID-6 vdisk.	Use the <code>trust</code> command as described in trust on page 84. If the <code>trust</code> operation succeeds, subsequently delete the vdisk. If <code>trust</code> is not successful, contact technical support
The disk status is FAILED or FAULT. The disk has excessive media errors, a SMART error, a hardware failure, or is not supported.	Replace the disk.
The status of the vdisk that originally had the failed disk status is DRV ABSENT or INCOMPLETE. These status indicators only occur when the enclosure is initially powered up. DRV ABSENT indicates that one disk is bad. INCOMPLETE indicates that two or more disks are bad.	Make sure the enclosures and associated data host were powered on in this order: first the drive enclosures, then the controller enclosure, then the data host. If the power-on sequence was correct, locate and replace the additional failed disks.

Identifying vdisk faults

Obvious vdisk problems involve the failure of a member disk drive. Table 30 describes additional issues that are not so obvious, which result in vdisk faults.

Table 21 Vdisk faults

Problem	Recommended actions
Expanding a vdisk requires days to complete.	<ul style="list-style-type: none"> In general, expanding a vdisk can take days to complete. You cannot stop the expansion once it is started. If you have an immediate need, create a new vdisk of the size you want, transfer your data to the new vdisk, and then delete the old vdisk
Failover causes a vdisk to become critical when one of its drives disappears.	<ul style="list-style-type: none"> In general, failover is not supported if a disk is in a drive enclosure that is connected to the controller enclosure with only one cable. Access to the drive enclosure will be lost if the controller to which it is connected fails. When the controller with the direct connection to the drive enclosure comes back online, access to the drive enclosure disks is restored. To avoid this problem, ensure that two cables are used to connect enclosures as shown in the Setup Guide. Verify that cables are not damaged, and that they are connected securely. If the problem persists or affects a disk in a controller enclosure, a hardware problem might have occurred in the disk drive module, dongle, midplane, or controller module. Identify and replace the FRU where the problem occurred.
A vdisk is smaller than it should be.	Verify that the disk drives are all the same size within the vdisk. The vdisk is limited by the smallest sized disk.

Table 21 Vdisk faults

Problem	Recommended actions
<p>Volumes in the vdisk are not visible to the host.</p>	<p>Verify that volumes are mapped to the host using RAIDar: In the Configuration View, expand Hosts, right-click the host and select Provisioning > Manage Host Mappings. See the AssuredSAN 4000 Series RAIDar User Guide for more information</p>
<p>Vdisk Degraded Event codes 58 and 1, or Event codes 8 and 1</p>	<ul style="list-style-type: none"> • If no spare was present and the dynamic spares feature is disabled (that is, event 37 was not logged), configure an available disk as a dedicated spare for the vdisk or replace the failed disk and configure the new disk as a dedicated spare for the vdisk. That spare will be used to automatically reconstruct the vdisk; confirm this by checking that events 9 and 37 are logged. • Otherwise, reconstruction automatically started and event 37 was logged. Replace the failed disk and configure the replacement as a dedicated or global spare for future use. • If the replacement disk was previously used in another vdisk and has a status of leftover (LEFTOVR), clear the disk's metadata so you can assign the disk as a spare. • Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. • Confirm that all failed disks have been replaced and that there are sufficient spare disks configured for future use. • See event 8 on page 151
<p>Vdisk Failure Event codes 58 and 3, or Event codes 8 and 3</p>	<ul style="list-style-type: none"> • Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. • Delete the vdisk (delete vdisks CLI command). • Recreate the vdisk (create vdisk CLI command). • To prevent this problem in the future, use a fault-tolerant RAID level, configure one or more disks as spare disks, and replace failed disks promptly. • See event 8 on page 151
<p>Vdisk Quarantined Event code 172</p>	<ul style="list-style-type: none"> • Ensure that all disks are latched into their slots and have power. • During quarantine, the vdisk is not visible to the host. If after latching disks into their slots and powering up the vdisk, the vdisk is still quarantined, you can manually remove the vdisk from quarantine so that the host can see the vdisk. The vdisk is still critical. • If disks have failed, replace them. • When the vdisk has been removed from quarantine, event 173 is logged.
<p>Spare Disk Failure Event code 62</p>	<ul style="list-style-type: none"> • Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. • If the failed disk was a global spare, configure the new disk as a global spare. • If the failed disk was a dedicated spare, configure the new disk as a dedicated spare for the same vdisk.

Table 21 Vdisk faults

Problem	Recommended actions
Spare Disk Unusable Event code 78	<ul style="list-style-type: none"> • Replace each failed disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. • Configure disks as dedicated spares or global spares. • For a dedicated spare, the disk must be of the same type as the other disks in the vdisk and at least as large as the smallest-capacity disk in the vdisk, and it should have the same or better performance. • For a global spare, it is best to choose a disk that is as big as or bigger than the largest disk of its type in the system and of equal or greater performance. If the system contains a mix of disk types (SAS SSD, enterprise SAS, or midline SAS), there should be at least one global spare of each type (unless dedicated spares are used to protect every vdisk of a given type).
Mixed drive type errors	<p>Vdisks do not support mixed drive types.</p> <ul style="list-style-type: none"> • Verify that the disks in the vdisk are of the same type (SAS SSD, enterprise SAS, or midline SAS), and that they possess the same capacity. If you attempt to build a vdisk using mixed disk types, you will receive an error. • If you attempt to build a vdisk using disks of varying sizes, you will receive a warning. The capacity of the smallest disk will be set for all other disks.

Replacing a PSU

This section provides procedures for replacing a failed AC or DC PSU.

-
- ⚠ **CAUTION:** PSU FRU replacement activities can cause enclosure cables to disconnect and disks to go offline. Take care to avoid accidentally disconnecting cables.
-

When replacing a PSU FRU, you might accidentally disconnect cables, causing disks to go offline. As a precaution — before installing or replacing a FRU — you should stop I/O to all vdisks. If stopping I/O is not possible, the next best action is to defer FRU replacement until such time as it is possible to stop all I/O. If immediate replacement is necessary during I/O, ensure that all cables are securely fastened, and *proceed with great caution* as you replace the PSU FRU within the controller enclosure. Be very careful if moving a cabled/operational enclosure during the FRU replacement process.

A single PSU is sufficient to maintain operation of the enclosure. You do not need to halt operations and completely power-off the enclosure when replacing only one PSU; however, a complete shutdown is required if replacing both PSUs.

-
- 💡 **TIP:** [PSU faults and recommended actions](#) on page 129 provides additional information.
-

Before you begin

-
- ⚠ **CAUTION:** Removing a PSU significantly disrupts the enclosure's airflow. Do not remove the PSU until you have received the replacement module.
-

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

Verifying component failure

When either a fan or PSU component fails, RAIDar provides notification; faults are recorded in the event log; and the PSU's status LED color changes to amber to indicate a fault condition.

Table 22 PSU faults and recommended actions

Problem	Recommended action
Event code 168: PSU fan warning or failure, or PSU warning or failure	<ul style="list-style-type: none">• Verify that all fans are working using RAIDar.• In the Configuration View, expand Physical, right-click the enclosure and select View > Overview. Select either Rear Graphical or Rear Tabular to view health attributes.• Ensure that the PSUs are properly seated and secured within their slots.• Ensure that no slots are left open for more than 2 minutes. If you must replace the FRU, leave the old module in place until the replacement arrives to maintain optimal airflow and avoid overheating.
Event code 168: PSU failure status, or voltage event notification	<ul style="list-style-type: none">• Verify that the PSU is powered on. If your PSU has a power switch, verify that it is switched on.
AC Power Good LED is off	<ul style="list-style-type: none">• Verify that the power cables are securely attached to the PSU and the appropriate power source.• Replace the FRU if necessary.
DC Voltage/Fan Fault/Service Required LED is illuminated	<ul style="list-style-type: none">• Replace the PSU FRU.

Alternatively, you can observe PSU component health (PSUs, fans) using management interfaces to verify component failure or component operation (see [Using management interfaces](#) on page 142 for more information).

PSUs

 **IMPORTANT:** Newer AC PSUs do not have power switches. These PSUs power on when connected to a power source, and power off when disconnected.

Power cycling procedures vary according to the type of PSU included within the enclosure. For controller and expansion enclosures configured with AC PSUs that do not have power switches, refer to the procedure described under [AC PSU](#). For procedures pertaining to controller enclosures configured with DC PSUs or previously installed drive enclosures featuring power switches, see [DC and AC PSUs with power switch](#) on page 130.

 **NOTE:** AC PSUs — with or without a power switch — are compatible with one another; the two different models can coexist in the same enclosure, and are interchangeable.

AC PSU

Enclosures configured with AC PSUs that do not have a power switch rely on the power cord for power cycling. Connecting the cord from the PSU power cord connector to the appropriate power source facilitates power on; whereas disconnecting the cord from the power source facilitates power off.

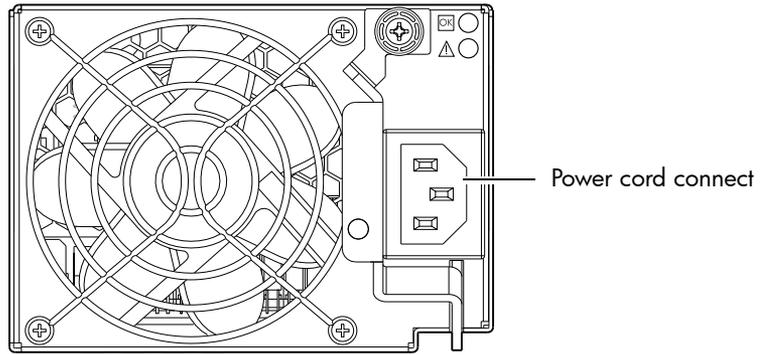


Figure 8 AC PSU

Powering off the PSU

1. Stop all I/O from hosts to the enclosure (see [Stopping I/O](#) on page 106).
2. Use management software to shut down any other system components necessary.

Disconnecting an AC power cord

1. Disconnect the power cord's male plug from the power source.
2. Disconnect the power cord's female plug from the power cord connector on the PSU.

 **NOTE:** See [Connecting a power cable](#) on page 133 for an illustration showing AC power cord connection/disconnection.

DC and AC PSUs with power switch

DC and legacy AC power supplies — each equipped with a power switch — are shown below.

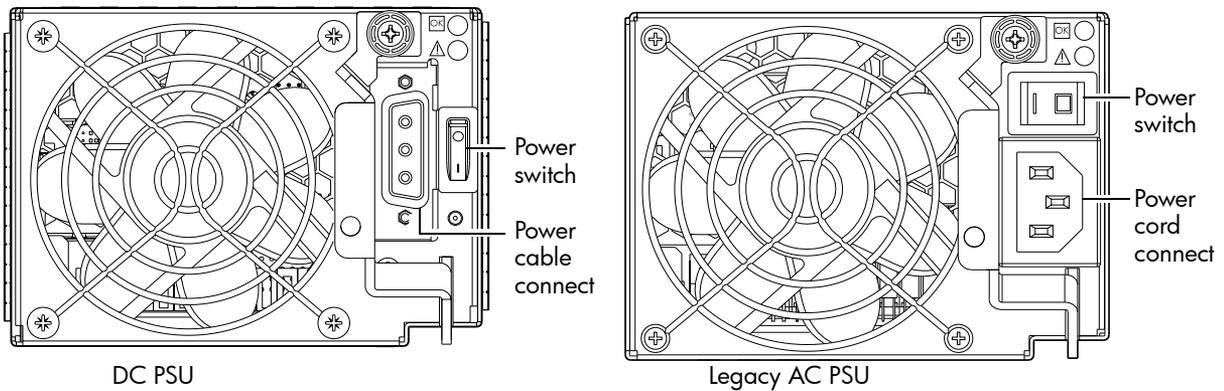


Figure 9 DC and AC PSUs with power switch

Powering off the PSU

1. Stop all I/O from hosts to the system (see [Stopping I/O](#) on page 106).
2. Use management software to shut down any other system components necessary.
3. Turn off the power switch on the PSU being replaced and on the replacement PSU.

Disconnecting an AC power cord

1. Verify that the power switch on the PSU being replaced is in the **Off** position.
2. Disconnect the power cord's male plug from the power source.
3. Disconnect the power cord's female plug from the power cord connector on the PSU.

NOTE: See [Connecting a power cable](#) on page 133 for illustrations showing both AC and DC power cord connection/disconnection.

Disconnecting a DC power cable

1. Verify that the power switch on the PSU being replaced is in the **Off** position.
2. Loosen the cable-locking screws that attach each D-shell connector to its PSU, and carefully disconnect the lugs on each cable wire component of the DC power cable from the DC power source ([Figure 13](#) on page 133 shows cable wire lugs and D-shell connector).
3. Loosen the cable-locking screws attaching the D-shell connector to the PSU, and disconnect the power cable from the PSU.

Removing a PSU

NOTE: If replacing both PSUs, verify that the enclosure is powered off.

1. If the PSU model has a power switch, verify that the switch is set to the **Off** position.
2. Verify that the power cord is disconnected.
3. Turn the thumbscrew at the top of the latch counterclockwise to loosen and disengage it from the module; however, do not remove the thumbscrew from the latch.
4. Rotate the latch downward by approximately 45°, supplying leverage to disconnect the module from the internal connector.

See [Figure 10](#) on page 131.

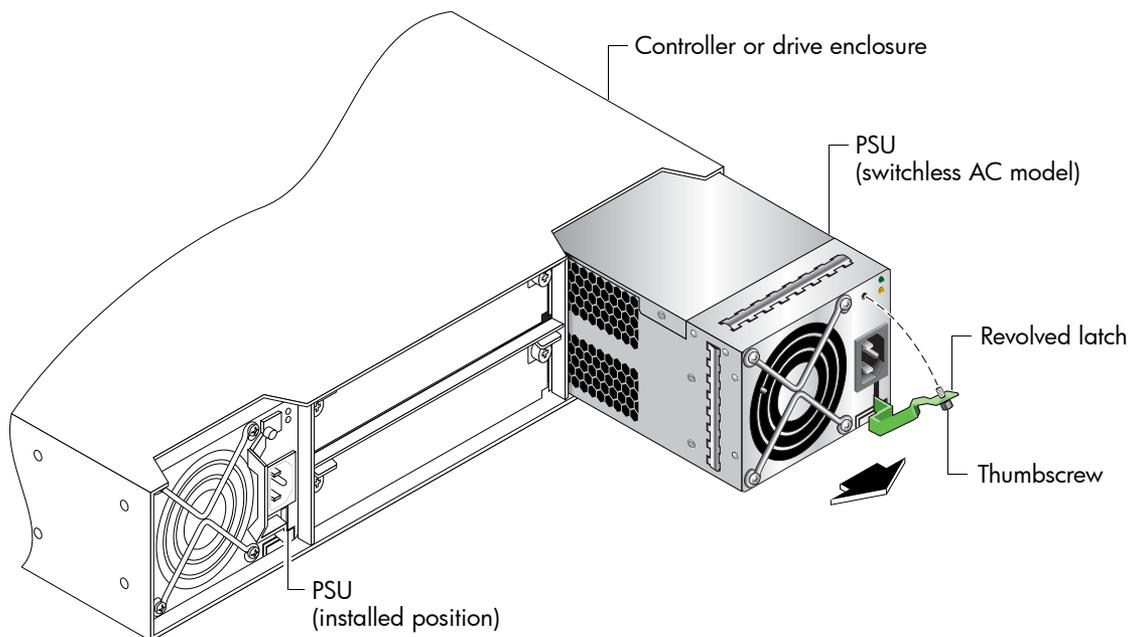


Figure 10 Removing a PSU

5. Use the latch to pull the module straight out of the chassis.
6. If replacing both PSUs, repeat step 3 through step 6.

CAUTION: Do not lift the module by its latch; doing so could damage the latch. Lift and carry the module using its metal casing.

Installing a PSU

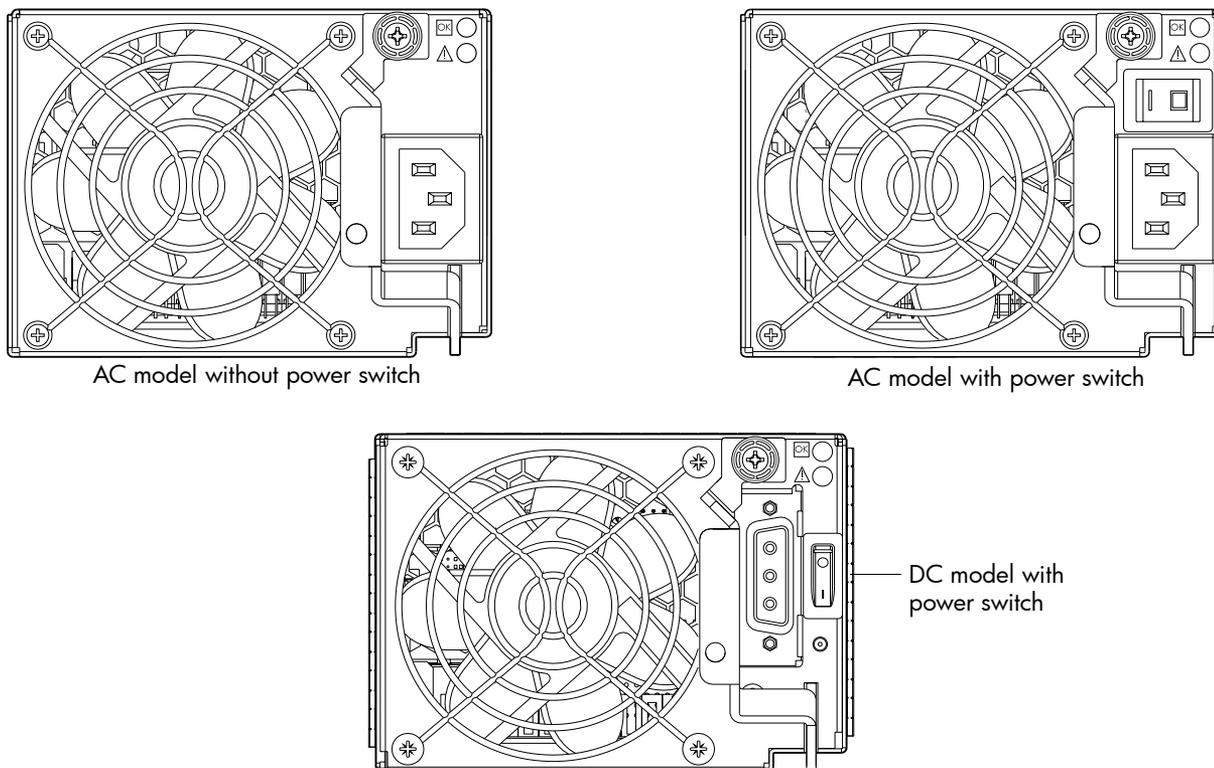


Figure 11 Orienting a PSU

To install a PSU, perform the following steps:

1. Orient the PSU with the AC or DC connector toward the right as shown in [Figure 11](#).
2. With the latch in the open position, slide the module into the appropriate PSU slot as far as it will go.
3. Rotate the PSU latch upward until it is flush against the PSU face, ensuring that the connector on the PSU engages the connector inside the chassis.
4. Turn the thumbscrew located at the top of the PSU latch clockwise, until it is finger-tight, to secure the latch to the PSU within the enclosure.
5. If replacing two PSUs, repeat step 1 through step 4.

NOTE: AC PSUs — with or without a power switch — are compatible with one another in that the two different models can coexist in the same enclosure, and are interchangeable.

Connecting a power cable

This section addresses power cable connection for enclosures configured with either AC or DC PSUs.

Connecting an AC power cord

Installation of a power cord is the same for both switchless and switched units.

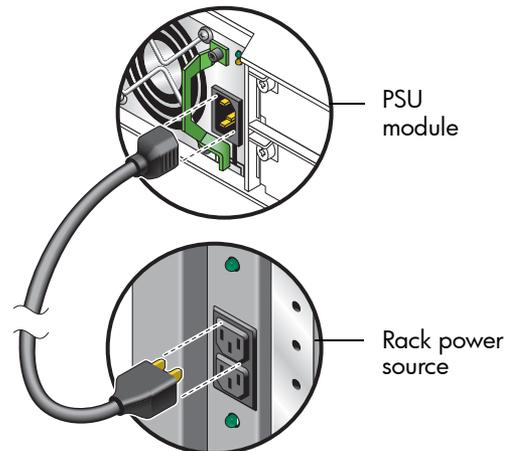


Figure 12 AC PSU power cable, switchless unit

1. Install the power cord. See [Figure 12](#).
 - a. Connect the female plug to the AC PSU cord inlet.
 - b. Connect the male plug to the rack power source.Verify connection of the primary power cord(s) from the rack to separate external power sources.
2. Power-on the newly-installed PSU:
 - Connecting the power cord effectively powers a switchless AC PSU on. Wait several seconds for the disks to spin up.
 - For AC PSUs equipped with a power switch, press the power switch to the **On** position. Wait several seconds for the disks to spin up.
3. If replacing two PSUs, repeat step 1 and 2.

Connecting a DC power cable

Locate the DC power cable that applies to the DC PSU being installed in the enclosure.

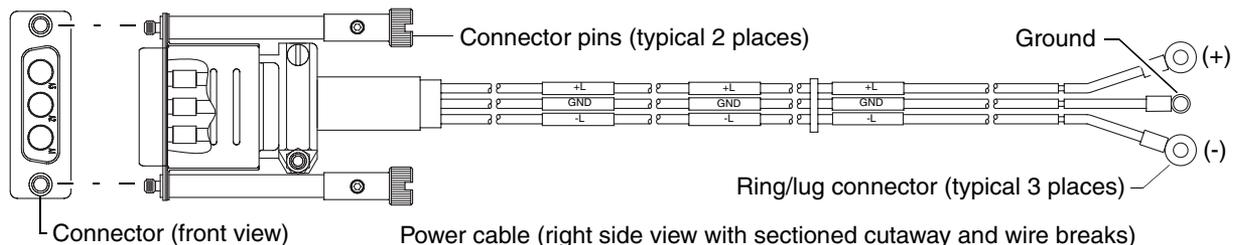
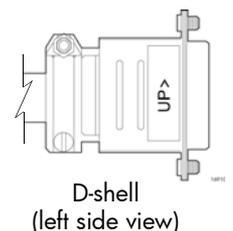


Figure 13 DC PSU power cable featuring D-shell and lug connectors

Install the appropriate DC power cable:

1. Connect a DC power cable to each DC PSU using the D-shell connector. Use the **UP>** arrow on the connector shell to ensure proper positioning (see adjacent left-side view of D-shell connector).
2. Tighten the screws at the top and bottom of the shell, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb), to securely attach the cable to the DC PSU.
3. To complete the DC connection, secure the other end of each cable wire component of the DC power cable to the target DC power source.



4. Check the three individual DC cable wire labels before connecting each cable wire lug to its power source. One cable wire is labeled ground (GND), and the other two are labeled positive (+) and negative (-), respectively. See [Figure 13](#).

△ **CAUTION:** Connecting to a DC power source outside the designated -48VDC nominal range (-36VDC to -72VDC) may damage the enclosure.

Powering on enclosures

If you did not perform a hot-swap, power-on storage system components in the following sequence. Allow time for each device to complete its POST before proceeding.

1. Drive enclosures.
2. Controller enclosures.
3. Data host (if powered down for maintenance).

Verifying component operation

Examine PSU module status as indicated in the table below.

Table 23 PSU LED descriptions

LED No./Description	Color	State	Definition
1 — Input Source Power Good	Green	On	Power is on and input voltage is normal.
		Off	Power is off, or input voltage is below the minimum threshold.
2 — Voltage/Fan Fault/Service Required	Amber	On	Output voltage is out of range, or a fan is operating below the minimum required r/min.
		Off	Output voltage is normal.

LEDs for a PSU are located in the top right corner of the module, as shown in [Figure 11](#) on page 132.

The top LED corresponds to LED number (1) above, and the bottom LED corresponds to number (2) above. If the Voltage/Fan Fault/Service Required LED is illuminated amber, the PSU module has not gone online, and likely failed its self-test. Remove and reinstall the PSU module. In addition to viewing the PSU LEDs, verify that the cooling fans are spinning. Also see [Using management interfaces](#) on page 142 as an alternative to physically observing LEDs to verify component operation.

Removing enclosure bezel

Position the bezel such that the mounting sleeves within the integrated ear caps align with the ball studs, and then gently push-fit the bezel onto the ball studs to attach the bezel to the front of the enclosure. To remove the bezel, while facing the front of the enclosure, place index and middle fingers of each hand on the top of the bezel—near each end—with thumbs on the bezel bottom. Gently pull the top of the bezel while applying slight inward pressure below, to release the bezel from the ball studs. See [Partial controller enclosure assembly showing alignment for 24-drive enclosure bezel](#) on page 210 and [Partial controller enclosure assembly showing bezel alignment \(2U12\)](#) on page 213

Replacing ear bezels

Before you begin

△ **CAUTION:** Verify that you have the proper FRU kit (left or right) for the ear that is being replaced.

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

Enclosure bezel ear FRUs are available for the left and right ears of the chassis front panel. The following bezel ear replacement procedure applies to ear kits provided with the 2U24 and 2U12 enclosure models, respectively. Refer to the following illustration(s) pertaining to your product's ear kit.

[Figure 14](#) illustrates the bezel ears for both 2U24 and 2U12 models. [Figure 15](#) illustrates exploded views of each.

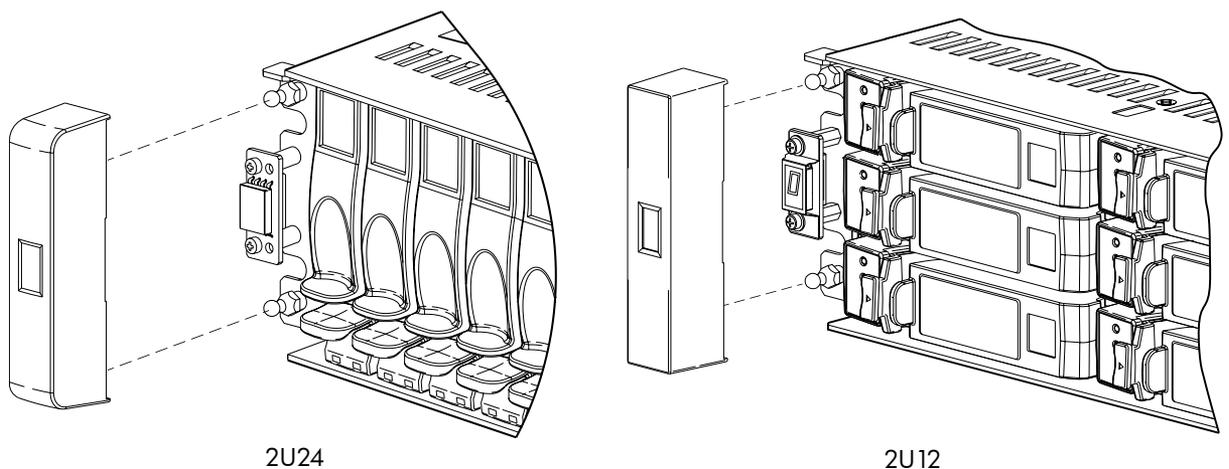


Figure 14 Ear bezel assembly

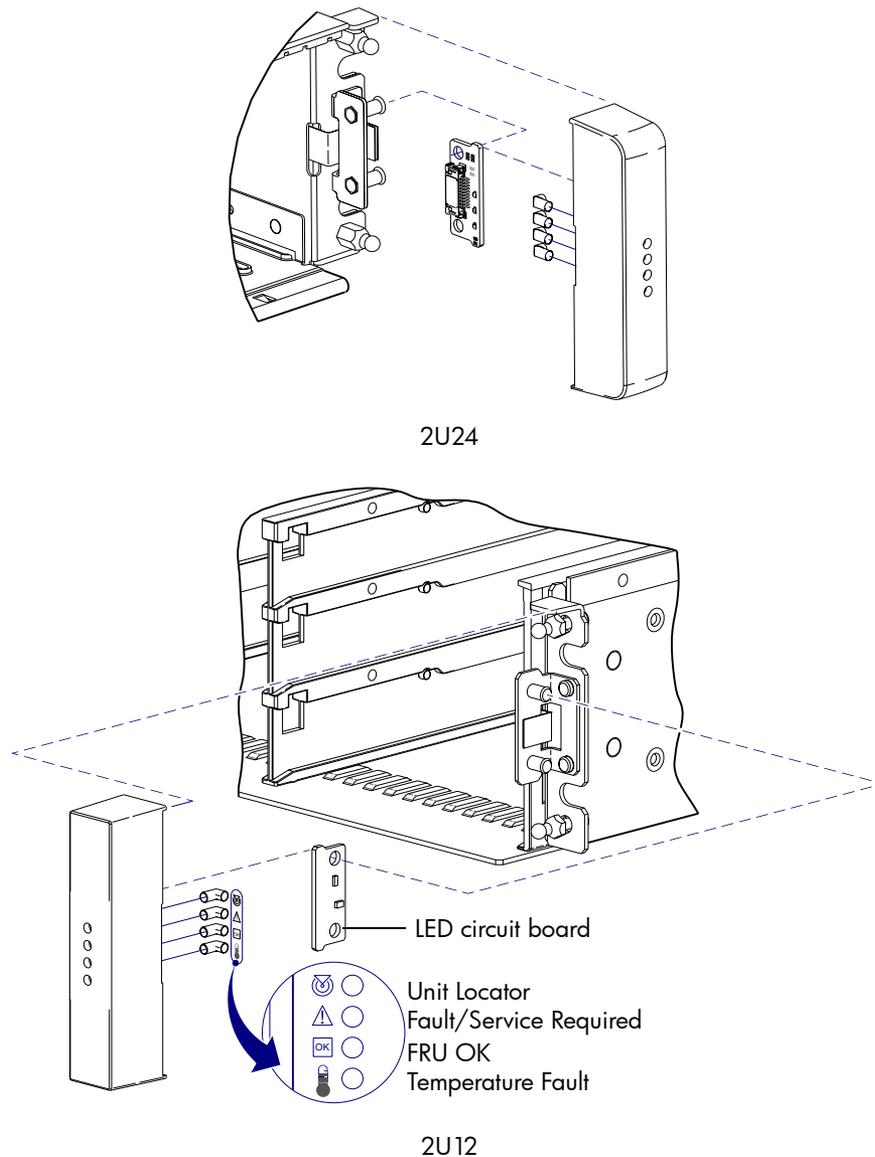


Figure 15 Ear bezel assembly: Exploded view

NOTE: Although the illustrations above show ear caps, newer product models feature an enclosure bezel instead of ear caps.

Removing the ear bezels

See [Figure 14](#) on page 135 and [Figure 15](#) on page 136 when removing the bezel ear sub-assemblies.

1. Stop all I/O from hosts to the system.
2. Use management software to shut down any other components necessary.
3. Power off the enclosure.
4. Gently squeeze the sides of the ear cover, and pull it straight forward to remove the ear from the push-fit mounting ball studs.
5. Loosen the hexagonal nuts that secure the LED circuit board to the mounting pins on the flange.
6. Remove the LED circuit board.

[Figure 15](#), right, lists LEDs common to the right ear of both 2U24 and 2U12 enclosures.

Installing the ear bezels

See [Figure 14](#) on page 135 and [Figure 15](#) on page 136 when installing the bezel ear sub-assemblies.

1. Verify that the enclosure is powered off.
2. Install the LED circuit board:
 - a. Insert the mounting pins into the through holes in the LED circuit board and mounting flange.
 - b. Thread the hexagonal nuts onto the inserted pins, and turn the nuts clockwise to tighten.
3. Gently slip the ear cover over onto the push-fit mounting ball studs, taking care to guide the LED indicators through the cover's through holes.
4. Power on the enclosure.

 **TIP:** See [System LEDs](#) on page 197 for descriptions of front panel LEDs.

Verifying component operation

Enclosure status LEDs are located on the front of the controller enclosure. See [24-disk enclosure front panel LEDs](#) on page 197 or [12-disk enclosure front panel LEDs](#) on page 198 for the enclosure front view pertaining to your model. During normal operation, the FRU OK and Temperature Fault LEDs are green, and the other status LEDs are off.

Replacing an FC transceiver

This section provides steps for replacing an SFP transceiver connector used in an FC controller host port. An example SFP connector is shown below.

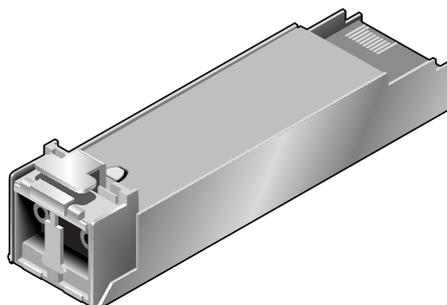


Figure 16 Sample SFP connector

Before you begin

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

△ **CAUTION:** Mishandling fibre-optic cables can degrade performance. Do not twist, fold, pinch, or step on fibre-optic cables. Do not bend them tighter than a 2-inch radius.

△ **CAUTION:** To prevent potential loss of access to data, be sure to identify the correct cable and SFP connector for subsequent removal.

Verifying component failure

Transceivers are part of a data path that includes multiple components, such as the transceiver, a cable, another SFP, and an HBA. A reported fault can be caused by any component in the data path. To identify the location of the fault, check the Link Status and Activity LEDs on the controller enclosure and server. Also, check the cable for kinks, crimping or other possible damage.

TIP: See [System LEDs](#) for descriptions of rear panel LEDs.

Removing an SFP module

Perform the following procedure to remove an SFP connector. When removing an FC SFP that has previously limited the port speed — and replacing it with a higher-rated SFP — it is possible, though rare, that auto-negotiation will not enable the higher port speed. Rebooting the array or the host resolves the problem.

1. Disconnect the fibre-optic interface cable by squeezing the end of the cable connector. If the SFP does not have a cable, it should have a plug (retained from installation).

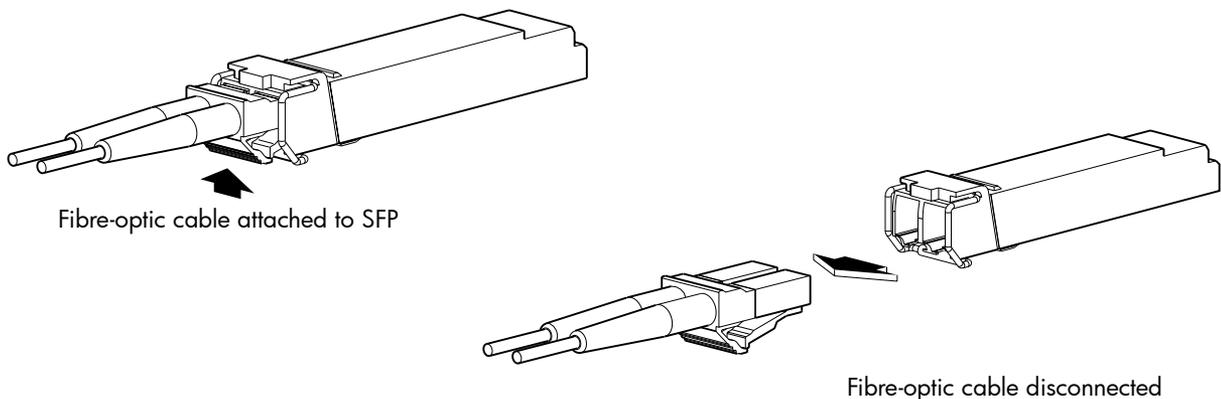


Figure 17 Disconnect fibre-optic interface cable from SFP

2. SFPs are commonly held in place by a small wire bail actuator. Flip the actuator up.

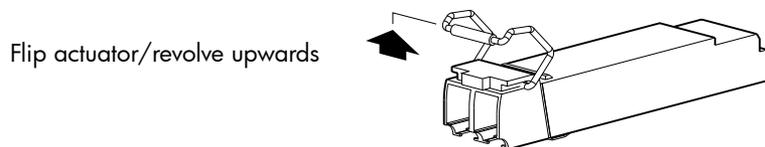


Figure 18 Flip SFP actuator upwards

3. Grasp the SFP between your thumb and index finger, and carefully remove it from the controller module.

Installing an SFP module

Perform the following procedure to install an SFP connector.

1. To connect to an empty port, slide the SFP connector into the port until it locks into place. If the SFP has a plug, remove it before sliding the connector into the FC port. Retain the plug.
2. Flip the actuator down.

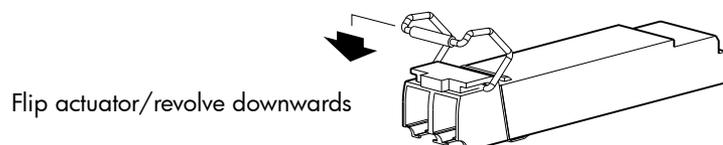


Figure 19 Flip SFP actuator downwards

3. Connect the fibre-optic interface cable into the duplex jack at the end of the SFP connector.

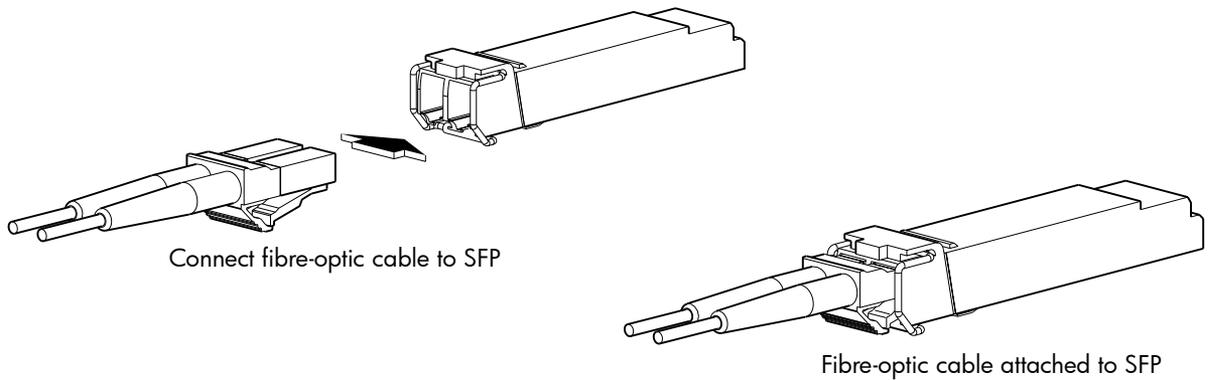


Figure 20 Connect fibre-optic interface cable to SFP

Verifying component operation

View the Link Status and Link Activity LEDs on the controller module face plate. A blinking LED indicates that no link is detected. Also check the link status and link activity LEDs on the host.

Replacing a controller enclosure chassis

The controller enclosure chassis replacement procedure replaces a damaged chassis FRU, which consists of the structural support metal, the exterior sheet metal housing, and the assembled/installed midplane. The procedure includes removing all FRU components from a damaged chassis and installing them in a replacement chassis.

NOTE: AssuredSAN 2U24 and 2U12 controller enclosure chassis models are described in [FRUs addressing 24-drive enclosures](#) on page 208 and [FRUs addressing 12-drive enclosures](#) on page 211.

Whether your controller enclosure product is a 2U24 or 2U12 model, a fully functional replacement chassis requires the successful removal and installation of the following components:

- All disk drive modules and air management modules
- Two ear bezels (for left and right ears)
Some models use an enclosure bezel instead of left and right ear covers
- Two PSUs of the same type (both AC or both DC)
- One or two controller modules (of the same model type)

Certain models also require the successful removal and installation of FC transceiver (SFP for 4720/4730 models).

Before you begin

Ensure you take proper precautions against static electricity. See [ESD](#) on page 103.

△ **CAUTION:** Do not remove the enclosure until you have received the replacement enclosure.

1. Schedule down time that will allow for shutdown, sixty minutes of replacement work, and restart.
2. Verify the existence of a known good backup of the system.
3. Record system settings for future use.
4. Label all cables.
5. Prepare a suitable work environment to accommodate chassis replacement.

Verifying component failure

The controller enclosure FRU includes the enclosure's metal housing and the midplane that connects controller modules, disk drive modules, and PSUs. This FRU replaces an enclosure that has been damaged, or whose midplane has been damaged.

Often times, a damaged midplane will appear as though a controller module has failed. If you replace a controller module, and it does not remedy the fault, you may need to replace the enclosure.

Alternatively, you can observe enclosure health (front panel and rear panel) using management interfaces to verify enclosure/component failure or enclosure/component operation (see [Using management interfaces](#) on page 142 for more information).

If necessary, use the CLI `set led` command to illuminate the enclosure locator LED.

Preparing to remove a damaged storage enclosure chassis

Since you are removing and replacing an entire controller enclosure, neither the hot-swap capability that applies to replacing individual redundant FRUs in an operational controller enclosure, nor the hot-add of a drive enclosure to an operational storage system, apply to this procedure.

1. Stop all I/O from hosts to the system. See [Stopping I/O](#) on page 106.
2. Shut down the controller(s). See [Shutting down a controller module](#) on page 106.
3. Power off the system (controller enclosure first, drive enclosure(s) next). See [PSUs on page 129](#) and refer to the power cycling procedures pertaining to your enclosure's PSUs.

Table 24 Removing and replacing a controller enclosure chassis and its FRUs

To accomplish this sequential process	See the following procedures
1. Remove disk drive modules and air management modules from the damaged chassis. ¹	<ol style="list-style-type: none">a. Air management modules on page 121.b. Before you begin on page 121.c. Removing a disk drive module on page 122.
2. Remove the ear bezels from the damaged chassis.	<ol style="list-style-type: none">a. Before you begin on page 135b. Removing the ear bezels on page 136
3. Remove the damaged storage enclosure chassis from the rack.	Removing a damaged storage enclosure chassis from the rack on page 141 .
4. Remove the PSUs from the damaged chassis, and install them in the replacement chassis.	<ol style="list-style-type: none">a. Before you begin on page 128.b. PSUs on page 129.c. Removing a PSU on page 131.d. Installing a PSU on page 132.
5. Remove each IOM from the damaged chassis, and install each in the replacement chassis. ²	<ol style="list-style-type: none">a. Before you begin on page 105.b. Removing a controller module or expansion module on page 107.c. Installing a controller module or expansion module on page 108.
6. Remove each FC transceiver from the damaged chassis, and install each in the replacement chassis (FC models only). ³	<ol style="list-style-type: none">a. Before you begin on page 137.b. Removing an SFP module on page 138.c. Installing an SFP module on page 138.
7. Install the ear bezels on the replacement chassis.	Installing the ear bezels on page 137
8. Install the replacement storage enclosure chassis in the rack.	Installing the replacement storage enclosure chassis in the rack on page 141 .
9. Install disk drive modules and air management module in the replacement chassis. ¹	Installing a disk drive module on page 123 .

Table 24 Removing and replacing a controller enclosure chassis and its FRUs (continued)

To accomplish this sequential process	See the following procedures
10. Complete the installation process.	<ul style="list-style-type: none">a. Connecting a power cable on page 133.b. Completing the process on page 142.
11. Verify proper operation for all removed and installed FRU components.	<ul style="list-style-type: none">a. Disks—Verifying component operation on page 125.b. Controller module(s)—Verifying component operation on page 110.c. PSUs—Verifying component operation on page 134.d. SFPs (if applicable)—Verifying component operation on page 139.e. Verify PFU enabled (if applicable)—Configuring PFU on page 105.

¹Within the replacement enclosure, reinstall each disk drive or disk drive blank into the same disk slot from which it was removed from the damaged enclosure.

²Within the replacement enclosure, the IOM(s) and IOM blank — if applicable — must be reinstalled into the same IOM slots from which they were extracted in the damaged enclosure.

³If your enclosure model does not support SFP connectors, ignore this step.

Removing a damaged storage enclosure chassis from the rack

Perform the following procedure to remove a damaged controller enclosure chassis from its rack location.

△ **CAUTION:** It is recommended that all disk drive modules and air management modules be removed before removing the enclosure. See [Removing a disk drive module on page 122](#).

If this is not possible, two people are required to move the enclosure.

-
1. Make sure the ear bezels are removed. See [Removing the ear bezels on page 136](#).
 2. Remove the retaining screws that secure the front and rear of the controller enclosure chassis to the rack and rails.
 3. Carefully slide the controller enclosure chassis from the rack.
 4. Place the chassis on a work surface near the replacement controller enclosure chassis, the removed disk drive modules, ear bezel components, and screws.
 5. Remove the side bracket from each side of the damaged controller enclosure chassis.
 6. Attach the side bracket to each side of the replacement controller enclosure chassis.

Installing the replacement storage enclosure chassis in the rack

Perform the following procedure to install the replacement controller enclosure chassis in its rack location.

△ **CAUTION:** It is recommended that all disk drive modules and air management modules be removed before lifting the enclosure. See [Removing a disk drive module on page 122](#).

If this is not possible, two people are required to move the enclosure.

 **NOTE:** Refer to the *AssuredSAN Rackmount Bracket Kit Installation* instructions or the *AssuredSAN 2-Post Rackmount Bracket Kit Installation* instructions for the correct installation procedure and mounting hardware.

1. Attach side brackets (standard rackmount installation) or main brackets (2-post rackmount installation) on the replacement controller enclosure chassis.
2. Support the bottom of the controller enclosure chassis. Carefully lift/align the chassis and slide it into the rack.
3. Using the appropriate mounting hardware, secure the controller enclosure chassis to the rack.
4. Install the ear bezels. [Installing the ear bezels on page 137](#)
5. Using the applicable retaining screws, secure the front and rear of the controller enclosure chassis to the rack and rails.

Completing the process

This section provides a procedure for ensuring that the FRU components installed in the replacement controller enclosure chassis function properly.

1. Reconnect data cables between devices, as needed, to return to the original cabling configuration:
 - Between cascaded enclosures.
 - Between the controller and peripheral or SAN devices.
 - Between the controller enclosure and the host.
2. Reconnect power cables to the controller enclosure. See [Connecting a power cable on page 133](#).
3. Turn on the power switch to PSUs if they are equipped with power switches.

 **NOTE:** For powering-on AC PSUs with or without a power switch, and DC and AC PSUs with a power switch, see [PSUs on page 129](#).

Verifying component operation

Restart system devices in the following sequence. Allow time for each device to complete its POST before proceeding:

1. Disk drive enclosures
2. Controller enclosure
3. Host (if powered down for maintenance)

Using LEDs

View LEDs on the front and rear of the enclosure (see [Troubleshooting using system LEDs](#)).

Verify front panel LEDs:

- Verify that the Enclosure ID LED (located on the left ear) is illuminated green.
- Verify that the FRU OK and Temperature Fault LEDs are illuminated green, and that the Fault/Service Required LED is off (all three LEDs are located on the right ear).
- For LFF disks, verify that the Power/Activity LED (top LED on front of disk) is illuminated green or blinking green (If your product model has an enclosure bezel, remove it to view disk LEDs).
- For SFF disks, verify that the Power/Activity LED (left LED on front of disk) is illuminated green or blinking green (If your product model has an enclosure bezel, remove it to view disk LEDs).

Verify rear panel LEDs:

- Verify that the each PSU's Input Source Power Good LED (top LED on PSU) is illuminated green.
- Verify that the FRU OK LED on each IOM face plate is illuminated green, indicating that the module has completed initializing, and is online.

Using management interfaces

In addition to viewing LEDs as described above, you can use management interfaces to monitor the health status of the system and its components, provided you have configured and provisioned the system (see "Getting Started" within the *AssuredSAN 4000 Series RAIDar User Guide* for more information).

Select from the following methods to verify component operation:

- Use RAIDar to check the health icons/values of the system and its components to either ensure that everything is okay, or to drill down to a problem component. RAIDar uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. If you discover a problem component, follow the actions in its Health Recommendations field to resolve the problem.
- As an alternative to using RAIDar, you can run the `show system` command in the CLI to view the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. If you discover a problem component, follow the actions in its Health Recommendations field to resolve the problem.
- Monitor event notification. With event notification configured and enabled, you can view event logs to monitor the health of the system and its components. If a message tells you to check whether an event has been logged, or to view information about an event in the log, you can do so using either RAIDar or the CLI. Using RAIDar, you would view the event log and then click on the event message to see detail about that event. Using the CLI, you would run the `show events detail` command (with additional parameters to filter the output) to see the detail for an event (see [show events](#) on page 63 for more information about command syntax and parameters).

7 Voltage and temperature warnings

The storage system provides voltage and temperature warnings, which are generally input or environmental conditions. Voltage warnings can occur if the input voltage is too low, or if a FRU is receiving too little or too much power from the PSU. Temperature warnings are generally the result of a fan failure, a FRU being removed from an enclosure for a lengthy time period, or a high ambient temperature around an enclosure.

This chapter describes the steps to take to resolve voltage and temperature warnings and provides information about the PSU, cooling fan, temperature and voltage sensor locations, and alarm conditions.

Resolving voltage and temperature warnings

1. Check that all of the fans are working by making sure the Voltage/Fan Fault/Service Required LED on each PSU is off, or by using RAIDar to check enclosure health status. In the Configuration View panel, right click the enclosure and click **View > Overview** to view the health status of the enclosure and its components.

See on page 19 for a description of health status icons and alternatives for monitoring enclosure health.

2. Make sure that all modules are fully seated in their slots and that their latches are locked.
3. Make sure that no slots are left open for more than two minutes.

If you need to replace a module, leave the old module in place until you have the replacement or use a blank module to fill the slot. Leaving a slot open negatively affects the airflow and can cause the enclosure to overheat.

4. Replace each PSU one at a time.
5. Replace the controller modules one at a time.

Sensors

The storage system monitors conditions at different points within each enclosure to alert you to problems. Power, cooling fan, temperature, and voltage sensors are located at key points in the enclosure. In each controller module and expansion module, the EMP monitors the status of these sensors to perform SES functions.

The following sections describe each element and its sensors.

PSU sensors

Each enclosure has two fully redundant power supplies with load-sharing capabilities. The PSU sensors described in [Table 25](#) monitor the voltage, current, temperature, and fans in each PSU. If the PSU sensors report a voltage that is under or over the threshold, check the input voltage.

Table 25 PSU sensor descriptions

Description	Event/Fault ID LED condition
PSU 1	Voltage, current, temperature, or fan fault
PSU 2	Voltage, current, temperature, or fan fault

Cooling fan sensors

Each PSU includes two fans. The normal range for fan speed is 4,000 to 6,000 r/min. When a fan speed drops below 4,000 r/min, the EMP considers it a failure and posts an alarm in the storage system's event log. [Table 26](#) lists the description, location, and alarm condition for each fan. If the fan speed remains under the 4,000 r/min threshold, the internal enclosure temperature may continue to rise. Replace the PSU reporting the fault.

Table 26 Cooling fan sensor descriptions

Description	Location	Event/Fault ID LED condition
Fan 1	PSU 1	< 4,000 r/min
Fan 2	PSU 1	< 4,000 r/min
Fan 3	PSU 2	< 4,000 r/min
Fan 4	PSU 2	< 4,000 r/min

During a shutdown, the cooling fans do not shut off. This allows the enclosure to continue cooling.

Temperature sensors

Extreme high and low temperatures can cause significant damage if they go unnoticed. Each controller module has six temperature sensors. Of these, if the CPU or FPGA temperature reaches a shutdown value, the controller module is automatically shut down. Each PSU has one temperature sensor.

When a temperature fault is reported, it must be remedied as quickly as possible to avoid system damage. This can be done by warming or cooling the installation location.

Table 27 Controller module temperature sensor descriptions

Description	Normal operating range	Warning operating range	Critical operating range	Shutdown values
CPU temperature	3°C – 88°C	0°C – 3°C, 88°C – 90°C	> 90°C	0°C 100°C
FPGA temperature	3°C – 97°C	0°C – 3°C, 97°C – 100°C	None	0°C 105°C
Onboard temperature 1	0°C – 70°C	None	None	None
Onboard temperature 2	0°C – 70°C	None	None	None
Onboard temperature 3 (Capacitor temperature)	0°C – 70°C	None	None	None
CM temperature	5°C – 50°C	≤ 5°C, ≥ 50°C	≤ 0°C, ≥ 55°C	None

When a PSU sensor goes out of range, the Fault/ID LED illuminates amber and an event is posted to the event log.

Table 28 PSU temperature sensor descriptions

Description	Normal operating range
PSU 1 temperature	–10°C – 80°C
PSU 2 temperature	–10°C – 80°C

PSU voltage sensors

PSU voltage sensors ensure that an enclosure's PSU voltage is within normal ranges. There are three voltage sensors per PSU.

Table 29 Voltage sensor descriptions

Sensor	Event/Fault LED condition
PSU 1 voltage, 12V	< 11.00V > 13.00V
PSU 1 voltage, 5V	< 4.00V > 6.00V
PSU 1 voltage, 3.3V	< 3.00V > 3.80V

A Event descriptions

Introduction

This appendix is for reference by storage administrators and technical support personnel to help troubleshoot storage-system issues. It describes event messages that may be reported during system operation and specifies any actions recommended in response to an event.

Events and event messages

When an event occurs in a storage system, an event message is recorded in the system's event log and, depending on the system's event notification settings, may also be sent to users (using email) and host-based applications (via SNMP or SMI-S).

Each event has a numeric code that identifies the type of event that occurred, and has one of the following severities:

- **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 immediate action is required. In this appendix, this severity is abbreviated as "Info."

An event message may specify an associated error code or reason code, which provides additional detail for technical support. Error codes and reason codes are outside the scope of this appendix.

Event format in this appendix

This appendix lists events by event code and severity, where the most severe form of an event is described first. Events are listed in the following format.

Event code

Severity Event description.

Recommended actions

- If the event indicates a problem, actions to take to resolve the problem.

Resources for diagnosing and resolving problems

For further information about diagnosing and resolving problems, see:

- 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
- For a summary of storage events and corresponding SMI-S indications, see [Events sent as indications to SMI-S clients](#) on page 195.

Event descriptions

1

Warning If the indicated vdisk is RAID 6, it is operating with degraded health due to the failure of two disks.

If the indicated vdisk is not RAID 6, it is operating with degraded health due to the failure of one disk. The vdisk is online but cannot tolerate another disk failure.

If a dedicated or global spare of the proper type and size is present, that spare is used to automatically reconstruct the vdisk; events 9 and 37 are logged to indicate this. If no usable spare disk is present, but an available disk of the proper type and size is present and the dynamic spares feature is enabled, that disk is used to automatically reconstruct the vdisk; event 37 is logged.

Recommended actions

- If no spare was present and the dynamic spares feature is disabled (that is, event 37 was *not* logged), configure an available disk as a dedicated spare for the vdisk or replace the failed disk and configure the new disk as a dedicated spare for the vdisk. That spare will be used to automatically reconstruct the vdisk; confirm this by checking that events 9 and 37 are logged.
- Otherwise, reconstruction automatically started and event 37 was logged. Replace the failed disk and configure the replacement as a dedicated or global spare for future use.
- If the replacement disk was previously used in another vdisk and has a status of leftover (LEFTOVR), clear the disk's metadata so you can assign the disk as a spare.
- Confirm that all failed disks have been replaced and that there are sufficient spare disks configured for future use.

3

Error The indicated vdisk went offline.

One disk failed for RAID 0 or NRAID, three disks failed for RAID 6, or two disks failed for other RAID levels. The vdisk cannot be reconstructed.

Recommended actions

- Replace the failed disk or disks. (Look for event 8 in the event log to determine which disks failed and for advice on replacing them.)
- Delete the vdisk (`delete vdisks` CLI command).
- Recreate the vdisk (`create vdisk` CLI command).
- To prevent this problem in the future, use a fault-tolerant RAID level, configure one or more disks as spare disks, and replace failed disks promptly.

4

Info. The indicated disk had an uncorrectable error and the controller reassigned the indicated block.

Recommended actions

- Monitor the error trend and whether the number of errors approaches the total number of bad-block replacements available.

6

Warning A failure occurred during initialization of the indicated vdisk. This was probably caused by the failure of a disk drive. The initialization may have completed but the vdisk is probably in a state of FTDN (fault tolerant with a down disk), CRIT (critical), or OFFL (offline), depending on the RAID level and the number of disks that failed.

Recommended actions

- Look for another event logged at approximately the same time that indicates a disk failure, such as event 55, 58, or 412. Follow the recommended actions for that event.

Info. Vdisk creation failed immediately. The user was given immediate feedback that it failed at the time they attempted to create the vdisk.

Recommended actions

- No action is required.

7

Error In a testing environment, a controller diagnostic failed and reports a product-specific diagnostic code.

Recommended actions

- Perform failure analysis.

8

Warning The indicated disk in the indicated vdisk failed and the vdisk has a status of FTDN (fault tolerant with a down disk), CRIT (critical), or OFFL (offline), depending on the RAID level and the number of disks that failed. If a spare is present and the vdisk is not offline, the controller automatically uses the spare to reconstruct the vdisk. Subsequent events indicate the changes that happen to the vdisk.

When the problem is resolved, event 9 is logged.

Recommended actions

Table 30 Disk error conditions and recommended actions

Condition	Recommended action
Excessive media errors.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
Disk failure is imminent.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
The disk has a possible hardware failure.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
The disk is not supported.	Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
A user forced the disk out of the vdisk.	If the associated vdisk is offline or quarantined, contact technical support; otherwise, clear the disk's metadata to reuse the disk.

Table 30 Disk error conditions and recommended actions (continued)

Condition	Recommended action
A previously detected disk is no longer present.	Reinsert the disk or insert a replacement disk of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity as the one that was in the slot. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. If the disk then has a status of leftover (LEFTOVR), clear the metadata to reuse the disk. If the associated vdisk is offline or quarantined, contact technical support.
Unknown reason	If the associated vdisk is offline or quarantined, contact technical support; otherwise, clear the disk's metadata to reuse the disk.

9

Info. The indicated spare disk has been used in the indicated vdisk to bring it back to a fault-tolerant status. Vdisk reconstruction starts automatically. This event indicates that a problem reported by event 8 is resolved.

Recommended actions

- No action is required.

16

Info. The indicated disk has been designated a global spare.

Recommended actions

- No action is required.

18

Warning Vdisk reconstruction failed.

Recommended actions

- Determine whether the reconstruction failed due to a disk failure and whether replacing that disk will enable reconstruction to start and complete without further errors. To determine this, look for another event logged at approximately the same time that indicates a disk failure, such as event 55, 58, or 412. Follow the recommended actions for that event.

Info. Vdisk reconstruction completed.

Recommended actions

- If the event message indicates that one or more uncorrectable media errors occurred during the reconstruction, some user data may have been lost. Use backup copies of the data or other means to restore any lost data.
- Otherwise, no action is required.

19

Info. A rescan has completed.

Recommended actions

- No action is required.

20

Info. Storage Controller firmware update has completed.

Recommended actions

- No action is required.

21

Error Vdisk verification completed. Errors were found but not corrected.

Recommended actions

- Perform a vdisk scrub to find and correct the errors.

Warning Vdisk verification did not complete because of an internally detected condition such as a failed disk.

If a disk fails, data may be at risk.

Recommended actions

- Resolve any non-disk hardware problems, such as a cooling problem or a faulty controller module, expansion module, or power supply.
- Check whether any disks in the vdisk have logged SMART events or unrecoverable read errors.
 - If so, and the vdisk is a non-fault-tolerant RAID level (RAID 0 or non-RAID), copy the data to a different vdisk and replace the faulty disks.
 - If so, and the vdisk is a fault-tolerant RAID level, replace the faulty disks. Before replacing a disk, confirm that a reconstruction is not currently running on the vdisk. It is also recommended to make a full backup of all the data in the vdisk before replacing disks. If more than one disk in the vdisk has errors, replace the disks one at a time and allow reconstruction to complete after each disk is replaced.

Info. Vdisk verification failed immediately, was aborted by a user, or succeeded.

- No action is required.

23

Info. Vdisk creation has started.

Recommended actions

- No action is required.

25

Info. The statistics for the indicated vdisk have been reset.

Recommended actions

- No action is required.

27

Info. Cache parameters have been changed for the indicated vdisk.

Recommended actions

- No action is required.

28

Info. Controller parameters have been changed.

This event is logged when general configuration changes are made; for example, utility priority, remote notification settings, user interface passwords, and network port IP values. This event is *not* logged when changes are made to vdisk or volume configuration.

Recommended actions

- No action is required.

31

Info. The indicated disk is no longer a global or dedicated spare.

Recommended actions

- No action is required.

32

Info. Vdisk verification has started.

Recommended actions

- No action is required.

33

Info. Controller time/date has been changed.

This event is logged before the change happens, so the timestamp of the event shows the old time. This event may occur often if NTP is enabled

Recommended actions

- No action is required.

34

Info. The controller configuration has been restored to factory defaults.

Recommended actions

- For an FC controller, restart it to make the default loop ID take effect.

37

Info. Vdisk reconstruction has started.

When complete, event 18 is logged.

Recommended actions

- No action is required.

39

Warning The sensors monitored a temperature or voltage in the warning range.

Recommended actions

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5–40° C (41° F–104° F).
- Check for any obstructions to the airflow.
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that reported the error.

When the problem is fixed, event 47 is logged.

40

Error The sensors monitored a temperature or voltage in the failure range.

Recommended actions

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5–40° C (41° F–104° F).
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that reported the error.

When the problem is fixed, event 47 is logged.

41

Info. A dedicated spare has been added.

Recommended actions

- No action is required.

43

Info. The indicated disk has been designated a spare for the indicated vdisk.

Recommended actions

- No action is required.

44

Warning The controller contains cache data for the indicated volume but the corresponding vdisk is not online.

Recommended actions

- Determine the reason why the disks comprising the vdisk are not online.
- If an enclosure is down, determine corrective action.
- If the vdisk is no longer needed, you can clear the orphan data; this will result in lost data.
- If the vdisk is missing and was not intentionally removed, see “Resources for diagnosing and resolving problems” in the WBI help for the event log panel, or the CLI help for the `show events` command.

47

Info. An error detected by the sensors has been cleared. This event indicates that a problem reported by event 39 or 40 is resolved.

Recommended actions

- No action is required.

48

Info. The indicated vdisk has been renamed.

Recommended actions

- No action is required.

49

Info. A lengthy SCSI maintenance command has completed. (This typically occurs during disk firmware update.)

Recommended actions

- No action is required.

50

Warning A correctable ECC error occurred in cache memory.

Recommended actions

- If this event occurs more than 10 times during any 24-hour period, replace the controller module that logged the events.

51

Error An uncorrectable ECC error occurred in cache memory.

Recommended actions

- If this event occurs more than once for the same controller module, replace the controller module.

52

Info. Vdisk expansion has started.

This operation can take days, or weeks in some cases, to complete. Allow adequate time for the expansion to complete.

When complete, event 53 is logged.

Recommended actions

- No action is required.

53

Warning Too many errors occurred during vdisk expansion to allow the expansion to continue.

Recommended actions

- If the expansion failed because of a disk problem, replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. If vdisk reconstruction starts, wait for it to complete and then retry the expansion.

Info. Vdisk expansion either completed successfully, failed immediately, or was aborted by a user.

Recommended actions

- If the expansion failed because of a disk problem, replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. If vdisk reconstruction starts, wait for it to complete and then retry the expansion.

55

Warning The indicated disk reported a SMART event.

A SMART event indicates impending disk failure.

Recommended actions

- Resolve any non-disk hardware problems, especially a cooling problem or a faulty power supply.
- If the disk is in a vdisk that uses a non-fault-tolerant RAID level (RAID 0 or non-RAID), copy the data to a different vdisk and replace the faulty disk.
- If the disk is in a vdisk that uses a fault-tolerant RAID level, replace the faulty disk. Before replacing the disk, confirm that a reconstruction is not currently running on the vdisk. It is also recommended to make a full backup of all the data in the vdisk before replacing disks. If more than one disk in the vdisk has reported SMART events, replace the disks one at a time and allow reconstruction to complete after each disk is replaced.

56

Info. A controller has powered up or restarted.

Recommended actions

- No action is required.

58

Error A disk drive detected a serious error, such as a parity error or disk hardware failure.

Recommended actions

- Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.

Warning A disk drive reset itself due to an internal logic error.

Recommended actions

- The first time this event is logged with Warning severity, if the indicated disk is not running the latest firmware, update the disk firmware.
- If this event is logged with Warning severity for the same disk more than five times in one week, and the indicated disk is running the latest firmware, replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one

Info. A disk drive reported an event.

Recommended actions

- No action is required.

59

Warning The controller detected a parity event while communicating with the indicated SCSI device. The event was detected by the controller, not the disk.

Recommended actions

- If the event indicates that a disk or an expansion module is bad, replace the indicated device.

Info. The controller detected a non-parity error while communicating with the indicated SCSI device. The error was detected by the controller, not the disk.

Recommended actions

- No action is required.

61

Error The controller reset a disk channel to recover from a communication error. This event is logged to identify an error trend over time.

Recommended actions

- If the controller recovers, no action is required.
- View other logged events to determine other action to take.

62

Warning The indicated global or dedicated spare disk has failed.

Recommended actions

- Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
- If the failed disk was a global spare, configure the new disk as a global spare.
- If the failed disk was a dedicated spare, configure the new disk as a dedicated spare for the same vdisk.

65

Error An uncorrectable ECC error occurred in cache memory on startup.

The controller is automatically restarted and its cache data is restored from the partner controller's cache.

Recommended actions

- Replace the controller module that logged this event.

67

Info. The controller has identified a new disk or group of disks that constitute a vdisk and has taken ownership of the vdisk. This can happen when disks containing data have been inserted from another enclosure. This event only applies to non-Active-Active controllers.

Recommended actions

- You may need to clear the disks' metadata if you want to reuse them in one or more new vdisks.

68

Info. The controller that logged this event is shut down, or both controllers are shut down.

Recommended actions

- No action is required.

71

Info. The controller has started or completed failing over.

Recommended actions

- No action is required.

72

Info. After failover, recovery has either started or completed.

Recommended actions

- No action is required.

73

Info. The two controllers are communicating with each other and cache redundancy is enabled.

Recommended actions

- No action is required.

74

Info. The FC loop ID for the indicated vdisk was changed to be consistent with the IDs of other vdisks. This can occur when disks containing a vdisk are inserted from an enclosure having a different FC loop ID.

This event is also logged by the new owning controller after vdisk ownership is changed.

Recommended actions

- No action is required.

75

Info. The indicated volume's LUN has been unassigned because it conflicts with LUNs assigned to other volumes. This can happen when disks containing data for a mapped volume have been moved from one storage system to another.

Recommended actions

- If you want hosts to access the volume data in the inserted disks, map the volume with a different LUN.

76

Info. The controller is using default configuration settings. This event occurs on the first power up, and might occur after a firmware update.

Recommended actions

- If you have just performed a firmware update and your system requires special configuration settings, you must make those configuration changes before your system will operate as before.

77

Info. The cache was initialized as a result of power up or failover.

Recommended actions

- No action is required.

78

Warning This occurs when a disk in a vdisk fails and there is no dedicated spare available and all global spares are too small or, if the dynamic spares feature is enabled, all global spares and available disks are too small, or if there is no spare of the correct type. There may be more than one failed disk in the system.

Recommended actions

- Replace each failed disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.
- Configure disks as dedicated spares or global spares.
 - For a dedicated spare, the disk must be of the same type as the other disks in the vdisk and at least as large as the smallest-capacity disk in the vdisk, and it should have the same or better performance.
 - For a global spare, it is best to choose a disk that is as big as or bigger than the largest disk of its type in the system and of equal or greater performance. If the system contains a mix of disk types (SAS SSD, enterprise SAS, or midline SAS), there should be at least one global spare of each type (unless dedicated spares are used to protect every vdisk of a given type).

79

Info. A trust operation has completed for the indicated vdisk.

Recommended actions

- Be sure to complete the trust procedure as documented in the CLI help for the `trust` command.

80

Info. The controller enabled or disabled the indicated parameters for one or more disks.

Recommended actions

- No action is required.

81

Info. The current controller has unkilld the partner controller. The other controller will restart.

Recommended actions

- No action is required.

83

Info. The partner controller is changing state (shutting down or restarting).

Recommended actions

- No action is required.

84

Warning The controller that logged this event forced the partner controller to fail over.

Recommended actions

- Download the debug logs from your storage system and contact technical support. A service technician can use the debug logs to determine the problem.

86

Info. Host-port or disk-channel parameters have been changed.

Recommended actions

- No action is required.

87

Warning The mirrored configuration retrieved by this controller from the partner controller has a bad cyclic redundancy check (CRC). The local flash configuration will be used instead.

Recommended actions

- Restore the default configuration by using the `restore defaults` command, as described in the CLI Reference Guide.

88

Warning The mirrored configuration retrieved by this controller from the partner controller is corrupt. The local flash configuration will be used instead.

Recommended actions

- Restore the default configuration by using the `restore defaults` command, as described in the CLI Reference Guide.

89

Warning The mirrored configuration retrieved by this controller from the partner controller has a configuration level that is too high for the firmware in this controller to process.

Recommended actions

- The controller that logged this event probably has down-level firmware. Update the firmware on the down-level controller. Both controllers should have the same firmware versions.

When the problem is resolved, event 20 is logged.

90

Info. The partner controller does not have a mirrored configuration image for the current controller, so the current controller's local flash configuration is being used.

This event is expected if the other controller is new or its configuration has been changed.

Recommended actions

- No action is required.

91

Error In a testing environment, the diagnostic that checks hardware reset signals between controllers in Active-Active mode failed.

Recommended actions

- Perform failure analysis.

95

Error Both controllers in an Active-Active configuration have the same serial number. Non-unique serial numbers can cause system problems; for example, WWNs are determined by serial number.

Recommended actions

- Remove one of the controller modules and insert a replacement, then return the removed module to be reprogrammed.

96

Info. Pending configuration changes that take effect at startup were ignored because customer data might be present in cache.

Recommended actions

- If the requested configuration changes did not occur, make the changes again and then use a user-interface command to shut down or restart the controller.

103

Info. The name has been changed for the indicated volume.

Recommended actions

- No action is required.

104

Info. The size has been changed for the indicated volume.

Recommended actions

- No action is required.

105

Info. The LUN (logical unit number) has been changed for the indicated volume.

Recommended actions

- No action is required.

106

Info. The indicated volume has been added to the indicated vdisk.

Recommended actions

- No action is required.

107

Error A serious error has been detected by the controller. In a single-controller configuration, the controller will restart automatically. In an Active-Active configuration, the partner controller will kill the controller that experienced the error.

Recommended actions

- Download the debug logs from your storage system and contact technical support. A service technician can use the debug logs to determine the problem.

108

Info. The indicated volume has been deleted from the indicated vdisk.

Recommended actions

- No action is required.

109

Info. The statistics for the indicated volume have been reset.

Recommended actions

- No action is required.

110

Info. Ownership of the indicated vdisk has been given to the other controller.

Recommended actions

- No action is required.

111

Info. The link for the indicated host port is up.

This event indicates that a problem reported by event 112 is resolved. For a system with FC ports, this event also appears after loop initialization.

Recommended actions

- No action is required.

112

Warning The link for the indicated host port has unexpectedly gone down.

Recommended actions

- Look for corresponding event 111 and monitor excessive transitions. If this event occurs more than 8 times per hour, it should be investigated.
- This event is probably caused by equipment outside of the storage system, such as faulty cabling or a faulty switch.
- If the problem is not outside of the storage system, replace the controller module that logged this event.

Info. The link for the indicated host port has gone down because the controller is starting up.

Recommended actions

- No action is required.

114

Info. The link for the indicated disk-channel port is down. Note that events 114 and 211 are logged whenever a user-requested rescan occurs and do not indicate an error.

Recommended actions

- Look for corresponding event 211 and monitor excessive transitions indicating disk problems. If more than 8 transitions occur per hour, see “Resources for diagnosing and resolving problems” in the WBI help for the event log panel, or the CLI help for the `show events` command.

116

Error After a recovery, the partner controller was killed while mirroring write-back cache data to the current controller that logged this event. The controller that logged this event restarted to avoid losing the data in the partner controller’s cache, but if the other controller does not restart successfully, the data will be lost.

Recommended actions

- To determine if data might have been lost, check whether this event was immediately followed by event 56 (Storage Controller booted up), closely followed by event 71 (failover started); the failover indicates that the restart did not succeed.

118

Info. Cache parameters have been changed for the indicated volume.

Recommended actions

- No action is required.

127

Warning The controller has detected an invalid disk dual-port connection. This event indicates that a controller host port is connected to an expansion port instead of to a port on a host or a switch.

Recommended actions

- Disconnect the host port and expansion port from each other and connect them to the proper devices.

136

Warning Errors detected on the indicated disk channel have caused the controller to mark the channel as degraded.

Recommended actions

- Determine the source of the errors on the indicated disk channel and replace the faulty hardware.

When the problem is resolved, event 189 is logged.

139

Info. The Management Controller (MC) has powered up or restarted.

Recommended actions

- No action is required.

140

Info. The Management Controller (MC) is about to restart.

Recommended actions

- No action is required.

141

Info. This event is logged when the IP address used for management of the system has been changed by a user or by a DHCP server (if DHCP is enabled). This event is also logged during power up or failover recovery, even when the address has not changed.

Recommended actions

- No action is required.

152

Warning The Management Controller (MC) has not communicated with the Storage Controller (SC) for 15 minutes and may have failed.

This event is initially logged as Informational severity. If the problem persists, this event is logged a second time as Warning severity and the MC is automatically restarted in an attempt to recover from the problem. Event 156 is then logged.

Recommended actions

- If this event is logged only one time as Warning severity, no action is required.
- If this event is logged more than one time as Warning severity, do the following:
 - If you are now able to access the management interfaces of the controller that logged this event, do the following:
 - Check the version of the controller firmware and update to the latest firmware if needed.
 - If the latest firmware is already installed, the controller module that logged this event probably has a hardware fault. Replace the module.
 - If you are *not* able to access the management interfaces of the controller that logged this event, do the following:
 - Shut down that controller and reseal the module.
 - If you are then able to access the management interfaces, check the version of the controller firmware and update to the latest firmware if needed.
 - If the problem recurs, replace the module.

Info. The Management Controller (MC) has not communicated with the Storage Controller (SC) for 160 seconds. If communication is restored in less than 15 minutes, event 153 is logged. If the problem persists, this event is logged a second time as Warning severity.

 **NOTE:** It is normal for this event to be logged as Informational severity during firmware update.

Recommended actions

- Check the version of the controller firmware and update to the latest firmware if needed.
- If the latest firmware is already installed, no action is required.

153

Info. The Management Controller (MC) has re-established communication with the Storage Controller (SC).

Recommended actions

- No action is required.

154

Info. New firmware has been loaded in the Management Controller (MC).

Recommended actions

- No action is required.

155

Info. New loader firmware has been loaded in the Management Controller (MC).

Recommended actions

- No action is required.

156

Warning The Management Controller (MC) has been restarted from the Storage Controller (SC) for the purpose of error recovery.

Recommended actions

- See the recommended actions for event 152, which is logged at approximately the same time.

Info. The Management Controller (MC) has been restarted from the Storage Controller (SC) in a normal case, such as when initiated by a user.

Recommended actions

- No action is required.

157

Error A failure occurred when trying to write to the Storage Controller (SC) flash chip.

Recommended actions

- Replace the controller module that logged this event.

158

Warning A correctable ECC error occurred in Storage Controller CPU memory.

Recommended actions

- If this event occurs more than once during any 12-hour period, replace the controller module that logged the events.

161

Info. One or more enclosures do not have a valid path to an enclosure management processor (EMP).

All enclosure EMPs are disabled.

Recommended actions

- Download the debug logs from your storage system and contact technical support. A service technician can use the debug logs to determine the problem.

162

Warning The host WWNs (node and port) previously presented by this controller module are unknown. In a dual-controller system this event has two possible causes:

- One or both controller modules have been replaced or moved while the system was powered off.
- One or both controller modules have had their flash configuration cleared (this is where the previously used WWNs are stored).

The controller module recovers from this situation by generating a WWN based on its own serial number.

Recommended actions

- If the controller was replaced or someone reprogrammed its FRU ID data, verify the WWN information for this controller module on all hosts that access it.

163

Warning The host WWNs (node and port) previously presented by the partner controller module, which is currently offline, are unknown.

This event has two possible causes:

- The online controller module reporting the event was replaced or moved while the system was powered off.
- The online controller module had its flash configuration (where previously used WWNs are stored) cleared.

The online controller module recovers from this situation by generating a WWN based on its own serial number for the other controller module.

Recommended actions

- If the controller was replaced or someone reprogrammed its FRU ID data, verify the WWN information for the other controller module on all hosts that access it.

166

Warning The RAID metadata level of the two controllers does not match, which indicates that the controllers have different firmware levels.

Usually, the controller at the higher firmware level can read metadata written by a controller at a lower firmware level. The reverse is typically not true. Therefore, if the controller at the higher firmware level failed, the surviving controller at the lower firmware level cannot read the metadata on disks that have failed over.

Recommended actions

- If this occurs after a firmware update, it indicates that the metadata format changed, which is rare. Update the controller with the lower firmware level to match the firmware level in the other controller.

167

Warning A diagnostic test at controller bootup detected an abnormal operation, which might require a power cycle to correct.

Recommended actions

- Download the debug logs from your storage system and contact technical support. A service technician can use the debug logs to determine the problem.

168

Error The indicated SES alert condition was detected in the indicated enclosure. This event is logged as Error severity when one of the power supplies in an enclosure has no power supplied to it or when a hardware failure is detected.

Recommended actions

- Check that all modules in the enclosure are properly seated in their slots and that their latches are locked.
- If the reported problem is with a power supply, perform these checks:
 - Check that each power supply module has its switch turned on (if equipped with a switch).
 - Check that each power cable is firmly plugged into both the power supply and a functional electrical outlet.
- If the reported problem is with a temperature sensor or fan or power supply, perform these checks:
 - Check that all of the enclosure's fans are running.
 - Check that the ambient temperature is not too warm. The enclosure operating range is 5°–40°C (41°–104°F).
 - Check for any obstructions to the airflow.
 - Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above resolve the issue, the indicated FRU has probably failed and should be replaced. The failed FRU will probably have an amber LED lit.

When the problem is resolved, event 169 is logged.

Warning The indicated SES alert condition was detected in the indicated enclosure.

Recommended actions

- Check that all modules in the enclosure are properly seated in their slots and that their latches are locked.
- If the reported problem is with a power supply, perform these checks:
 - Check that each power supply module has its switch turned on.
 - Check that each power cable is firmly plugged into both the power supply and a functional electrical outlet.
- If the reported problem is with a temperature sensor or fan or power supply, perform these checks:
 - Check that all of the enclosure's fans are running.
 - Check that the ambient temperature is not too warm. The enclosure operating range is 5°–40°C (41°–104°F).
 - Check for any obstructions to the airflow.
 - Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above resolve the issue, the indicated FRU has probably failed and should be replaced. The failed FRU will probably have an amber LED lit.

When the problem is resolved, event 169 is logged.

Info. The indicated SES alert condition was detected in the indicated enclosure.

Recommended actions

- No action is required.

169

Info. The indicated SES alert condition has been cleared in the indicated enclosure. This event indicates that a problem reported by event 168 is resolved.

Recommended actions

- No action is required.

170

Info. The last rescan detected that the indicated enclosure was added to the system.

Recommended actions

- No action is required.

171

Info. The last rescan detected that the indicated enclosure was removed from the system.

Recommended actions

- No action is required.

172

Warning The indicated vdisk has been quarantined because not all of its disks are available. The vdisk does not contain enough disks to be fault tolerant. The partial vdisk will be held in quarantine until it becomes fault tolerant.

Recommended actions

- Ensure that all disks are latched into their slots and have power.
- During quarantine, the vdisk is not visible to the host. If after latching disks into their slots and powering up the vdisk, the vdisk is still quarantined, you can manually remove the vdisk from quarantine so that the host can see the vdisk. The vdisk is still critical.
- If disks have failed, replace them.

When the vdisk has been removed from quarantine, event 173 is logged.

173

Info. The indicated vdisk has been removed from quarantine.

Recommended actions

- No action is required.

174

Info. Enclosure or disk firmware update has succeeded, been aborted by a user, or failed.

If the firmware update fails, the user will be notified about the problem immediately and should take care of the problem at that time, so even when there is a failure, this event is logged as Informational severity.

Recommended actions

- No action is required.

175

Info. The network-port Ethernet link has changed status (up or down) for the indicated controller.

Recommended actions

- If this event is logged indicating the network port is up shortly after the Management Controller (MC) has booted up (event 139), no action is required.
- Otherwise, monitor occurrences of this event for an error trend. If this event occurs more than 8 times per hour, it should be investigated.
 - This event is probably caused by equipment outside of the storage system, such as faulty cabling or a faulty Ethernet switch.
 - If this event is being logged by only one controller in a dual-controller system, swap the network-port Ethernet cables between the two controllers. This will show whether the problem is outside or inside the storage system.
 - If the problem is not outside of the storage system, replace the controller module that logged this event.

176

Info. The error statistics for the indicated disk have been reset.

Recommended actions

- No action is required.

177

Info. Cache data were purged for the indicated missing volume.

Recommended actions

- No action is required.

181

Info. One or more configuration parameters associated with the Management Controller (MC) have been changed, such as configuration for SNMP, SMI-S, email notification, and system strings (system name, system location, etc.).

Recommended actions

- No action is required.

182

Info. All disk channels have been paused. I/O will not be performed on the disks until all channels are unpaused.

Recommended actions

- If this event occurs in relation to disk firmware update, no action is required. When the condition is cleared, event 183 is logged.
- If this event occurs and you are not performing disk firmware update, see “Resources for diagnosing and resolving problems” in the WBI help for the event log panel, or the CLI help for the `show events` command.

183

Info. All disk channels have been unpaused, meaning that I/O can resume. An unpaused initiates a rescan, which when complete is logged as event 19.

This event indicates that the pause reported by event 182 has ended.

Recommended actions

- No action is required.

185

Info. An enclosure management processor (EMP) write command has completed.

Recommended actions

- No action is required.

186

Info. Enclosure parameters have been changed by a user.

Recommended actions

- No action is required.

187

Info. The write-back cache has been enabled.

Event 188 is the corresponding event that is logged when write-back cache is disabled.

Recommended actions

- No action is required.

188

Info. Write-back cache has been disabled.

Event 187 is the corresponding event that is logged when write-back cache is disabled.

Recommended actions

- No action is required.

189

Info. A disk channel that was previously degraded or failed is now healthy.

Recommended actions

- No action is required.

190

Info. The controller module's supercapacitor pack has started charging.

This change met a condition to trigger the auto-write-through feature, which has disabled write-back cache and put the system in write-through mode. When the fault is resolved, event 191 is logged to indicate that write-back mode has been restored.

Recommended Actions:

- If event 191 is not logged within 5 minutes after this event, the supercapacitor has probably failed and the controller module should be replaced.

191

Info. The auto-write-through trigger event that caused event 190 to be logged has been resolved.

Recommended Actions:

- No action is required.

192

Info. The controller module's temperature has exceeded the normal operating range.

This change met a condition to trigger the auto-write-through feature, which has disabled write-back cache and put the system in write-through mode. When the fault is resolved, event 193 is logged to indicate that write-back mode has been restored.

Recommended Actions:

- If event 193 has not been logged since this event was logged, the over-temperature condition probably still exists and should be investigated. Another over-temperature event was probably logged at approximately the same time as this event (such as event 39, 40, 168, 307, 469, 476, or 477); see the recommended actions for that event.

193

Info. The auto-write-through trigger event that caused event 192 to be logged has been resolved.

Recommended Actions:

- No action is required.

194

Info. The Storage Controller in the partner controller module is not up.

This indicates that a trigger condition has occurred that has caused the auto-write-through feature to disable write-back cache and put the system in write-through mode. When the fault is resolved, event 195 is logged to indicate that write-back mode has been restored.

Recommended Actions:

- If event 195 has not been logged since this event was logged, the other Storage Controller is probably still down and the cause should be investigated. Other events were probably logged at approximately the same time as this event; see the recommended actions for those events.

195

Info. The auto-write-through trigger event that caused event 194 to be logged has been resolved.

Recommended Actions:

- No action is required.

198

Info. A power supply has failed.

This indicates that a trigger condition has occurred that has caused the auto-write-through feature to disable write-back cache and put the system in write-through mode. When the fault is resolved, event 199 is logged to indicate that write-back mode has been restored.

Recommended Actions:

- If event 199 has not been logged since this event was logged, the power supply probably does not have a health of OK and the cause should be investigated. Another power-supply event was probably logged at approximately the same time as this event (such as event 168); see the recommended actions for that event.

199

Info. The auto-write-through trigger event that caused event 198 to be logged has been resolved.

Recommended Actions:

- No action is required.

200

Info. A fan has failed.

This indicates that a trigger condition has occurred that has caused the auto-write-through feature to disable write-back cache and put the system in write-through mode. When the fault is resolved, event 201 is logged to indicate that write-back mode has been restored.

Recommended Actions:

- If event 201 has not been logged since this event was logged, the fan probably does not have a health of OK and the cause should be investigated. Another fan event was probably logged at approximately the same time as this event (such as event 168); see the recommended actions for that event.

201

Info. The auto-write-through trigger event that caused event 200 to be logged has been resolved.

Recommended Actions:

- No action is required.

202

Info. An auto-write-through trigger condition has been cleared, causing write-back cache to be re-enabled. The environmental change is also logged at approximately the same time as this event (event 191, 193, 195, 199, 201, and 241.)

Recommended actions

- No action is required.

203

Warning An environmental change occurred that allows write-back cache to be enabled, but the auto-write-back preference is not set. The environmental change is also logged at approximately the same time as this event (event 191, 193, 195, 199, 201, or 241).

Recommended actions

- Manually enable write-back cache.

204

Error This event is generated by the hardware-flush firmware when the boot-processing firmware needs to inform the user about something.

The CompactFlash card is used for backing up unwritten cache data when a controller goes down unexpectedly, such as when a power failure occurs. This event is generated when the Storage Controller (SC) detects a problem with the CompactFlash as it is booting up.

Recommended actions

- Restart the SC that logged this event.
- If this event is then logged again, replace the controller module.

Warning This event is generated by the hardware-flush firmware when the boot-processing firmware needs to inform the user about something.

The CompactFlash card is used for backing up unwritten cache data when a controller goes down unexpectedly, such as when a power failure occurs. This event is generated when the Storage Controller (SC) detects a problem with the CompactFlash as it is booting up.

Recommended actions

- Restart the Storage Controller that logged this event.
- If this event is logged again, shut down the Storage, replace the controller module.

Info. This event is generated by the hardware-flush firmware when the boot-processing firmware needs to inform the user about something.

When logged as Informational severity, this event contains information that is primarily of interest to engineers.

Recommended actions

- No action is required.

205

Info. The indicated volume has been mapped or unmapped.

Recommended actions

- No action is required.

206

Info. Vdisk scrub has started.

The scrub checks disks in the vdisk for the following types of errors:

- Data parity errors for a RAID 3, 5, 6, or 50 vdisk.
- Mirror verify errors for a RAID 1 or RAID 10 vdisk.
- Media errors for all RAID levels including RAID 0 and non-RAID vdisk.

When errors are detected, they are automatically corrected.

When the scrub is complete, event 207 is logged.

Recommended actions

- No action is required.

207

Error Vdisk scrub completed and found an excessive number of errors in the indicated vdisk.

This event is logged as Error severity when more than 100 parity or mirror mismatches are found and corrected during a scrub or when 1 to 99 parity or mirror mismatches are found and corrected during each of 10 separate scrubs of the same vdisk.

For non-fault-tolerant RAID levels (RAID 0 and non-RAID), media errors may indicate loss of data.

Recommended actions

- Resolve any non-disk hardware problems, such as a cooling problem or a faulty controller module, expansion module, or power supply.
- Check whether any disks in the vdisk have logged SMART events or unrecoverable read errors.
 - If so, and the vdisk is a non-fault-tolerant RAID level (RAID 0 or non-RAID), copy the data to a different vdisk and replace the faulty disks.
 - If so, and the vdisk is a fault-tolerant RAID level, replace the faulty disks. Before replacing a disk, confirm that a reconstruction is not currently running on the vdisk. It is also recommended to make a full backup of all the data in the vdisk before replacing disks. If more than one disk in the vdisk has errors, replace the disks one at a time and allow reconstruction to complete after each disk is replaced.

Warning Vdisk scrub did not complete because of an internally detected condition such as a failed disk.

If a disk fails, data may be at risk.

Recommended actions

- Resolve any non-disk hardware problems, such as a cooling problem or a faulty controller module, expansion module, or power supply.
- Check whether any disks in the vdisk have logged SMART events or unrecoverable read errors.
 - If so, and the vdisk is a non-fault-tolerant RAID level (RAID 0 or non-RAID), copy the data to a different vdisk and replace the faulty disks.
 - If so, and the vdisk is a fault-tolerant RAID level, replace the faulty disks. Before replacing a disk, confirm that a reconstruction is not currently running in the vdisk. It is also recommended to make a full backup of all the data in the vdisk before replacing disks. If more than one disk in the vdisk has errors, replace the disks one at a time and allow reconstruction to complete after each disk is replaced.

Info. Vdisk scrub completed or was aborted by a user.

This event is logged as Informational severity when fewer than 100 parity or mirror mismatches are found and corrected during a scrub.

For non-fault-tolerant RAID levels (RAID 0 and non-RAID), media errors may indicate loss of data.

Recommended actions

- No action is required.

208

Info. A scrub-disk job has started for the indicated disk. The result will be logged with event 209.

Recommended actions

- No action is required.

209

Error A scrub-disk job logged with event 208 has completed and found one or more media errors, SMART events, or hard (non-media) errors. If this disk is used in a non-fault-tolerant vdisk, data may have been lost.

Recommended actions

- Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.

Warning A scrub-disk job logged with event 208 has reassigned a disk block. These bad-block replacements are reported as "other errors". If this disk is used in a non-fault-tolerant vdisk, data may have been lost.

Recommended actions

- Monitor the error trend and whether the number of errors approaches the total number of bad-block replacements available.

Info. A scrub-disk job logged with event 208 has completed and found no errors, or a disk being scrubbed (with no errors found) has been added to a vdisk, or a user has aborted the job.

Recommended actions

- No action is required.

211

Warning SAS topology has changed; no elements are detected in the SAS map. The message specifies the number of elements in the SAS map, the number of expanders detected, the number of expansion levels on the native (local controller) side and on the partner (partner controller) side, and the number of device PHYs.

Recommended actions

- Perform a rescan to repopulate the SAS map.
- If a rescan does not resolve the problem, then shut down and restart both controllers.
- If the problem persists, see "Resources for diagnosing and resolving problems" in the WBI help for the event log panel, or the CLI help for the `show events` command.

217

Error A supercapacitor failure occurred in the controller.

Recommended actions

- Replace the controller module that logged this event.

218

Warning The supercapacitor pack is near end of life.

Recommended actions

- Replace the controller module reporting this event.

219

Info. Utility priority has been changed by a user.

Recommended actions

- No action is required.

232

Warning The maximum number of enclosures allowed for the current configuration has been exceeded.

The platform does not support the number of enclosures that are configured. The enclosure indicated by this event has been removed from the configuration.

Recommended actions

- Reconfigure the system.

233

Warning The indicated disk type is invalid and is not allowed in the current configuration.

All disks of the disallowed type have been removed from the configuration.

Recommended actions

- Replace the disallowed disks with ones that are supported.

235

Error An enclosure management processor (EMP) detected a serious error.

Recommended actions

- Replace the indicated controller module or expansion module.

Info. An EMP reported an event.

Recommended actions

- No action is required.

236

Info. A special shutdown operation has started. These special shutdown types are used as part of the firmware-update process.

Recommended actions

- No action is required.

237

Info. A firmware update has started and is in progress. This event provides details of the steps in a firmware-update operation that may be of interest if you have problems updating firmware.

Recommended actions

- No action is required.

238

Warning An attempt to install a licensed feature failed due to an invalid license.

Recommended actions

- Check the license for what is allowed for the platform, make corrections as appropriate, and reinstall.

239

Warning A timeout occurred while flushing the CompactFlash.

Recommended actions

- Restart the Storage Controller that logged this event.
- If this event is logged again, shut down the Storage Controller and replace the controller module.

240

Warning A failure occurred while flushing the CompactFlash.

Recommended actions

- Restart the Storage Controller that logged this event.
- If this event is logged again, shut down the Storage Controller and replace the controller module.

241

Info. The auto-write-through trigger event that caused event 242 to be logged has been resolved.

Recommended actions

- No action is required.

242

Error The controller module's CompactFlash card has failed.

This change met a condition to trigger the auto-write-through feature, which has disabled write-back cache and put the system in write-through mode. When the fault is resolved, event 241 is logged to indicate that write-back mode has been restored.

Recommended actions

- If event 241 has not been logged since this event was logged, the CompactFlash probably does not have health of OK and the cause should be investigated. Another CompactFlash event was probably logged at approximately the same time as this event (such as event 239, 240, or 481); see the recommended actions for that event.

243

Info. A new controller enclosure has been detected. This happens when a controller module is moved from one enclosure to another and the controller detects that the midplane WWN is different from the WWN it has in its local flash.

Recommended actions

- No action is required.

245

Info. An existing disk channel target device is not responding to SCSI discovery commands.

Recommended actions

- Check the indicated target device for bad hardware or bad cable, then initiate a rescan.

246

Warning The coin battery is not present, is not properly seated, or has reached end-of-life.

The battery provides backup power for the real-time (date/time) clock. In the event of a power failure, the date and time will revert to 1980-01-01 00:00:00.

Recommended actions

- Replace the controller module that logged this event.

247

Warning The FRU ID SEEPROM for the indicated field replaceable unit (FRU) cannot be read; FRU ID data might not be programmed.

FRU ID data includes the worldwide name, serial numbers, firmware and hardware versions, branding information, etc. This event is logged once each time a Storage Controller (SC) is started for each FRU that is not programmed.

Recommended actions

- Return the FRU to have its FRU ID data reprogrammed.

248

Info. A valid feature license was successfully installed. See event 249 for details about each licensed feature.

Recommended actions

- No action is required.

249

Info. After a valid license is installed, this event is logged for each licensed feature to show the new license value for that feature. The event specifies whether the feature is licensed, whether the license is temporary, and whether the temporary license is expired.

Recommended actions

- No action is required.

250

Warning A license could not be installed.

The license is invalid or specifies a feature that is not supported on your product.

Recommended actions

- Review the readme file that came with the license. Verify that you are trying to install the license in the system that the license was generated for.

255

Info. The PBCs across controllers do not match as PBC from controller A and PBC from controller B are from different vendors. This may limit the available configurations.

Recommended actions

- No action is required.

259

Info. In-band CAPI commands have been disabled.

Recommended actions

- No action is required.

260

Info. In-band CAPI commands have been enabled.

Recommended actions

- No action is required.

261

Info. In-band SES commands have been disabled.

Recommended actions

- No action is required.

262

Info. In-band SES commands have been enabled.

Recommended actions

- No action is required.

263

Warning The indicated spare disk is missing. Either it was removed or it is not responding.

Recommended actions

- Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity.
- Configure the disk as a spare.

269

Info. A partner firmware update operation has started. This operation is used to copy firmware from one controller to the other to bring both controllers up to the same version of firmware.

Recommended actions

- No action is required.

270

Warning Either there was a problem reading or writing the persistent IP data from the FRU ID SEEPROM, or invalid data were read from the FRU ID SEEPROM.

Recommended actions

- Check the IP settings (including iSCSI host-port IP settings for an iSCSI system), and update them if they are incorrect.

271

Info. The storage system could not get a valid serial number from the controller's FRU ID SEEPROM, either because it couldn't read the FRU ID data, or because the data on it isn't valid or hasn't been programmed. Therefore, the MAC address is derived by using the controller's serial number from flash. This event is only logged one time during bootup.

Recommended actions

- No action is required.

273

Info. PHY fault isolation has been enabled or disabled by a user for the indicated enclosure and controller module.

Recommended actions

- No action is required.

274

Warning The indicated PHY has been disabled, either automatically or by a user. Drive PHYs are automatically disabled for empty disk slots or if a problem is detected. The following reasons indicate a likely hardware fault:

- Disabled because of error count interrupts
- Disabled because of excessive PHY change counts
- PHY is ready but did not pass COMINIT

Recommended actions

- If none of the reasons listed in the event description is indicated, no action is required.
- If any of the reasons listed in the event description is indicated and the event occurs shortly after the storage system is powered up, do the following:
 - Shut down the Storage Controllers. Then turn off the power for the indicated enclosure, wait a few seconds, and turn it back on.
 - If the problem recurs and the event message identifies a disk slot, replace the disk in that slot.
 - If the problem recurs and the event message identifies a module, do the following:
 - If the indicated PHY type is Egress, replace the cable in the module's egress port.
 - If the indicated PHY type is Ingress, replace the cable in the module's ingress port.
 - For other indicated PHY types or if replacing the cable does not fix the problem, replace the indicated module.
 - If the problem persists, check for other events that may indicate faulty hardware, such as an event indicating an over-temperature condition or power supply fault, and follow the recommended actions for those events.
 - If the problem still persists, the fault may be in the enclosure midplane. Replace the chassis-and-midplane FRU.
- If any of the reasons listed in the event description is indicated and this event is logged shortly after a failover, user-initiated rescan, or restart, do the following:
 - If the event message identifies a disk slot, reseal the disk in that slot.
 - If the problem persists after reseating the disk, replace the disk.
 - If the event message identifies a module, do the following:
 - If the indicated PHY type is Egress, replace the cable in the module's egress port.
 - If the indicated PHY type is Ingress, replace the cable in the module's ingress port.
 - For other indicated PHY types or if replacing the cable does not fix the problem, replace the indicated module.
 - If the problem persists, check for other events that may indicate faulty hardware, such as an event indicating an over-temperature condition or power supply fault, and follow the recommended actions for those events.
 - If the problem still persists, the fault may be in the enclosure midplane. Replace the chassis-and-midplane FRU.

275

Info. The indicated PHY has been enabled.

Recommended actions

- No action is required.

298

Warning The controller's real-time clock (RTC) setting is invalid.

This event will most commonly occur after a power loss if the real-time clock battery has failed. The time may have been set to a time that is up to 5 minutes before the power loss occurred, or it may have been reset to 1980-01-01 00:00:00.

Recommended actions

- Check the system date and time. If either is incorrect, set them to the correct date and time.
- Also look for event 246 and follow the recommended action for that event.

299

Info. The controller's real-time clock (RTC) setting was successfully recovered.

This event will most commonly occur after an unexpected power loss.

Recommended actions

- No action is required, but if event 246 is also logged, follow the recommended action for that event.

300

Info. CPU frequency has changed to high.

Recommended actions

- No action is required.

301

Info. CPU frequency has changed to low.

Recommended actions

- No action is required.

302

Info. DDR memory clock frequency has changed to high.

Recommended actions

- No action is required.

303

Info. DDR memory clock frequency has changed to low.

Recommended actions

- No action is required.

304

Info. The controller has detected I²C errors that may have been fully recovered.

Recommended actions

- No action is required.

305

Info. A serial number in Storage Controller (SC) flash memory was found to be invalid when compared to the serial number in the controller-module or midplane FRU ID SEEPROM. The valid serial number has been recovered automatically.

Recommended actions

- No action is required.

306

Info. The controller-module serial number in Storage Controller (SC) flash memory was found to be invalid when compared to the serial number in the controller-module FRU ID EEPROM. The valid serial number has been recovered automatically.

Recommended actions

- No action is required.

307

Critical A temperature sensor on a controller FRU detected an over-temperature condition that caused the controller to shut down.

Recommended actions

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5° C–40° C (41° F–104° F).
- Check for any obstructions to the airflow.
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that logged the error.

309

Info. Normally when the Management Controller (MC) is started, the IP data is obtained from the midplane FRU ID EEPROM where it is persisted. If the system is unable to write it to the EEPROM the last time it changed, a flag is set in flash memory. This flag is checked during startup, and if set, this event is logged and the IP data that is in flash memory is used. The only time that this would not be the correct IP data would be if the controller module was swapped and then whatever data is in the controller's flash memory is used.

Recommended actions

- No action is required.

310

Info. After a rescan, back-end discovery and initialization of data for at least one EMP (Enclosure Management Processor) has completed. This event is not logged again when processing completes for other EMPs in the system.

Recommended actions

- No action is required.

311

Info. This event is logged when a user initiates a ping of a host via the iSCSI interface.

Recommended actions

- If the ping operation failed, check connectivity between the storage system and the remote host.

312

Info. This event is used by email messages and SNMP traps when testing notification settings. This event is not recorded in the event log.

Recommended actions

- No action is required.

313

Error The indicated controller module has failed. This event can be ignored for a single-controller configuration.

Recommended actions

- If this is a dual-controller system, replace the failed controller module. The module's Fault/Service Required LED will be illuminated (not blinking).

314

Error The indicated FRU has failed or is not operating correctly. This event follows some other FRU-specific event indicating a problem.

Recommended actions

- To determine whether the FRU needs to be replaced, see the topic about verifying component failure in your product's FRU Installation and Replacement Guide.

315

Critical The controller module is incompatible with the enclosure.

The controller will automatically shut down. If two incompatible controllers are inserted at the same time or booted at the same time, one controller will crash and the other will hang. This behavior is expected and prevents data loss.

Recommended actions

- Move the controller module to a compatible enclosure.

317

Error A serious error has been detected on the Storage Controller's disk interface. The controller that logged this event will be killed by its partner.

Recommended actions

- Visually trace the cabling between the controller modules and expansion modules.
- If the cabling is OK, replace the controller module that logged this event.
- If the problem recurs, replace the expansion module that is connected to the controller module.

319

Warning The indicated available disk has failed.

Recommended actions

- Replace the disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing.

322

Warning The controller has an older Storage Controller (SC) version than the version used to create the CHAP authentication database in the controller's flash memory.

The CHAP database cannot be read or updated. However, new records can be added, which will replace the existing database with a new database using the latest known version number.

Recommended actions

- Upgrade the controller firmware to a version whose SC is compatible with the indicated database version.
- If no records were added, the database becomes accessible and remains intact.
- If records were added, the database becomes accessible but contains only the new records.

352

Info. Expander Controller (EC) assert data or stack-dump data is available.

Recommended actions

- No action is required.

353

Info. Expander Controller (EC) assert data and stack-dump data have been cleared.

Recommended actions

- No action is required.

354

Warning SAS topology has changed on a host port; at least one PHY has gone down. For example, the SAS cable connecting a controller host port to a host has been disconnected.

Recommended actions

- Check the cable connection between the indicated port and the host.
- Monitor the log to see if the problem persists.

Info. SAS topology has changed on a host port; at least one PHY has gone up. For example, the SAS cable connecting a controller host port to a host has been connected.

Recommended actions

- No action is required.

355

Warning The controller module's debug button was found to be stuck in the On position during boot up.

Recommended actions

- If the button remains stuck, replace the controller module.

356

Warning This event can only result from tests that are run in the manufacturing environment.

Recommended actions

- Follow the manufacturing process.

357

Warning This event can only result from tests that are run in the manufacturing environment.

Recommended actions

- Follow the manufacturing process.

358

Critical All PHYs are down for the indicated disk channel. The system is degraded and is not fault-tolerant because all disks are in a single-ported state.

Recommended actions

- Turn off the power for the controller enclosure, wait a few seconds, and turn it back on.
- If the condition doesn't persist (that is, if event 359 has been logged for the indicated channel), no further action is required.
- If the condition persists, this indicates a hardware problem in one of the controller modules or in the controller enclosure midplane. For help identifying which FRU to replace, see "Resources for diagnosing and resolving problems" in the WBI help for the event log panel, or the CLI help for the `show events` command.

Warning Some, but not all, PHYs are down for the indicated disk channel.

Recommended actions

- Monitor the log to see whether the condition persists.
- If the condition doesn't persist (that is, if event 359 has been logged for the indicated channel), no further action is required.
- If the condition persists, this indicates a hardware problem in one of the controller modules or in the controller enclosure midplane. For help identifying which FRU to replace, see "Resources for diagnosing and resolving problems" in the WBI help for the event log panel, or the CLI help for the `show events` command.

359

Info. All PHYs that were down for the indicated disk channel have recovered and are now up.

Recommended actions

- No action is required.

360

Info. The speed of the indicated disk PHY was renegotiated.

Recommended actions

- No action is required.

361

Critical, Error, or Warning The scheduler experienced a problem with the indicated schedule.

Recommended actions

- Take appropriate action based on the indicated problem.

Info. A scheduled task was initiated.

Recommended actions

- No action is required.

362

Critical, Error, or Warning The scheduler experienced a problem with the indicated task.

Recommended actions

- Take appropriate action based on the indicated problem.

Info. The scheduler experienced a problem with the indicated task.

Recommended actions

- No action is required.

363

Error When the Management Controller (MC) is restarted, firmware versions that are currently installed are compared against those in the bundle that was most recently installed. When firmware is updated, it is important that all components are successfully updated or the system may not work correctly. Components checked include the CPLD, Expander Controller (EC), Storage Controller (SC), and MC.

Recommended actions

- Reinstall the firmware bundle.

Info. When the Management Controller (MC) is restarted, firmware versions that are currently installed are compared against those in the bundle that was most recently installed. If the versions match, this event is logged as Informational severity. Components checked include the CPLD, Expander Controller (EC), Storage Controller (SC), and MC.

Recommended actions

- No action is required.

364

Info. The broadcast bus is running as generation 1.

Recommended actions

- No action is required.

365

Error An uncorrectable ECC error occurred in Storage Controller CPU memory.

Recommended actions

- If this event occurs more than once for the same controller module, replace the controller module.

400

Info. The indicated log has filled to a level at which it needs to be transferred to a log-collection system.

Recommended actions

- No action is required.

401

Warning The indicated log has filled to a level at which diagnostic data will be lost if not transferred to a log-collection system.

Recommended actions

- Transfer the log file to the log-collection system.

402

Error The indicated log has wrapped and has started to overwrite its oldest diagnostic data.

Recommended actions

- Investigate why the log-collection system is not transferring the logs before they are overwritten. For example, you might have enabled managed logs without configuring a destination to send logs to.

412

Warning One disk in the indicated RAID 6 vdisk failed. The vdisk is on line but has a status of FTDN (fault tolerant with a down disk).

If a dedicated spare or global spare of the proper type and size is present, that spare is used to automatically reconstruct the vdisk; events 9 and 37 are logged to indicate this. If no usable spare disk is present, but an available disk of the proper type and size is present and the dynamic spares feature is enabled, that disk is used to automatically reconstruct the vdisk; event 37 is logged.

Recommended actions

- If no spare was present and the dynamic spares feature is disabled (that is, event 37 was *not* logged), configure an available disk as a dedicated spare for the vdisk or replace the failed disk and configure the new disk as a dedicated spare for the vdisk. That spare be used to automatically reconstruct the vdisk; confirm this by checking that events 9 and 37 are logged.
- Otherwise, reconstruction automatically started and event 37 was logged. Replace the failed disk and configure the replacement as a dedicated or global spare for future use.
- Confirm that all failed disks have been replaced and that there are sufficient spare disks configured for future use.

427

Warning A communication error occurred when sending information between storage systems.

Recommended actions

- Check your network or fabric for abnormally high congestion or connectivity issues.

442

Warning Power-On Self Test (POST) diagnostics detected a hardware error in a UART chip.

Recommended actions

- Replace the controller module that logged this event.

Info. A user changed the drive-spin-down delay for the indicated vdisk to the indicated value.

Recommended actions

- No action is required.

455

Warning The controller detected that the configured host-port link speed exceeded the capability of an FC SFP. The speed has been automatically reduced to the maximum value supported by all hardware components in the data path.

Recommended actions

- Replace the SFP in the indicated port with an SFP that supports a higher speed.

456

Warning The system's IQN was generated from the default OUI because the controllers could not read the OUI from the midplane FRU ID data during startup. If the IQN is wrong for the system's branding, iSCSI hosts might be unable to access the system.

Recommended actions

- If event 270 with status code 0 is logged at approximately the same time, restart the controllers.

464

Warning A user inserted an unsupported cable or SFP into the indicated controller host port.

Recommended actions

- Replace the cable or SFP with a supported type, as specified in your product's Setup Guide.

465

Info. A user removed an unsupported cable or SFP from the indicated controller host port.

Recommended actions

- No action is required.

468

Info. FPGA temperature has returned to the normal operating range and the speed of buses connecting the FPGA to downstream adapters has been restored. The speed was reduced to compensate for an FPGA over-temperature condition.

This event indicates that a problem reported by event 469 is resolved.

Recommended actions

- No action is required.

469

Warning The speed of buses connecting the FPGA to downstream adapters has been reduced to compensate for an FPGA over-temperature condition.

The storage system is operational but I/O performance is reduced.

Recommended actions

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5°C–40°C (41°F–104°F).
- Check for any obstructions to the airflow.
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that logged the error.

When the problem is resolved, event 468 is logged.

476

Warning The CPU temperature exceeded the safe range so the CPU entered its self-protection state. IOPS were reduced.

Recommended actions:

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5°C–40°C (41°F–104°F).
- Check for any obstructions to the airflow.
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that logged the error.

When the problem is resolved, event 478 is logged.

477

Info. The CPU temperature exceeded the normal range so the CPU speed was reduced. IOPS were reduced.

Recommended actions:

- Check that the storage system's fans are running.
- Check that the ambient temperature is not too warm. The enclosure operating range is 5°C–40°C (41°F–104°F).
- Check for any obstructions to the airflow.
- Check that there is a module or blank plate in every module slot in the enclosure.
- If none of the above explanations apply, replace the controller module that logged the error.

When the problem is resolved, event 478 is logged.

478

Info. This event indicates that a problem reported by event 476 or 477 is resolved.

Recommended actions:

- No action is required.

479

Error The controller reporting this event was unable to flush data to or restore data from non-volatile memory.

This mostly likely indicates a CompactFlash failure, but it could be caused by some other problem with the controller module. The Storage Controller that logged this event will be killed by its partner controller, which will use its own copy of the data to perform the flush or restore operation.

Recommended actions

- If this is the first time this event has been logged, restart the killed Storage Controller.
- If this event is then logged again, replace the controller module.

480

Error An IP address conflict was detected for the indicated iSCSI port of the storage system. The indicated IP address is already in use.

Recommended actions

- Contact your data-network administrator to help resolve the IP address conflict.

481

Error The periodic monitor of CompactFlash hardware detected an error. The controller was put in write-through mode, which reduces I/O performance.

Recommended actions

- Restart the Storage Controller that logged this event.
- If this event is logged again, shut down the Storage Controller and replace the controller module.

482

Warning One of the PCIe buses is running with fewer lanes than it should.

This event is the result of a hardware problem that has caused the controller to use fewer lanes. The system works with fewer lanes, but I/O performance is degraded.

Recommended actions:

- Replace the controller module that logged this event.

483

Error An invalid expansion-module connection was detected for the indicated disk channel. An egress port is connected to an egress port, or an ingress port is connected to an incorrect egress port.

Recommended actions

- Visually trace the cabling between enclosures and correct the cabling.

484

Warning No compatible spares are available to reconstruct this vdisk if it experiences a disk failure. Only vdisks that have dedicated spares will start reconstruction automatically.

This situation puts data at increased risk because it will require user action to configure a disk as a dedicated or global spare before reconstruction can begin on the indicated vdisk if a disk in that vdisk fails in the future.

If the last global spare has been deleted or used for reconstruction, *all* vdisks that do not have at least one dedicated spare are at increased risk.

Note that even though there may be global spares still available, they cannot be used for reconstruction of a vdisk if that vdisk uses larger-capacity disks or a different type of disk; so this event may be logged even when there are unused global spares. If the dynamic spares feature is enabled, this event will be logged even if there is an available disk that may be used for reconstruction.

Recommended actions

- Configure disks as dedicated spares or global spares.
- For a dedicated spare, the disk must be of the same type as the other disks in the vdisk and at least as large as the smallest-capacity disk in the vdisk, and it should have the same or better performance.
- For a global spare, it is best to choose a disk that is as big as or bigger than the largest disk of its type in the system and of equal or greater performance. If the system contains a mix of disk types (SAS SSD, enterprise SAS, or midline SAS), there should be at least one global spare of each type (unless dedicated spares are used to protect every vdisk of a given type).

485

Warning The indicated vdisk was quarantined to prevent writing invalid data that may exist in the controller that logged this event.

This event is logged to report that the indicated vdisk has been put in the quarantined offline state (status of QTOF) to prevent loss of data. The controller that logged this event has detected (via information saved in the vdisk metadata) that it may contain outdated data that should not be written to the vdisk. Data may be lost if you do not follow the recommended actions carefully. This situation is typically caused by removal of a controller module without shutting it down first, then inserting a different controller module in its place. To avoid having this problem occur in the future, always shut down the Storage Controller in a controller module before removing it. This situation may also be caused by failure of the CompactFlash card, as indicated by event 204.

Recommended actions

- If event 204 is logged, follow the recommended actions for event 204.
- If event 204 is *not* logged, perform the following recommended actions:
 - If event 486 is not logged at approximately the same time as event 485, reinsert the removed controller module, shut it down, then remove it again.
 - If events 485 and 486 are both logged at approximately the same time, wait at least 5 minutes for the automatic recovery process to complete. Then sign in and confirm that both controller modules are operational. (You can determine if the controllers are operational with the `show controllers` CLI command or with the WBI.) In most cases, the system will come back up and no further action is required. If both controller modules do not become operational in 5 minutes, data may have been lost. If both controllers are not operational, follow this recovery process:
 - Remove the controller module that first logged event 486.
 - Turn off the power for the controller enclosure, wait a few seconds, then turn it back on.
 - Wait for the controller module to restart, then sign in again.
 - Check the status of the vdisks. If any of the vdisks have a status of quarantined offline (QTOF), dequarantine those vdisks.
 - Reinsert the previously removed controller module. It should now restart successfully.

486

Info. A recovery process was initiated to prevent writing invalid data that may exist in the controller that logged this event. The controller that logged this event has detected (via information saved in the vdisk metadata) that it may contain outdated data that should not be written to the vdisks. The controller will log this event, restart the partner controller, wait 10 seconds, then kill itself. The partner controller will then unkill this controller and mirror the correct cache data to it. This procedure will, in most cases, allow all data to be correctly written without any loss of data and without writing any outdated data.

Recommended actions

- Wait at least 5 minutes for the automatic recovery process to complete. Then sign in and confirm that both controller modules are operational. (You can determine if the controllers are operational with the `show redundancy-mode` CLI command or the System Redundancy table in the System Overview panel of the WBI.) In most cases, the system will come back up and no action is required.
- If both controller modules do not become operational in 5 minutes, see the recommended actions for event 485, which will be logged at approximately the same time.

487

Info. Historical performance statistics were reset.

Recommended actions

- No action is required.

488

Info. Creation of a set of volumes started.

Recommended actions

- No action is required.

489

Info. Creation of a set of volumes completed.

Recommended actions

- No action is required.

490

Info. Creation of a set of volumes failed.

Recommended actions

- No action is required.

495

Warning The algorithm for best-path routing selected the alternate path to the indicated disk because the I/O error count on the primary path reached its threshold.

The controller that logs this event indicates which channel (path) has the problem. For example, if the B controller logs the problem, the problem is in the chain of cables and expansion modules connected to the B controller module.

Recommended actions

- If this event is consistently logged for only one disk in an enclosure, perform the following actions:
 - Replace the disk.
 - If that does not resolve the problem, the fault is probably in the enclosure midplane. Replace the chassis-and-midplane FRU for the indicated enclosure.
- If this event is logged for more than one disk in an enclosure or disks in multiple enclosures, perform the following actions:
 - Check for disconnected SAS cables in the bad path. If no cables are disconnected, replace the cable connecting to the ingress port in the most-upstream enclosure with reported failures. If that does not resolve the problem, replace other cables in the bad path, one at a time until the problem is resolved.
 - If that does not resolve the problem, replace the expansion modules that are in the bad path. Begin with the most-upstream module that is in an enclosure with reported failures. If that does not resolve the problem, replace other expansion modules (and the controller module) upstream of the affected enclosure(s), one at a time until the problem is resolved.
 - If that does not resolve the problem, the fault is probably in the enclosure midplane. Replace the chassis-and-midplane FRU of the most-upstream enclosure with reported failures. If that does not resolve the problem and there is more than one enclosure with reported failures, replace the chassis-and-midplane FRU of the other enclosures with reported failures until the problem is resolved.

496

Warning An unsupported disk type was found.

Recommended actions

- Replace the disk with a supported type.

497

Info. A disk copyback operation started. The indicated disk is the source disk.

When a disk fails, reconstruction is performed using a spare disk. When the failed disk is replaced, the data that was reconstructed on the spare disk (and any new data that was written to it) is copied to the disk in the slot where the data was originally located. This is known as slot affinity. For the copyback operation, the reconstructed disk is called the source disk, and the newly replaced disk is called the destination disk. All of the data is copied from the source disk to the destination disk and the source disk then becomes a spare disk again.

Recommended actions

- No action is required.

498

Warning A disk copyback operation failed.

When a disk fails, reconstruction is performed using a spare disk. When the failed disk is replaced, the data that was reconstructed in the spare disk (and any new data that was written to it) is copied to the disk in the slot where the data was originally located. However, this copyback operation failed. This is probably because the disk that was inserted as a replacement for the failed disk is also faulty. This failure could also be caused by a fault in the midplane that the disk is inserted into.

Recommended actions

- Replace the destination disk with one of the same type (SAS SSD, enterprise SAS, or midline SAS) and the same or greater capacity. For continued optimum I/O performance, the replacement disk should have performance that is the same as or better than the one it is replacing. (See event 499 to identify the destination disk.)
- If the problem then recurs for the same slot, replace the chassis-and-midplane FRU.

Info. A disk copyback operation completed.

Recommended actions

- If the event message indicates that one or more uncorrectable media errors occurred during the copyback, some user data may have been lost. Use backup copied of the data or other means to restore any lost data.
- Otherwise, no action is required.

499

Info. A disk copyback operation started. The indicated disk is the destination disk.

When a disk fails, reconstruction is performed using a spare disk. When the failed disk is replaced, the data that was reconstructed in the spare disk (and any new data that was written to it) is copied to the disk in the slot where the data was originally located. This is known as slot affinity. For the copyback operation, the reconstructed disk is called the source disk, and the newly replaced disk is called the destination disk. All of the data is copied from the source disk to the destination disk and the source disk then becomes a spare disk again.

Recommended actions

- If the event message indicates that one or more uncorrectable media errors occurred during the copyback, some user data may have been lost. Use backup copies of the data or other means to restore any lost data.
- Otherwise, no action is required.

500

Info. A disk copyback operation completed. The indicated disk was restored to being a spare.

When a disk fails, reconstruction is performed using a spare disk. When the failed disk is replaced, the data that was reconstructed in the spare disk (and any new data that was written to it) is copied to the disk in the slot where the data was originally located. This is known as slot affinity. For the copyback operation, the reconstructed disk is called the source disk, and the newly replaced disk is called the destination disk. All of the data is copied from the source disk to the destination disk and the source disk then becomes a spare disk again.

Recommended actions

- No action is required.

501

Error The enclosure hardware is not compatible with the I/O module firmware.

The Expander Controller firmware detected an incompatibility with the midplane type. As a preventive measure, disk access was disabled in the enclosure.

Recommended actions

- Update the storage system to the latest firmware.

502

Error The indicated solid-state disk (SSD) has 1% of its life remaining.

Recommended actions

- Replace the SSD with one of the same type and capacity.

Warning The indicated solid-state disk (SSD) has 5% of its life remaining.

When the device has 1% of its life left, this event will be logged again with a severity of Error.

Recommended actions

- Be sure you have a spare SSD of the same type and capacity available.
- If a spare is available, it is recommended to replace the SSD now.

Info. The indicated solid-state disk (SSD) has 20% of its life remaining.

When the device has 5% of its life left, this event will be logged again with a severity of Warning.

Recommended actions

- You should obtain a replacement SSD of the same type and capacity if you do not already have one available.

503

Info. A disk that was previously reported as 'Not Ready' is now ready.

This event indicates that a condition reported by event 58 is resolved. Event 58 reported this disk to be 'Not Ready'.

Recommended actions

- No action is required.

Info. Service debug access to the system has been enabled or disabled by a user.

Allowing service debug access may have security implications. After the diagnosis is complete you may want to disallow such access.

Recommended actions

- No action is required.

Troubleshooting steps for leftover disk drives

Storage systems use metadata on hard drives to identify vdisk members and identify other disk members of the vdisk.

Hard drives enter a Leftover state for several reasons:

- Drive spin up was not completed before a controller polled the drive. When the controller queries the drive and finds the drive is not in a ready state, the controller may place the drive into a Leftover state.
- Improper power-on sequences.
- Firmware upgrade (due to a timing issue).
- Failover taking longer than expected.
- The drive is swapped from another system, or removed and reinserted in the storage system.

Metadata on a disk identifies the disk as being a member of a vdisk. Improperly clearing the metadata from a disk may cause permanent data loss.

△ **CAUTION:** Clearing metadata from a leftover drive should be done with extreme care. Only clear metadata if you are certain the drive has never been associated with a vdisk in this system or contains no data. This situation most often occurs when inserting a previously used hard drive into a live system or moving a drive between two systems.

Never clear metadata from a drive if any vdisk in the storage system is in an Offline, Quarantined, or inaccessible state. Do not clear metadata from a drive if you are unsure this is the correct step to take. Clearing metadata from a drive permanently clears all data from the drive. In these types of situations, a backup of data should be done if possible.

Using the trust command

The CLI `trust` command should only be used as a last step in a disaster recovery situation. This command has the potential to cause permanent data loss and unstable operation of the vdisk. If a vdisk with a single disk is in a leftover or failed condition, the `trust` command should never be used. The `trust` command should only be used if the vdisk is in an Offline state.

If a single disk in a vdisk has failed or been placed into a Leftover state due to errors, reintegrating the disk into the same or a different vdisk has the potential to cause data loss. A hard drive that has failed or been placed into a Leftover state due to multiple errors should be replaced with a new hard drive. Assign the new hard drive back to the vdisk as a spare and allow reconstruction to complete in order to return the vdisk to a fault-tolerant state.

The `trust` command attempts to resynchronize leftover disks in order to make any leftover disk an active member of the vdisk again. The user might need to take this step when a vdisk is offline because there is no data backup, or as a last attempt to try to recover the data on a vdisk. In this case, `trust` may work, but only as long as the leftover disk continues to operate. When the “trusted” vdisk is back online, backup all data on the vdisk and verify all data to ensure it is valid. The user then needs to delete the trusted vdisk, create a new vdisk, and restore data from the backup to the new vdisk.

 **IMPORTANT:** Using `trust` on a vdisk is only a disaster-recovery measure; the vdisk has no tolerance for additional failures and should never be put back into a production environment.

 **CAUTION:** Before trusting a vdisk, carefully read the cautions and procedures for using the `trust` command in the CLI Reference Guide and online help.

Once the `trust` command has been issued on a vdisk, further troubleshooting steps may be limited towards disaster recovery. If you are unsure of the correct action to take, contact technical support for further assistance.

PSU faults and recommended actions

Table 31 PSU faults and recommended actions

Fault	Recommended action
PSU fan warning or failure. PSU warning or failure. PSU module status is listed as failed or you receive a voltage event notification. (Event code 168.)	<ul style="list-style-type: none"> Check that all modules in the enclosure are properly seated in their slots and that their latches are locked. Check that each PSU module with a switch has that switch turned on. Check that each power cable is firmly plugged into both the PSU and a functional electrical outlet. Check that all of the enclosure's fans are running. Check that the ambient temperature is not too warm. The enclosure operating range is 5°–40°C (41°–104°F). Check for any obstructions to the airflow. Check that there is a module or blank plate in every module slot in the enclosure. If none of the above resolve the issue, the indicated PSU has probably failed and should be replaced. The failed PSU will probably have an amber LED lit.
Power LED is off.	Same as above.
Voltage/Fan Fault/Service Required LED is on.	Replace the PSU module.

Events sent as indications to SMI-S clients

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 the chapter about configuring the system in the RAIDar User Guide.

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

Table 32 Events and corresponding SMI-S indications

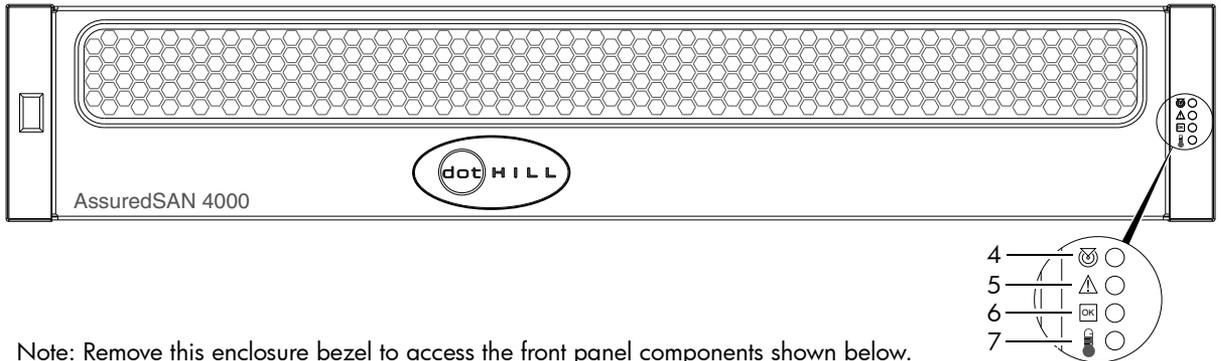
FRU/Event category	Corresponding SMI-S class	Operation status values that would trigger alert conditions
Controller	DHS_Controller	Down, Not Installed, OK
Hard Disk Drive	DHS_DiskDrive	Unknown, Missing, Error, Degraded, OK
Fan	DHS_PSUFan	Error, Stopped, OK
PSU	DHS_PSU	Unknown, Error, Other, Stressed, Degraded, OK
Temperature Sensor	DHS_OverallTempSensor	Unknown, Other, Error, Non-Recoverable Error, Degraded, OK
Battery/SuperCap	DHS_SuperCap	Unknown, Error, OK
FC Port	DHS_FCPort	Stopped, OK

Table 32 Events and corresponding SMI-S indications (continued)

FRU/Event category	Corresponding SMI-S class	Operation status values that would trigger alert conditions
SAS Port	DHS_SASTargetPort	Stopped, OK
iSCSI Port	DHS_ISCSIEthernetPort	Stopped, OK

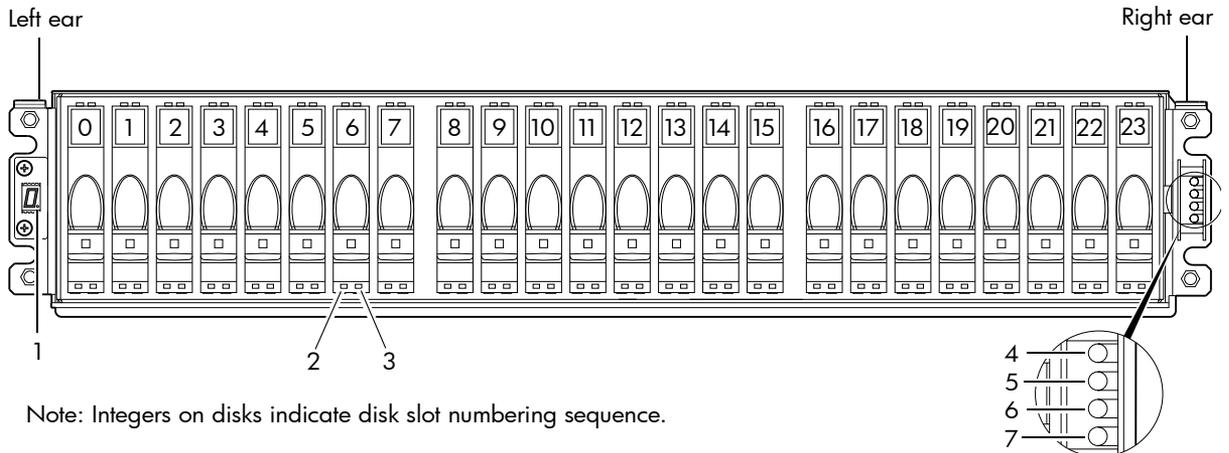
B System LEDs

24-disk enclosure front panel LEDs



Note: Remove this enclosure bezel to access the front panel components shown below.

Figure 21 24-disk enclosure with bezel installed



Note: Integers on disks indicate disk slot numbering sequence.

Figure 22 24-disk enclosure with bezel removed

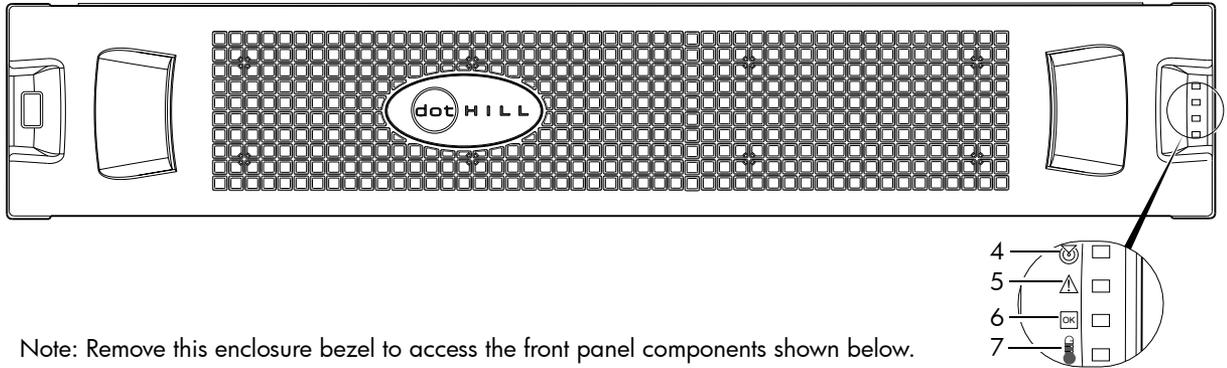
Table 33 LEDs: 2U24 enclosure front panel

LED	Description	Definition
1	Enclosure ID	Green — On Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 0. The enclosure ID for an attached disk enclosure is nonzero.
2	Disk drive — Left LED	See Disk drive LEDs on page 199.
3	Disk drive — Right LED	See Disk drive LEDs on page 199.
4	Unit Locator	White blink — Enclosure is identified Off — Normal operation
5	Fault/Service Required	Amber — On Enclosure-level fault condition exists. The event has been acknowledged but the problem needs attention. Off — No fault condition exists.

Table 33 LEDs: 2U24 enclosure front panel (continued)

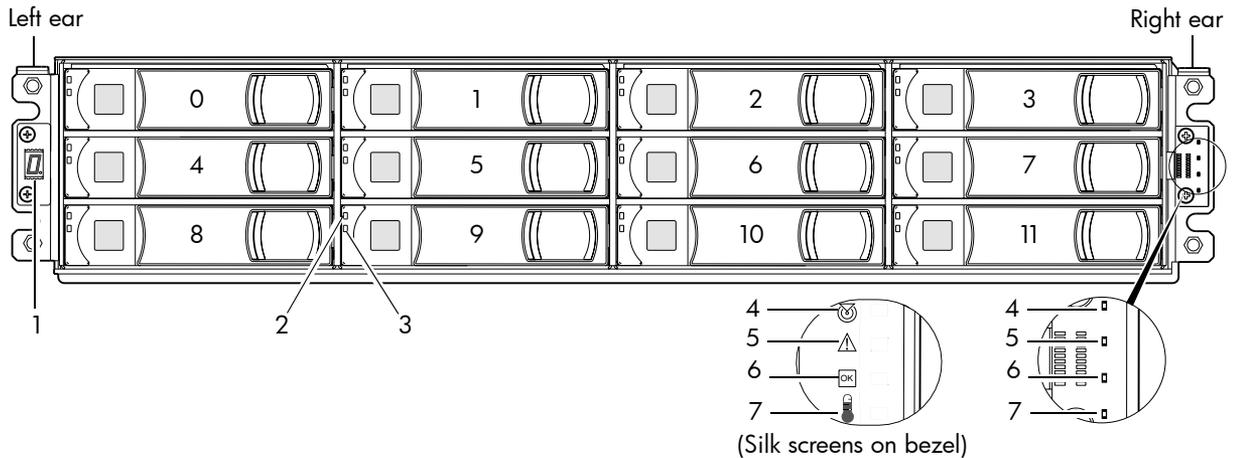
LED	Description	Definition
6	FRU OK	Green — On The enclosure is powered on with at least one PSU operating normally. Off — Both power supplies are off; the system is powered off.
7	Temperature Fault	Green — On The enclosure temperature is normal. Amber — On The enclosure temperature is above threshold.

12-disk enclosure front panel LEDs



Note: Remove this enclosure bezel to access the front panel components shown below.

Figure 23 12-disk enclosure with bezel installed



Note: Bezel is removed to show front panel LEDs. Integers on disks indicate disk slot numbering sequence.

Figure 24 12-disk enclosure with bezel removed

Table 34 LEDs: 2U12 enclosure front panel

LED	Description	Definition
1	Enclosure ID	Green — On Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 0. The enclosure ID for an attached disk enclosure is nonzero.
2	Disk drive — Upper LED	See Disk drive LEDs on page 199.
3	Disk drive — Lower LED	See Disk drive LEDs on page 199.

Table 34 LEDs: 2U12 enclosure front panel (continued)

LED	Description	Definition
4	Unit Locator	White blink — Enclosure is identified Off — Normal operation
5	Fault/Service Required	Amber — On Enclosure-level fault condition exists. The event has been acknowledged but the problem needs attention. Off — No fault condition exists.
6	FRU OK	Green — On The enclosure is powered on with at least one PSU operating normally. Off — Both power supplies are off; the system is powered off.
7	Temperature Fault	Green — On The enclosure temperature is normal. Amber — On The enclosure temperature is above threshold.

Disk drive LEDs

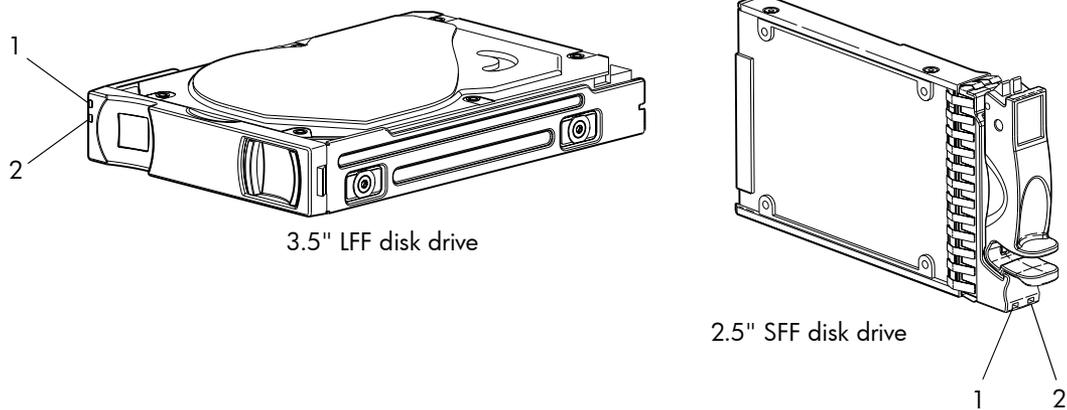


Figure 25 Disk drives

Table 35 LEDs: Disk drive

LED No./Description	Color	State	Definition
1 — Power/Activity	Green	On	The disk drive module is operating normally.
		Blink	The disk drive module is initializing; active and processing I/O; performing a media scan; or the vdisk is initializing or reconstructing.
		Off	If not illuminated and Fault is not illuminated, the disk is not powered on.
2 — Fault	Amber	On	The disk has failed; experienced a fault; is a leftover; or the vdisk that it is associated with is down or critical.
		Blink	Physically identifies the disk; or locates a leftover (also see Blue).
	Off	If not illuminated and Power/Activity is not illuminated, the disk is not powered on.	
	Blue	Blink	Leftover disk from vdisk is located (alternates blinking amber).

NOTE: If a user interface shows the disk LED is Fault (amber), while the enclosure shows it is green, the fault might be in the midplane or the disk's midplane connector.

Table 36 LEDs: Disks in LFF and SFF enclosures

Disk drive module LED behavior		LFF — 12-disk ¹		SFF — 24-disk	
Description	State	Color	Action	Color	Action
Disk drive OK, FTOL	Off	None	None	None	None
	On (operating normally)	Green	On	Green	On
	OK to remove	Green	Blink	Green	On
		Blue	On	Blue	On
	Identifying self — offline/online		Amber	Blink	Green ²
Amber					Blink
Disk drive I/O	Initializing	Green	Blink	Green	Blink
	Active and processing I/O	Green	Blink	Green	Blink
	Performing a media scan	Green	Blink	Green	Blink
Disk drive leftover	Disk drive is a leftover	Amber	On	Amber	On
	Identifying a leftover	Amber ³	Blink	Amber	Blink
		Blue ²	On	Blue ²	Blink
Disk drive failed	Fault or failure	Amber	On	Green ²	On
				Amber	On
	Fault and remove disk drive	Amber	On	Green	On
				Blue	On
	Fault and identify disk drive	Amber	Blink	Green	On
				Amber	On
	Fault, identify, and remove disk drive	Amber	Blink	Green	On
				Blue	On
				Blue	On

¹The LFF disks used in the 4000 Series 12-disk enclosures follow SFF 24-disk LED behavior.

²This color may or may not illuminate.

³Bitonal LED blinks amber/green.

 **NOTE:** If a user interface shows the disk LED is Fault (amber), while the enclosure shows it is green, the fault might be in the midplane or the disk's midplane connector.

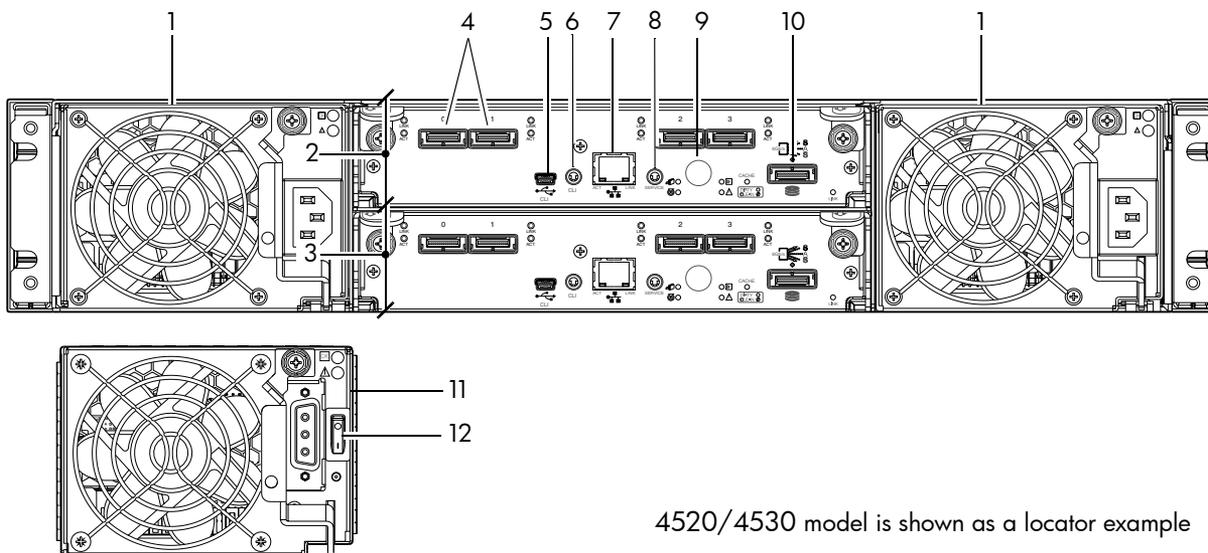
Table 37 LEDs: Vdisks in LFF and SFF enclosures

Vdisk LED behavior		LFF — 12-disk ¹		SFF — 24-disk	
Description	State	Color	Action	Color	Action
FTOL	On (operating normally)	Green	Blink	Green	On
Vdisk activity	Vdisk is reconstructing	Green	Blink	Green	Blink
	Vdisk is initializing	Green	Blink	Green	Blink
Vdisk degraded	Vdisk is critical/down	See note 1 below		See note 1 below	

¹Individual disks will display fault LEDs

Controller enclosure: Rear panel layout

The diagram and table below display and identify important component items that comprise the rear panel layout of an AssuredSAN 4000 Series controller enclosure. The 4520/4530 is shown as a representative example of controller enclosure models included in the product series.



4520/4530 model is shown as a locator example

- | | |
|-----------------------------|---|
| 1 AC power supplies | 7 Network port |
| 2 Controller module A | 8 Service port (used by service personnel only) |
| 3 Controller module B | 9 Disabled button (used by engineering/test only) |
| 4 SAS ports: host interface | 10 Expansion port |
| 5 CLI port (USB - Type B) | 11 DC Power supply (2) — (DC model only) |
| 6 Reserved for future use | 12 DC Power switch |

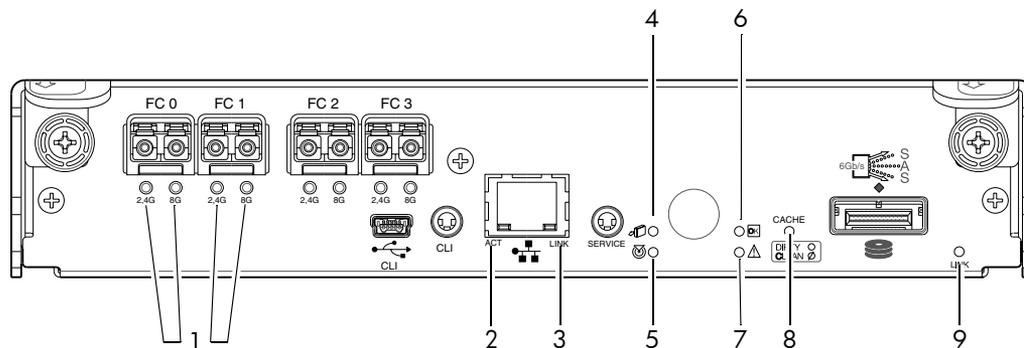
Figure 26 4520/4530 controller enclosure: Rear panel layout

A controller enclosure accommodates two PSU FRUs of the same type (either both AC or both DC) within the two PSU slots. The controller enclosure accommodates up to two controller module FRUs of the same type within the IOM slots.

Figure 27 and Figure 28 provide descriptions for the different controller modules and PSUs that can be installed into the rear panel of a 4000 Series controller enclosure. Showing controller modules and PSUs separately from the enclosure enables improved clarity in identifying the component items called out in the diagrams and described in the tables.

LED descriptions are also provided for optional disk enclosures supported by the 4000 Series controller enclosures.

4720/4730 controller module: Rear panel LEDs

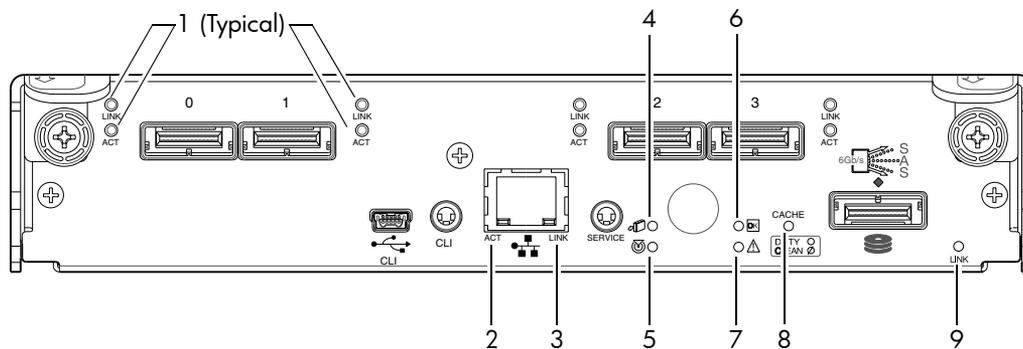


LED No./Description	Color	State	Definition
1 — Host 2/4/8 Gbit FC Link Status/ Link Activity	Green	On	Port is connected and the link is up. 2,4 G LED illuminates — link speed is 2 or 4 Gbit/s 8 G LED illuminates — link speed is 8 Gbit/s
		Off	Both LEDs off — link speed is 1 Gbit/s ¹
		Blink	1Hz — no link detected
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	The Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 204)
9 — Expansion Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.

¹The 8 Gbit SFP modules do not support 1 Gbit link speeds.

Figure 27 4720/4730 controller module

4520/4530 controller module: Rear panel LEDs



LED No./Description	Color	State	Definition
1 — 6 Gbit SAS Link Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.
6 Gbit SAS Link Activity	Green	Blink	Link has I/O activity.
		Off	Link is idle.
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty (contains unwritten data) and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 204)
9 — Expansion Port Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.

Figure 28 4520/4530 controller module

NOTE: Once a Link Status LED is lit, it remains so, even if the controller is shut down via RAIDar or CLI.

When a controller is shut down or otherwise rendered inactive, its Link Status LED remains illuminated, falsely indicating that the controller can communicate with the host. Though a link exists between the host

and the chip on the controller, the controller is not communicating with the chip. To reset the LED, the controller must be power-cycled.

Cache Status LED details

If the LED is blinking evenly, a cache flush is in progress. When a controller module loses power and write cache is dirty (contains data that has not been written to disk), the supercapacitor pack provides backup power to flush (copy) data from write cache to CompactFlash memory. When cache flush is complete, the cache transitions into self-refresh mode.

If the LED is blinking momentarily slowly, the cache is in a self-refresh mode. In self-refresh mode, if primary power is restored before the backup power is depleted (3–30 minutes, depending on various factors), the system boots, finds data preserved in cache, and writes it to disk. This means the system can be operational within 30 seconds, and before the typical host I/O time-out of 60 seconds, at which point system failure would cause host-application failure. If primary power is restored after the backup power is depleted, the system boots and restores data to cache from CompactFlash, which can take about 90 seconds.

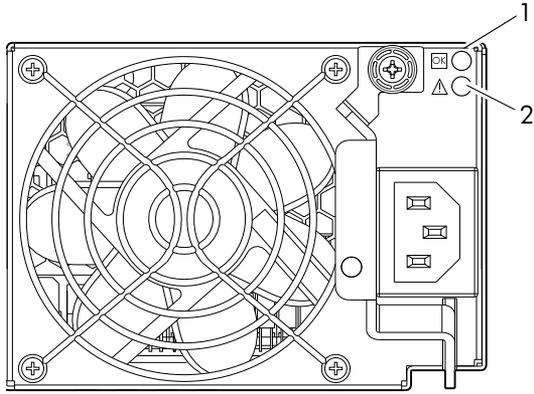
The cache flush and self-refresh mechanism is an important data protection feature; essentially four copies of user data are preserved: one in controller cache and one in CompactFlash of each controller.

The LED becomes solid green during the boot-up process. This indicates the cache is logging all POSTs, which will be flushed to the CompactFlash the next time the controller shuts down.

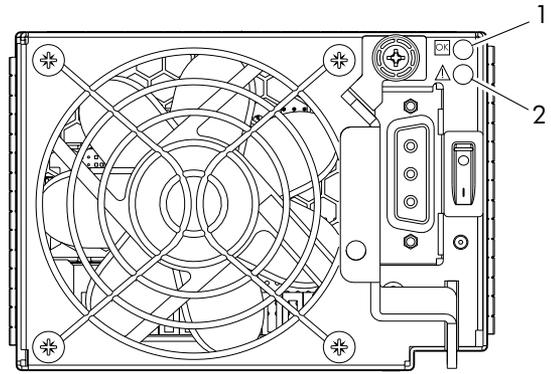
△ **CAUTION:** If the Cache Status LED is solid green, the controller should be shut-down from the user interface so unwritten data can be flushed to the CompactFlash.

PSU LEDs

Power redundancy is achieved through two independent load-sharing power supplies. In the event of a PSU failure, or the failure of the power source, the storage system can operate continuously on a single PSU. Greater redundancy can be achieved by connecting the power supplies to separate circuits. DC power supplies are equipped with a power switch. AC power supplies may or may not have a power switch (the newer model in [Figure 29](#) has no power switch). Whether a PSU has a power switch is significant to powering on/off.



AC model



DC model

LED No./Description	Color	State	Definition
1 — Input Source Power Good	Green	On	Power is on and input voltage is normal.
		Off	Power is off, or input voltage is below the minimum threshold.
2 — Voltage/Fan Fault/Service Required	Amber	On	Output voltage is out of range, or a fan is operating below the minimum required r/min.
		Off	Output voltage is normal.

Figure 29 PSUs

C Available FRUs

You can determine which FRUs pertain to your controller enclosure using the CLI. Access the controller via a telnet client; log into the controller over the network (default user name `manage` and password `!manage`). If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the defaults shown above.

Enter a `show frus` query.

Execution of the `show frus` CLI command displays the FRU information pertaining to chassis (with midplane), controller module(s), and power supplies.

 **NOTE:** See *AssuredSAN 4000 Series CLI Reference Guide* for more information.

You can also determine which FRUs pertain to your controller enclosure by visual inspection of the component, noting serial number and part number. This method applies to disk drives. FRUs and FRU make-up are subject to change independent of documentation versions.

See Dot Hill's products: <http://www.dothill.com/products> page for the latest product information. For interoperability information, see Dot Hill's Customer Resource Center (CRC) website: <http://crc.dothill.com>.

Product overview

 **NOTE:** Tables and companion illustrations show FRUs for 4000 Series products.

[Table 38](#) provides summary descriptions of the individual product models comprising the 4000 Series product line.

Table 38 Individual product models comprising 4000 Series

AssuredSAN 4000 Series Controller enclosures					
2.5" 24-drive Controller enclosures (SFF)			3.5" 12-drive Controller enclosures (LFF)		
Model	Description	Form	Model	Description	Form
4720	FC host ports	2U24	4730	FC host ports	2U12
4520	SAS host ports	2U24	4530	SAS host ports	2U12

[Table 39](#) on page 208 shows components for the 2.5" 24-drive enclosure models (also 2U24). [Table 40](#) on page 211 shows components for the 3.5" 12-drive enclosure models (also 2U12).

Tables and supporting illustrations (following tables) show components for the 4000 Series product line that can be ordered for replacement in the field. Contact your account manager for packaged FRU numbers and ordering information. Data addressing 4000 Series 24-drive and 12-drive enclosure products is provided to supplement the illustrated replacement procedures described in [Troubleshooting and replacing FRUs](#).

The illustrations following herein show various 2U24 and 2U12 chassis used in 24-drive and 12-drive enclosures, respectively. These chassis support controller enclosure and drive (expansion) enclosure configurations.

FRUs addressing 24-drive enclosures

Table 39 4000 Series product components for 24-drive enclosures

Item	Enclosure component descriptions
1	Disk drive (SFF) a. 2.5" disk drive module (various models of differing storage capacities: SAS, SSD) b. Air management module (disk drive blank to maintain optimum air flow within enclosure)
2	Ear kit a. Left ear assembly (including ear cap) b. Right ear assembly (including ear cap) Also see Enclosure bezel for 24-drive models on page 210
3	Chassis
4	Midplane (included with chassis)
5	Power supplies (one shown) a. AC PSU for enclosure (newer power supplies do not have a power switch) b. DC PSU for enclosure
6	Controller module for enclosure (one shown) a. 4720, 1RM, FC, 4-port b. 4520, 1RM, SAS, 4-port
7	Enclosure cover (included with chassis)

 **NOTE:** The following illustrations visually describe [Table 39](#) components:

- Exploded view: [Figure 30](#) on page 209
- Assembly: [Figure 31](#) on page 209
- Internal components sub-assembly: [Figure 32](#) on page 210

[Figure 30](#) through [Figure 32](#) are shown with the enclosure bezel removed

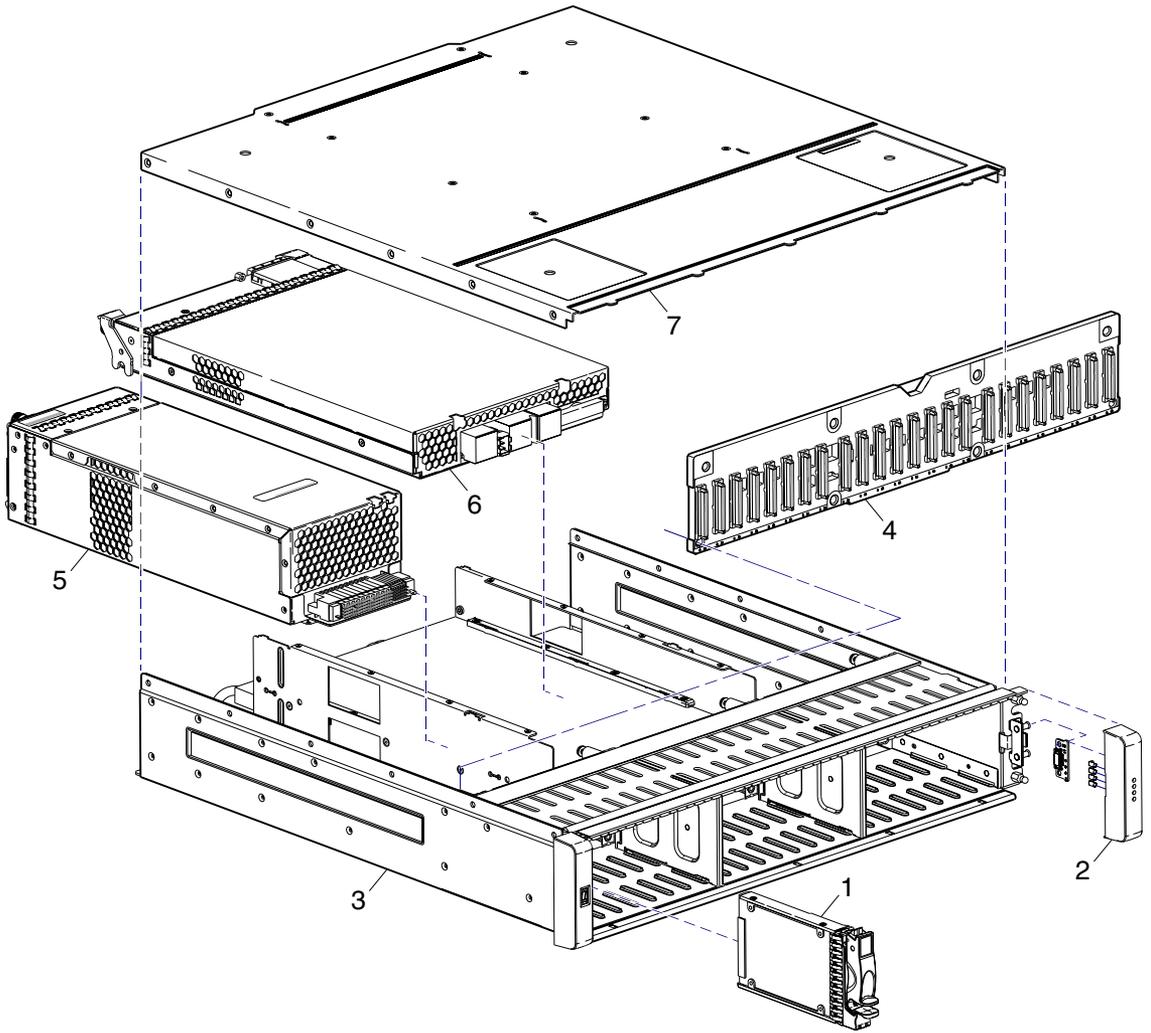


Figure 30 Controller enclosure exploded view (2U24)

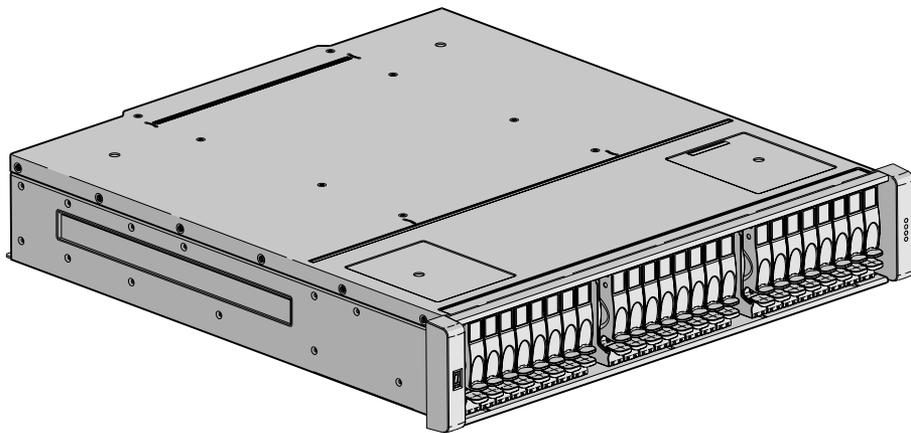


Figure 31 Controller enclosure assembly (2U24)

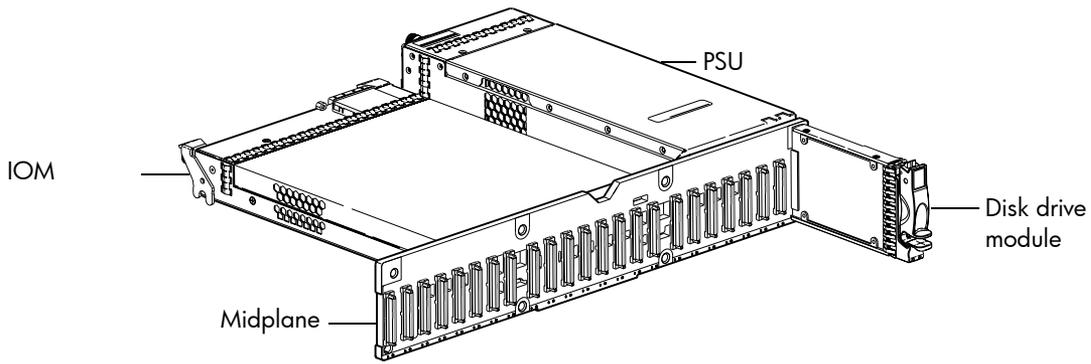


Figure 32 Controller enclosure architecture — internal components sub-assembly (2U24)

Enclosure bezel for 24-drive models

Newer models of the SFF 24-drive enclosure support a bezel sub-assembly that attaches to the front of the chassis (see [Figure 33](#) on page 210). The bezel—comprised of a vented sheet metal cover secured to an ear cap on each end—is pre-assembled and packed with foam into a box included in the master shipping container.

Alternatively, you can access the document online. For additional information, see Dot Hill’s Customer Resource Center (CRC) website: <http://crc.dothill.com>.

NOTE: The enclosure bezel geometry shown in illustrations within this document may be slightly different than the bezel shipped with your product, but the ball stud attachment points are the same.

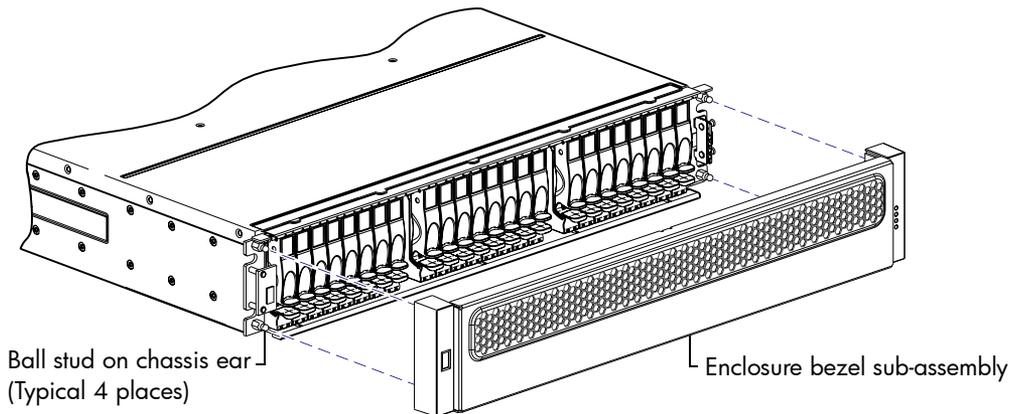


Figure 33 Partial controller enclosure assembly showing alignment for 24-drive enclosure bezel

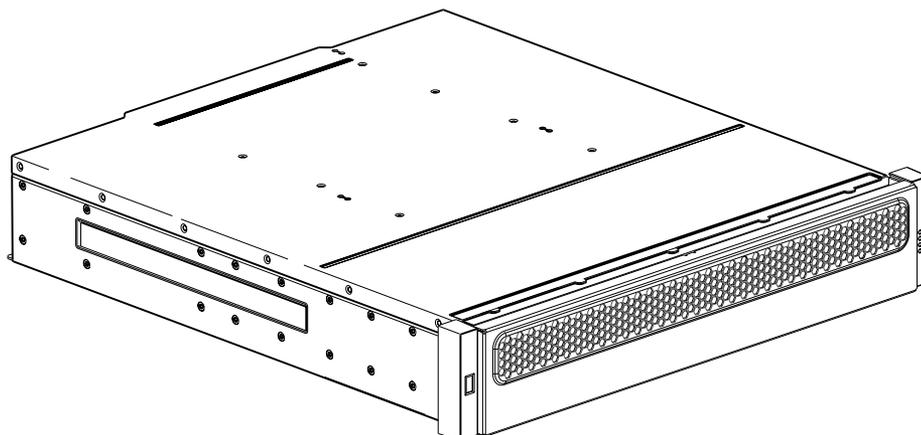


Figure 34 Controller enclosure assembly with 24-drive enclosure bezel installed

FRUs addressing 12-drive enclosures

Table 40 4000 Series product components for 12-drive enclosures

Item	Enclosure component descriptions
1	Disk drive (LFF without dongle) <ul style="list-style-type: none">a. 3.5" disk drive module (various models of differing storage capacities: SAS)b. Air management module (disk drive blank to maintain optimum air flow within enclosure)
2	Chassis
3	Midplane (included with chassis)
4	Power supplies (one shown) <ul style="list-style-type: none">a. AC PSU for enclosure (newer power supplies do not have a power switch)b. DC PSU for enclosure
5	Controller module for enclosure (one shown) <ul style="list-style-type: none">a. 4730, 1RM, FC, 4-portb. 4530, 1RM, SAS, 4-port
6	Enclosure cover (included with chassis)
Not Shown	Enclosure bezel sub-assembly featuring EMI shield and removable air filter (see Enclosure bezel for 12-drive model on page 213)

 **NOTE:** The following illustrations visually describe [Table 40](#) components:

- Exploded view: [Figure 35](#) on page 212
- Assembly: [Figure 36](#) on page 212
- Internal components sub-assembly: [Figure 37](#) on page 212

[Figure 35](#) through [Figure 37](#) are shown with the enclosure bezel removed.

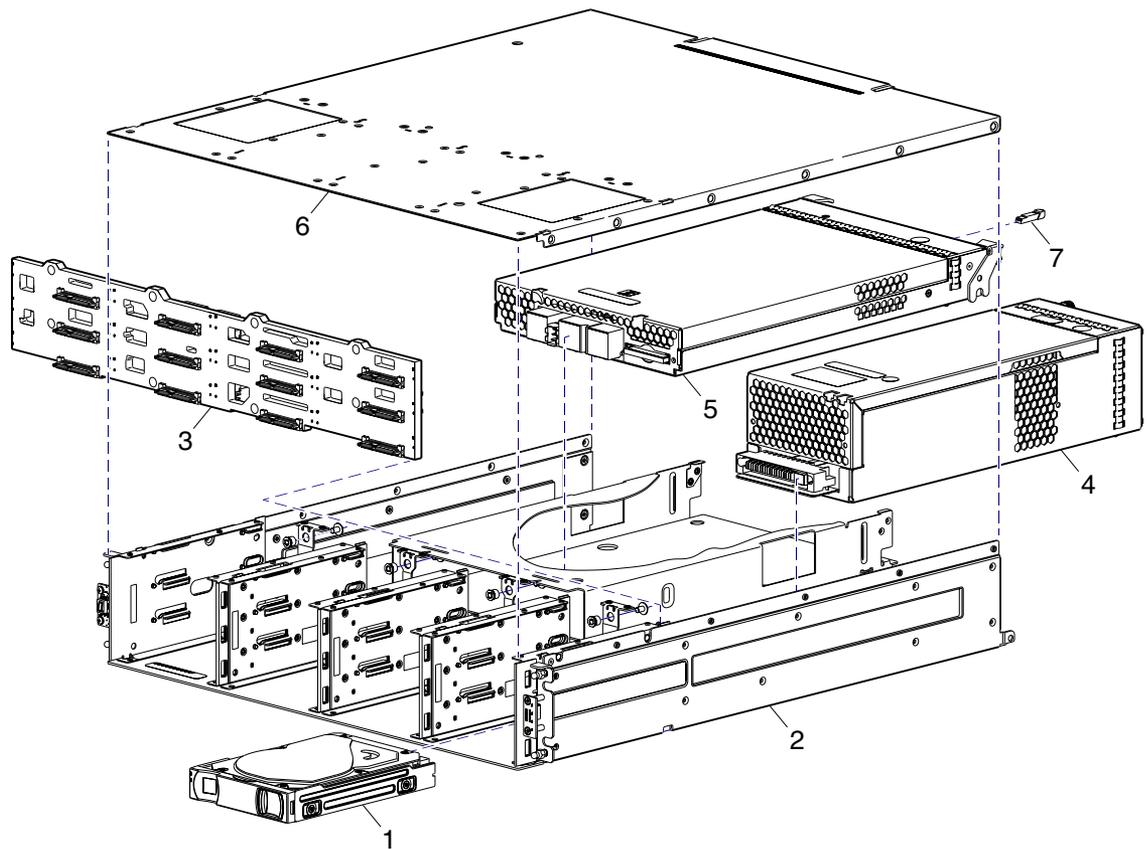


Figure 35 Controller enclosure exploded view (2U12)

The enclosure illustration in [Figure 35](#) intentionally does not show exploded ear covers. See [Figure 38](#) on page 213 for an illustration showing how the bezel aligns for attachment to the enclosure front panel, via press-fit onto four mounting ball studs located on chassis ears.

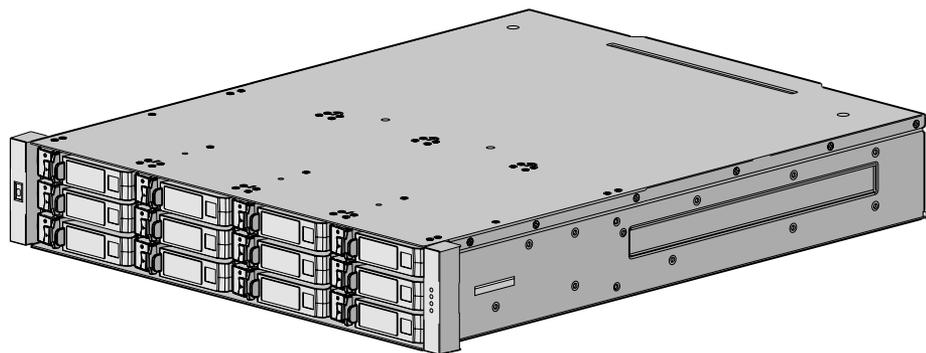


Figure 36 Controller enclosure assembly (2U12)

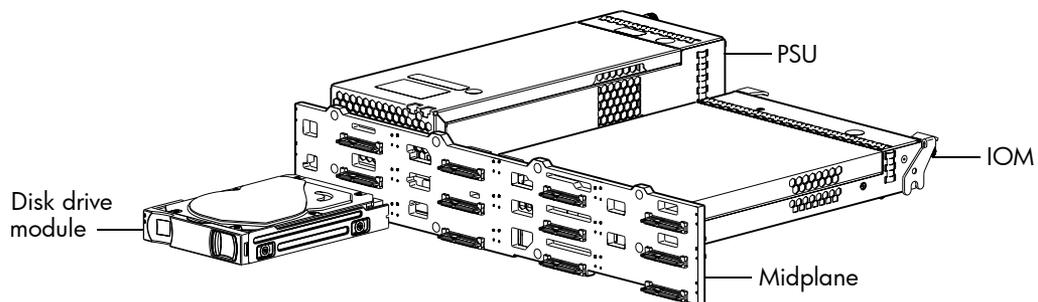


Figure 37 Controller enclosure architecture — internal components sub-assembly (2U12)

Enclosure bezel for 12-drive model

The 12-drive enclosure includes a bezel sub-assembly that attaches to the front of the chassis (see [Figure 38](#)). The bezel — comprised of a vented cover attached to an EMI shield — is pre-assembled and foam-packed within a box contained in the enclosure master shipping container. The bezel might optionally include a removable air filter that can be serviced or replaced. Hard copy instructions for attaching/removing the bezel, and for servicing or replacing the air filter, are provided in the shipping container of a new enclosure.

Alternatively, you can access the document online. For additional information, see Dot Hill's Customer Resource Center (CRC) website: <http://crc.dothill.com>.

 **NOTE:** The air filter is optional and may or may not be used in your product.

 **CAUTION:** Whether configured with or without an air filter, to ensure adequate EMI protection for the disk drives, the bezel should be properly installed while the enclosure is in operation.

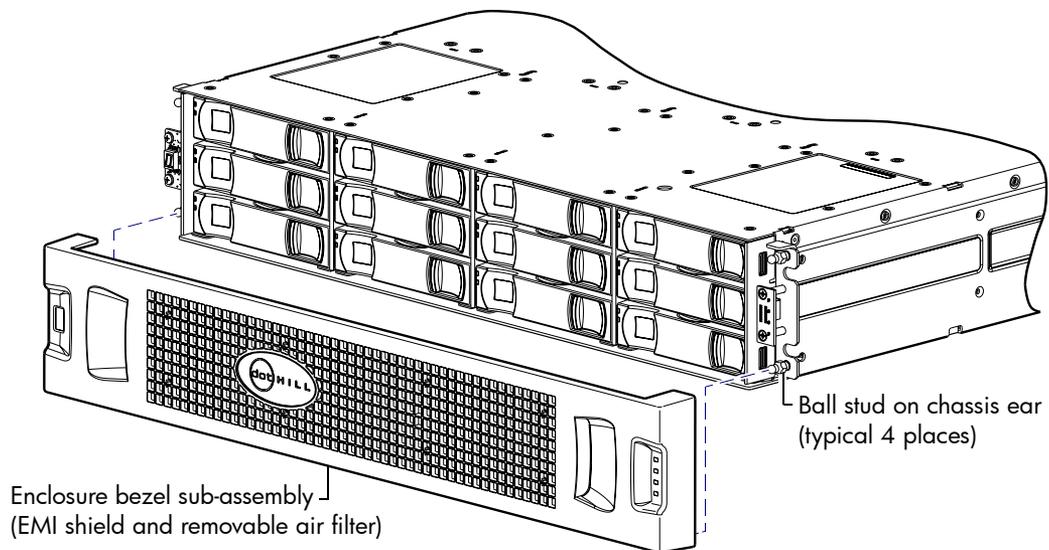


Figure 38 Partial controller enclosure assembly showing bezel alignment (2U12)

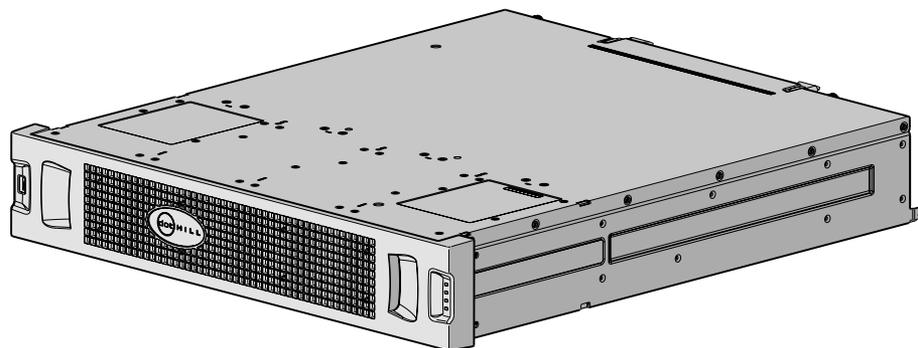


Figure 39 Controller enclosure assembly with bezel installed (2U12)

Glossary

array	See storage system
atomic write	A mode that guarantees if a failure (such as I/O being aborted or a controller failure) interrupts a data transfer between a host and the storage system, controller cache will contain either all the old data or all the new data, not a mix of old and new data. This option has a slight performance cost because it maintains a secondary copy of data in cache so that if a data transfer is not completed, the old cache data can be restored.
auto-write-through	See AWT.
available disk	A disk that is not being used in a vdisk, is not configured as a spare, and is not in the leftover state. It is available to be configured as a part of a vdisk or as a spare. See also compatible disk, dedicated spare, dynamic spare, and global spare.
AWT	Auto-write-through. A setting that specifies when the RAID controller cache mode automatically changes from write-back to write-through.
CAPI	Configuration Application Programming Interface. A proprietary protocol used for communication between the SC and the MC in a controller module. CAPI is always enabled.
chassis	The sheetmetal housing of an enclosure.
chunk size	The amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk.
compatible disk	A disk that can be used to replace a failed member disk of a vdisk because it both has enough capacity and is of the same type (SAS SSD, enterprise SAS, or midline SAS) as the disk that failed. See also available disk, dedicated spare, dynamic spare, and global spare.
complex programmable logic device	See CPLD.
Configuration Application Programming Interface	See CAPI
controller A (or B)	A short way of referring to controller module A (or B).
controller enclosure	An enclosure that contains one or two controller modules.
controller module	A FRU that contains the following subsystems and devices: an SC processor; an MC processor; a SAS expander and an EC 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 <i>A</i> and the lower one is designated <i>B</i> .
CPLD	Complex programmable logic device. An electronic component used to build reconfigurable digital circuits. It can replace large numbers of logic gates.
CRC	Cyclic Redundancy Check. A mathematical algorithm that, when implemented in software or hardware, can be used to detect errors in data.
CSV	Comma separated values. A format to store tabular data in plain-text form.
Cyclic Redundancy Check	See CRC.
DAS	Direct Attach Storage. A dedicated storage device that connects directly to a host without the use of a switch.
Data Encryption Standard	See DES.
DDR	Double data rate. A class of memory integrated circuits use in computers.

dedicated spare	A disk that is reserved for use by a specific vdisk to replace a failed disk. See also available disk, compatible disk, dynamic spare, and global spare.
default mapping	Host-access settings that are configured when a volume is created, and that apply to all hosts that are not explicitly mapped to that volume using different settings. See also explicit mapping and masking.
DES	Data Encryption Standard. An algorithm for the encryption of electronic data.
DHCP	Dynamic Host Configuration Protocol. A network configuration protocol for hosts on IP networks.
Direct Attach Storage	See DAS.
double data rate	See DDR.
drive enclosure	An enclosure that contains one or two expansion modules. Drive enclosures can be connected to a controller enclosure to provide additional storage capacity.
drive spin down	See DSD.
DSD	Drive spin down. A power-saving feature that monitors disk activity in the storage system and spins down inactive SAS disks based on user-selectable policies.
dual-port disk	A disk that is connected to both controllers so its data path is fault-tolerant.
Dynamic Host Configuration Protocol	See DHCP.
dynamic spare	An available disk that is automatically assigned, if the dynamic spares option is enabled, to replace a failed disk in a vdisk. See also available disk, compatible disk, dedicated spare, and global spare.
EC	Expander Controller. A processor, located in the SAS expander in each controller module and expansion module, that controls the SAS expander and provides SES functionality. See also EMP, MC, and SC.
electromagnetic interface	See EMI.
EMI	Electromagnetic interface.
EMP	Enclosure management processor. An EC subsystem that provides SES data such as temperature, PSU and fan status, and the presence or absence of disks.
enclosure	A physical storage device that contains disk drives and other FRUs.
enclosure management processor	See EMP.
Expander Controller	See EC.
expansion enclosure	See drive enclosure.
expansion module	A FRU that contains the following subsystems and devices: a SAS expander and EC processor; host, expansion, and service ports; and midplane connectivity. In a drive enclosure, the upper expansion module is designated <i>A</i> and the lower one is designated <i>B</i> .
explicit mapping	Access settings for a host to a volume that override the volume's default. 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 volumes, cache data, host ID information, and LUNs and WWNs. See also Host, LUN, recovery, volume, and WWN.
FC-AL	Fibre Channel Arbitrated Loop. The FC topology in which devices are connected in a one-way loop.
Fibre Channel Arbitrated Loop	See FC-AL.
field-programmable gate array	See FPGA.

field-replaceable unit	See FRU.
FPGA	Field-programmable gate array. An integrated circuit designed to be configured after manufacturing.
FRU	Field-replaceable unit. A part that can be removed and replaced by the user or support technician without having to send the product to a repair facility.
global spare	A compatible disk that is reserved for use by any vdisk to replace a failed disk. See also compatible disk and vdisk. See also available disk, compatible disk, dedicated spare, and dynamic spare.
HBA	Host bus adapter. A device that facilitates I/O processing and physical connectivity between a host and the storage system.
host	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. Product interfaces use the terms host and initiator interchangeably.
host port	A port on a controller module that interfaces to a host computer, either directly or through a network switch.
host bus adapter	See HBA.
I/O Manager	A MIB-specific term for a controller module.
I/O module	See IOM.
IOM	I/O module. An IOM can be either a controller module or an expansion module.
JBOD	"Just a bunch of disks." See also drive enclosure.
large form factor	See LFF.
LBA	Logical Block Address. The address used for specifying the location of a block of data.
leftover	The state of a disk that the system has excluded from a vdisk because the timestamp in the disk's metadata is older than the timestamp of other disks in the vdisk, or because the disk was not detected during a rescan. A leftover disk cannot be used in another vdisk until the disk's metadata is cleared; for information and cautions about doing so, see documentation topics about clearing disk metadata.
LFF	Large form factor. A type of disk drive.
LIP	Loop Initialization Primitive. An FC primitive used to determine the loop ID for a controller.
Logical Block Address	See LBA.
Logical Unit Number	See LUN.
loop	FC-AL topology.
Loop Initialization Primitive	See LIP.
LUN	Logical Unit Number. A number that identifies a mapped Volume to a host.
MAC Address	Media Access Control Address. A unique identifier assigned to network interfaces for communication on a network.
Management Controller	See MC.
Management Information Base	See MIB.
map/mapping	Settings that specify whether a volume is presented as a storage device to a host, 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, explicit mapping, and masking.
masking	A volume-mapping setting that specifies no access to that volume by hosts. See also default mapping, explicit mapping, and map/mapping.

MC	Management Controller. A processor located in a controller module that is responsible for human-computer interfaces and computer-computer interfaces, including the WBI, CLI, and FTP interfaces, and interacts with the SC. See also EC and SC.
Media Access Control Address	See MAC Address.
metadata	Data in the first sectors of a disk drive that stores all disk-, vdisk-, and volume-specific information including vdisk membership or spare ID, vdisk ownership, volumes in the vdisk, host mapping of volumes, and results of the last media scrub.
MIB	Management Information Base. A database used for managing the entities in SNMP.
network port	An Ethernet port on a controller module through which its MC is connected to the network.
network time protocol	See NTP.
NTP	Network time protocol.
orphan data	See unwritable cache data.
Partner Firmware Upgrade	See PFU.
PCBA	Printed circuit board assembly. A printed circuit board populated with electronic components.
PFU	Partner Firmware Upgrade. The automatic update of the partner controller when the user updates firmware on one controller.
PHY	One of two hardware components that form a physical connection between devices in a SAS network that enables transmission of data.
physical layer	See PHY.
point-to-point	The FC topology where two ports are directly connected.
POST	Power-On Self Test. Tests that run immediately after a device is powered on.
Power-on Self Test	See POST.
Power Supply Unit	See PSU.
printed circuit board assembly	See PCBA.
PSU	Power Supply Unit. The power supply FRU.
RAID head	See controller enclosure.
real-time clock	See RTC.
recovery	In an active-active configuration, recovery is the act of returning ownership of controller resources to a controller (which was offline) from its partner controller. The resources include volumes, cache data, host ID information, and LUNs and WWNs. See also failover.
remote syslog support	See syslog.
RTC	Real-time clock. A circuit in the controller module that maintains the date and time. The RTC has a battery backup that maintains the time even when there is no power attached to the module.
SC	Storage Controller. A processor located in a controller module that is responsible for RAID controller functions. The SC is also referred to as the RAID controller. See also EC and MC.
SCSI Enclosure Services	See SES.
secure shell	See SSH.
SEEPROM	Serial electrically erasable programmable ROM. A type of nonvolatile (persistent if power removed) computer memory used as FRU ID devices.
Self-Monitoring Analysis and Reporting Technology	See SMART.

serial electrically erasable programmable ROM	See SEEPROM.
SES	SCSI Enclosure Services. The protocol that allows the initiator to communicate with the enclosure using SCSI commands.
SFF	Small form factor. A type of disk drive.
small form factor	See SFF.
SMART	Self-Monitoring Analysis and Reporting Technology. A monitoring system for disk drives that monitors reliability indicators for the purpose of anticipating disk failures and reporting those potential failures.
SMI-S	Storage Management Initiative - Specification. The SNIA standard that enables interoperable management of storage networks and storage devices. The interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques.
SNIA	Storage Networking Industry Association. An association regarding storage networking technology and applications.
SSH	Secure Shell. A network protocol for secure data communication.
Storage Controller	See SC.
Storage Management Initiative - Specification	See SMI-S.
Storage Networking Industry Association	See SNIA.
storage system	A controller enclosure with at least one connected drive enclosure. Product documentation and interfaces use the terms storage system and system interchangeably.
syslog	Remote syslog support. A configuration that, when enabled, sends selected event messages to the syslog on a remote system.
ULP	Unified LUN Presentation. A RAID controller feature that enables a host to access mapped volumes through either controller's host ports. ULP incorporates ALUA extensions.
Unified LUN Presentation	See ULP.
Uninterruptible Power Source	See UPS.
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. Unwritable cache data is also called orphan data.
UPS	Uninterruptible Power Source.
vdisk	A virtual disk comprised of the capacity of one or more physical disks. The number of disks that a vdisk can contain is determined by its RAID level.
virtual disk	See vdisk.
volume	A portion of the capacity of a vdisk that can be presented as a storage device to a host.
web-based interface/web-browser interface	See WBI.
WBI	Web-based interface/web-browser interface. The primary interface for managing the system. A user can enable the use of HTTP, HTTPS for increased security, or both.
World Wide Name	See WWN.
World Wide Node Name	See WWNN.
World Wide Port Name	See WWPN.

WWN	World Wide Name. A globally unique 64-bit number that identifies a device used in storage technology.
WWNN	World Wide Node Name. A globally unique 64-bit number that identifies a node.
WWPN	World Wide Port Name. A globally unique 64-bit number that identifies a port.

Index

Numerics

- 4000 Series
 - product overview table [207](#)

A

- audience [13](#)

B

- bezel
 - enclosure, removing [134](#)
- bezel ear kits
 - 2U24 [135](#)

C

- cache
 - clearing [38](#)
 - enable/disable auto-write-back [47](#)
 - set host access to [48](#)
 - chassis
 - 2U12 [211](#)
 - 2U24 [208](#)
 - CLI
 - accessing [207](#)
 - default password [207](#)
 - default user name [207](#)
 - more information [207](#)
 - show FRUs (show frus) command [207](#)
 - CLI help, view command [37](#)
 - collecting data from an offline vdisk [84](#)
 - CompactFlash
 - properties [24](#)
 - CompactFlash failure trigger
 - enable/disable [48](#)
 - components
 - PSU, AC [201](#)
 - PSU, DC [201](#)
 - controller
 - notify partner when auto-write-through is triggered [49](#)
 - controller failure trigger
 - enable/disable [48](#)
 - controller module
 - properties [23](#)
 - controller modules
 - IOM blank [104](#)
 - controller redundancy mode, showing [75](#)
 - conventions
 - document [14](#)
 - create
 - tasks [42](#)
- ## D
- data paths
 - isolating faults [33](#)

- debug interface
 - enable/disable [55](#)
 - debug log parameters
 - setting [51](#)
 - viewing [58](#)
 - default configuration settings, restoring [45](#)
 - delete
 - schedules [43](#)
 - disabled PHY [34](#)
 - disk
 - air management modules [121](#)
 - enable/disable background scrub [47](#)
 - enable/disable SMART [49](#)
 - enable/disable spin down [50](#)
 - errors [118](#), [125](#)
 - fault [119](#)
 - faults, identifying [27](#)
 - identifying fault [27](#)
 - LEDs [91](#)
 - LEDs, 2U12 [198](#)
 - LEDs, 2U24 [197](#)
 - LEDs, Fault [199](#)
 - LEDs, general [199](#)
 - LEDs, Power/Activity [199](#)
 - LEDs, SFF [125](#)
 - LEDs, specific states [200](#)
 - LEDs, troubleshooting [95](#)
 - leftover [26](#), [39](#)
 - LFF [211](#)
 - locating [27](#)
 - metadata, clear [39](#)
 - metadata, clearing [26](#)
 - missing [124](#)
 - properties [21](#), [22](#)
 - removing [122](#)
 - replacing [121](#)
 - set spin-down delay [50](#)
 - SFF [208](#)
 - show data transfer rate [23](#)
 - document
 - conventions [14](#)
 - prerequisite knowledge [13](#)
 - related documentation [13](#)
 - dynamic spares
 - enable/disable [48](#)
- ## E
- electrostatic discharge [103](#)
 - grounding methods [103](#)
 - precautions [103](#)
 - EMP polling rate
 - set [48](#)

- enclosure
 - properties [22](#)
 - viewing information about [21](#)
- enclosure status, showing [76](#)
- enclosures, re-evaluate IDs [30](#)
- error code [149](#)
- errors
 - PHY [34](#)
- event code [89](#)
- event log
 - clear [40](#)
 - viewing [25](#)
- event logs
 - viewing using RAIDar [87](#)
- event severity [89](#)
- event severity icons [25](#)
- events
 - clear log [40](#)
 - code [89](#)
 - log [25](#)
 - log file [89](#), [149](#)
 - severity [87](#), [89](#)
 - showing [63](#)
 - SMI-S [149](#)
 - SNMP [149](#)
 - viewing logs using RAIDar [87](#)
- expander fault isolation, enabling or disabling [52](#)
- expander PHYs, enabling or disabling [53](#)
- expander status and error counters, clearing [40](#)
- expander status, showing [66](#)
- expansion module
 - properties [24](#)
- expansion port
 - properties [24](#)

F

- fan failure trigger
 - enable/disable [48](#)
- fault
 - expansion port connection [100](#)
- faults
 - cable [115](#)
 - data path, isolating [33](#)
 - disk [119](#)
 - disk, identifying [27](#)
 - external data path, isolating [35](#)
 - identifying disk [27](#)
 - internal data path, isolating [34](#)
 - isolating data path [33](#)
 - isolating, expansion port connection fault [100](#)
 - isolating, host-side connection [98](#)
 - isolating, methodology [15](#)
 - isolation [34](#)
 - LEDs [199](#)
 - PSU [129](#), [195](#)
 - troubleshooting, expansion port connection [100](#)
 - troubleshooting, host-side connection [98](#)
 - vdisk [126](#)

- firmware
 - dual controller [106](#)
 - update [111](#)
 - updating controller module [111](#), [112](#)
 - updating expansion module [114](#)
 - updating, disk [119](#)
- firmware update, partner
 - enable/disable [49](#)
- firmware, updating [111](#)
- FRU information, showing [69](#)
- FRUs
 - available for 4000 Series
 - determining FRU identifiers [207](#)
 - enclosure assembly
 - 2U12 [213](#)
 - 2U24 [209](#)
 - illustrated parts breakdown
 - 2U24 [209](#)
 - internal components sub-assembly
 - 2U12 [212](#)
 - 2U24 [210](#)
 - Interoperability Matrix (CRC) [207](#)
- FTP interface
 - enable/disable [55](#)

G

- global spares
 - enable/disable spin down [50](#)
 - set spin-down delay [50](#)

H

- host access to cache
 - set [48](#)
- host channel
 - See* host ports
- host link
 - See* host ports
- host port
 - properties [24](#)
- host ports
 - reset [44](#)
- hosts
 - stopping I/O [17](#), [106](#)
- HTTP interface
 - enable/disable [55](#)
- HTTPS interface
 - enable/disable [55](#)

I

- icons, event severity [25](#)
- In port
 - properties [25](#)
- independent cache performance mode
 - set [48](#)
- installing
 - air management module [124](#)
 - bezel, ear [137](#)
 - chassis [141](#)

- controller module [108](#)
- expansion module [108](#)
- PSU [132](#)
- SFP module [138](#)

IOM

- properties [24](#)

L

LEDs

- 2U12 front panel, disk [198](#)
- 2U12 front panel, Enclosure ID [198](#)
- 2U12 front panel, FRU OK [199](#)
- 2U12 front panel, Temperature Fault [199](#)
- 2U12 front panel, Unit Locator [199](#)
- 2U24 front panel, disk [197](#)
- 2U24 front panel, Enclosure ID [197](#)
- 2U24 front panel, Fault/Service Required [197](#)
- 2U24 front panel, FRU OK [198](#)
- 2U24 front panel, Temperature Fault [198](#)
- 2U24 front panel, Unit Locator [197](#)
- 4520/4530 rear panel, Cache Status [203](#)
- 4520/4530 rear panel, Expansion Port Status [203](#)
- 4520/4530 rear panel, Fault/Service Required [203](#)
- 4520/4530 rear panel, FRU OK [203](#)
- 4520/4530 rear panel, Link Activity [203](#)
- 4520/4530 rear panel, Link Status [203](#)
- 4520/4530 rear panel, Network Port Activity [203](#)
- 4520/4530 rear panel, Network Port Link Status [203](#)
- 4520/4530 rear panel, OK to Remove [203](#)
- 4520/4530 rear panel, Unit Locator [203](#)
- 4720/4730 rear panel, Cache Status [202](#)
- 4720/4730 rear panel, Expansion Port Status [202](#)
- 4720/4730 rear panel, Fault/Service Required [202](#)
- 4720/4730 rear panel, FRU OK [202](#)
- 4720/4730 rear panel, Link Activity [202](#)
- 4720/4730 rear panel, Link Status [202](#)
- 4720/4730 rear panel, Network Port Activity [202](#)
- 4720/4730 rear panel, Network Port Link Status [202](#)
- 4720/4730 rear panel, OK to Remove [202](#)
- 4720/4730 rear panel, Unit Locator [202](#)
- controller enclosure, rear panel [201](#)
- controller module [106](#), [143](#)
- disk [91](#)
- disk drive module
 - SFF [125](#)
- disk, Fault [199](#)
- disk, general [199](#)
- disk, Power/Activity [199](#)
- disk, specific states [200](#)
- enclosure status [91](#)
- enclosure status, front panel [142](#)
- enclosure, rear panel [142](#)
- expansion module [94](#)
- expansion port [92](#)
- illuminating disk Power/Activity/Fault [54](#)
- illuminating enclosure Unit Locator [54](#)
- network port [92](#)
- PSU [93](#), [97](#)
- PSU, AC [134](#), [205](#)
- PSU, DC [134](#), [205](#)
- status [93](#)
- link rate adjustment [23](#)
- log file
 - event messages [149](#)
 - events [89](#)
- log management
 - enable/disable [48](#)
- LUNs
 - set response to missing [49](#)

M

- managed logs
 - enable/disable [48](#)
- Management Controller, restarting [44](#)
- metadata
 - clear disk [39](#)
 - clearing disk [26](#)
- missing LUN response
 - set [49](#)
- missing parameter data error [37](#)

N

- network port
 - properties [23](#)

O

- Out port
 - properties [24](#), [25](#)

P

- PFU [105](#)
 - enable/disable [49](#)
- PHY
 - disabled [34](#)
 - errors [34](#)
 - fault isolation [34](#)
 - fencing [34](#)
 - rescan disks [34](#)
- power-on, problems after [30](#)
- prerequisite knowledge [13](#)
- priority
 - set utility [50](#)
- procedures
 - general precaution [103](#)
 - replacing a controller enclosure chassis [139](#)
 - components (common) [139](#)
 - components (model-specific) [139](#)
 - damaged chassis removal [141](#)
 - replacement chassis installation [141](#)
 - replacing a controller or expansion module [104](#)
 - replacing a disk drive module [121](#)
 - replacing a Fibre Channel SFP [137](#)
 - replacing a PSU [128](#)
 - replacing chassis FRUs [104](#)
- properties
 - CompactFlash [24](#)
 - controller module [23](#)

- disk [21](#), [22](#)
- enclosure [22](#)
- expansion module [24](#)
- expansion port [24](#)
- host port [24](#)
- In port [25](#)
- IOM [24](#)
- network port [23](#)
- Out port [24](#), [25](#)
- PSU [23](#)
- vdisk [20](#)
- protocols, service and security
 - enabling or disabling [55](#)
 - showing status of [74](#)
- PSU [128](#)
 - AC [201](#)
 - AC, compatibility [129](#)
 - AC, with power switch [130](#)
 - AC, without power switch [129](#)
 - DC [130](#), [201](#)
 - failure trigger, enable/disable [49](#)
 - faults [195](#)
 - faults and error conditions [129](#)
 - installing [132](#)
 - LEDs [93](#), [97](#)
 - LEDs, AC [134](#), [205](#)
 - LEDs, DC [134](#), [205](#)
 - power cable [133](#)
 - power cable, AC [133](#)
 - power cable, DC [133](#)
 - properties [23](#)
 - removing [131](#)
 - replacing [128](#)
 - sensors [145](#)
 - verifying component failure [129](#)

Q

- quarantine [28](#)

R

- RAIDar
 - locating a disk [27](#)
- reconstruct [27](#)
- redundancy mode, showing [75](#)
- related documentation [13](#)
- removing
 - bezel, ear [136](#)
 - bezel, enclosure [134](#)
 - chassis [141](#)
 - controller module [107](#)
 - disk [122](#)
 - expansion module [107](#)
 - PSU [131](#)
- replacing
 - controller enclosure chassis [139](#)
 - FC transceiver [137](#)
 - PSU [128](#)
- rescan
 - disks [34](#)

- restart, problems after [30](#)

S

- SAS expander. See expander and Expander Controller
- schedules
 - create [41](#)
 - delete [43](#)
- scrub
 - abort [38](#)
 - enable/disable background for disks [47](#)
 - enable/disable background for vdisks [47](#)
 - set interval for vdisk background [47](#)
- SCSI MODE SELECT command
 - set handling of [48](#)
- SCSI sense key [117](#)
- SCSI SYNCHRONIZE CACHE command
 - set handling of [49](#)
- sensors
 - fan [145](#)
 - PSU [145](#)
 - temperature [146](#)
 - voltage [147](#)
- SES interface
 - enable/disable [55](#)
- SFP transceiver
 - fibre-optic cable [137](#)
 - SFF pluggable [137](#)
- SMART
 - enable/disable [49](#)
- SMI-S
 - event logs [149](#)
- SMI-S interface
 - enable/disable secure [55](#)
 - enable/disable unsecure [56](#)
- SNMP
 - enable/disable interface [55](#)
 - event logs [149](#)
- spares
 - See also dedicated spare, dynamic spare, and global spare
- spin down
 - enable/disable for available disks and global spares [50](#)
 - set delay for available disks and global spares [50](#)
- SSH interface
 - enable/disable [55](#)
- statistics
 - show vdisk performance [79](#)
 - show volume performance [83](#)
- Storage Controller, restarting [44](#)
- supercapacitor failure trigger
 - enable/disable [49](#)
- synchronize-cache mode
 - set [49](#)
- system
 - viewing event log [25](#)

T

task schedule

See schedules

tasks

 create [42](#)

 delete [43](#)

Telnet interface

 enable/disable [55](#)

temperature

 enable/disable controller shutdown for high [50](#)

troubleshooting

 enclosure IDs [30](#)

 expansion port connection [100](#)

 expansion port connection fault [100](#)

 host-side connection fault [98](#)

 host-side connection, SAS [99](#)

 LEDs, disk [91](#), [95](#)

 LEDs, enclosure status [91](#)

 LEDs, expansion module [94](#)

 LEDs, expansion port [92](#)

 LEDs, network port [92](#)

 LEDs, PSU [93](#)

 LEDs, rear panel [92](#)

 LEDs, status [93](#)

 performance [30](#), [35](#)

 tasks [36](#)

trusting an offline vdisk [84](#)

U

utility priority

 set [50](#)

V

vdisk

 abort scrub [38](#)

 enable/disable background scrub [47](#)

 properties [20](#)

 reconstructing [28](#)

 set interval for background [47](#)

 show performance statistics [79](#)

 status values [20](#)

 trusting an offline [84](#)

 viewing information about [20](#)

 viewing information about all [20](#)

volumes

 show performance statistics [83](#)

W

warnings

 temperature [145](#)

 voltage [145](#)

