



IBM SAS RAID Controller Module
Installation and User's Guide
IBM BladeCenter S SAS RAID Controller Module





IBM SAS RAID Controller Module
Installation and User's Guide
IBM BladeCenter S SAS RAID Controller Module

Note

Before using this information and the product it supports, read the information in the “Notices” on page 195 section.

Twentieth Edition (September 2015)

© Copyright IBM Corporation 2008, 2015.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Tables	v	Configuring blades for Microsoft Cluster Service ..	38
Chapter 1. Introduction	1	Chapter 8. Using the RAID Controller command line interface	53
Product description and package contents	2	Display commands	54
System requirements.	3	detail controller	54
Interface choices and functions	3	detail drive	55
Workflow notes	4	detail pool.	56
Documentation notes	4	detail volume.	57
Preinstallation safety information	5	detail volume verbose	59
Handling static-sensitive devices.	8	list controller	59
Hardware features and specifications	9	list drive	60
Component illustrations	10	list pool	61
Logical identifiers and physical location codes..	11	list volume	62
Option package contents	11	System control and configuration commands . .	62
Related documentation	12	alert	62
Chapter 2. Prerequisite hardware	13	battery	63
Understanding Battery Backup Units	13	cache settings.	64
Quick facts about Battery Backup Units	13	chpasswd	65
Installing the Battery Backup Unit	14	clilog	65
Removing the Battery Backup Unit hardware ..	15	commparams.	65
Chapter 3. Understanding the Telnet interface	17	configure access	66
Establishing a Telnet session to RAID Controller ..	17	configure alert	67
Chapter 4. Installing the IBM BladeCenter S SAS RAID Controller Module.	19	configure pool	68
Installation and setup	19	configure timeout	68
The Advanced Management Module method . . .	21	controller config.	69
Installing IBM Storage Configuration Manager ..	22	email alert.	70
User ID and password requirements	23	enclosure reporting	71
Resetting the passwords on an SAS RAID Module.	23	event log	72
Configuring storage through the CLI	24	locate	72
Upgrading from a single to a dual controller configuration	24	list features	75
Chapter 5. Disconnecting power to the BladeCenter unit	29	mountstate	75
Chapter 6. Updating firmware	31	post result.	77
Subscribing to notifications	32	service mode	77
Installing and configuring firmware updates . . .	32	shellscript	79
Chapter 7. Working with storage pools and volumes	33	show raid levels.	79
Understanding storage pools	33	shutdown	79
Understanding volumes	33	swversion	80
Understanding RAID levels	34	time	81
Understanding the predefined storage configuration	35	validate key	81
Configuring volumes for use with VMware. . . .	36	Volume management commands	82
		add mirror	82
		assimilate drive	82
		copyback	83
		create pool	84
		create volume	85
		delete pool	86
		delete volume	86
		global spare	87
		host	88
		hostlun	88
		Volume services commands	89
		add capacity	90
		datascrub	90
		delete all	91

expand -volume	91
initialize	92
list killedpaths	92
synchronize volume	93
view long running tasks	93
Using the command line to configure storage . .	94
Example of a RAID 5 configuration	94

Chapter 9. Configuring zones 97

Understanding the predefined zone	97
---	----

Chapter 10. Attaching an external tape device to the SAS RAID Module 99

Tape device considerations	99
Updating firmware prior to connecting a tape device	100
Installing and configuring a tape device	100

Chapter 11. Troubleshooting 101

Putting the IBM BladeCenter S SAS RAID Controller Module into service mode	101
Understanding LEDs	101
Performing advanced verification procedures. .	108
Understanding IBM BladeCenter S SAS RAID Controller Module alerts	109
System enclosure alerts	112
Drive enclosure alerts	114
Controller informational alert history log events	119
Controller informational alerts.	120
Controller warning alerts	121
Controller critical alerts	124
Battery informational alert history log events	127
Battery alerts	129
Disk drive informational alerts	132
Disk drive alerts	135
Drive group alerts.	143
Volume alerts	149
Host and connectivity alerts	151
Controller configuration alerts.	152
Understanding the logs	155
Capturing logs with the First Time Data Capture Utility	155
Command line parameters	156
Non-concurrent repair procedures	158
Replacing a single controller using the CLI ..	158
Replacing a single controller using the SCM ..	159
Replacing both controllers	161
Replacing 6-Disk storage module with 12-Disk Storage Module from Command Line Interface (CLI)	162
Updating controller firmware	164
Replacing a Disk Storage Module (non-concurrent procedure).	165
Replacing a media tray	166
Concurrent repair procedures	168
Replacing a single controller in a dual controller configuration using the CLI	168
Replacing a single controller in a dual controller configuration using the SCM	170
Replacing a failed drive	171

Replacing a Disk Storage Module	172
Removing and reinserting an active controller	177
Replacing a media tray	179
Replacing a Battery Backup Unit	181
Troubleshooting known issues.	184
Brown out conditions and the IBM BladeCenter S SAS RAID Controller Module	184
Data package collection in the intermediate state	185
VLAN 4095 with the Intelligent Copper Pass thru Module.	185
POST and TCP/XML communication error upon startup or reboot	186
RAID Controller critical and warning errors interfere with firmware update process. . . .	186
How to reset the SAS RAID controllers to the factory defaults.	187
Resolving DSM firmware mismatch issue when DSM_SFF is installed.	188

Appendix. Getting help and technical assistance. 191

Before you call	191
Using the documentation	192
Getting help and information from the World Wide Web	192
How to send DSA data to IBM	192
Creating a personalized support web page . . .	193
Software service and support	193
Hardware service and support	193
IBM Taiwan product service	193

Notices 195

Trademarks	196
Important notes	196
Particulate contamination	197
Documentation format	198
Telecommunication regulatory statement . . .	198
Electronic emission notices	199
Federal Communications Commission (FCC) statement.	199
Industry Canada Class A emission compliance statement.	199
Avis de conformité à la réglementation d'Industrie Canada	199
Australia and New Zealand Class A statement	199
European Union EMC Directive conformance statement.	200
Germany Class A statement	200
Japan VCCI Class A statement.	201
Japan Electronics and Information Technology Industries Association (JEITA) statement . .	202
Korea Communications Commission (KCC) statement.	202
Russia Electromagnetic Interference (EMI) Class A statement	202
People's Republic of China Class A electronic emission statement	202
Taiwan Class A compliance statement . . .	203

Index 205

Tables

1. Interfaces and functions	3	7. Tape devices supported by the IBM	
2. Important notes	4	BladeCenter S SAS RAID Controller Module .	99
3. Features	9	8. Light path diagnostics LED details	102
4. RAID levels and characteristics	34	9. Alert types generated by the RAID Controller	110
5. Drive configurations per RAID level for		10. Alert Attribute descriptions	111
DSM_LFF (DSM-6) enclosure.	35	11. Configuration and Log Files	155
6. Service mode conditions	77	12. Limits for particulates and gases	197

Chapter 1. Introduction

The IBM BladeCenter S SAS RAID Controller Module provides a fully-integrated shared storage solution in an IBM BladeCenter S chassis. This guide contains instructions for the installation of the IBM BladeCenter S SAS RAID Controller Modules (SAS RAID Modules) into an IBM BladeCenter S chassis. This guide also contains information about the interfaces you can use to configure and maintain your SAS RAID Modules and other associated components you might be using.

Data storage subsystems

Two subsystems are involved in IBM BladeCenter S data storage: the Disk Storage Module (DSM), and SAS RAID Module. The Disk Storage Module (DSM) is an enclosure holding up to six Disk Drive Modules (DDMs). There are a maximum of two DSMs installed in an IBM BladeCenter S chassis.

SAS RAID Module subsystems

The SAS RAID Module includes two subsystems: a RAID Controller subsystem, and a SAS Switch subsystem. The SAS RAID Modules provide a connection between the Blade servers and the DSMs that allow you to design storage configurations and volumes for your data.

In addition, a SAS Expansion Card must be installed in each blade server for the blades to connect to the RAID Data Storage subsystem and modules.

Firmware updates

The DDM, DSM, RAID Controller, and SAS Switch require firmware updates. Two methods of updating the firmware are as follows:

- IBM Storage Configuration Manager (SCM)

The IBM Storage Configuration Manager is a web-based system management application that you can use to update firmware on the IBM BladeCenter S SAS RAID Controller Module, DSM, and DDM, as well as manage and configure IBM® BladeCenter devices.

Note:

1. The IBM Storage Configuration Manager (SCM) is Not supported with RSSM systems on the firmware version 1.3.x.x and above.
2. Install IBM Storage Configuration Manager on an Ethernet connected workstation or laptop. For installation and configuration instructions, refer to the IBM Storage Configuration Manager documentation.

- SAS RAID Controller Firmware Update Package

The SAS RAID Controller Firmware Update Package is a CLI- based application package that you can use to update the IBM BladeCenter S SAS RAID Controller Module, DSM and DDM firmware. You can also write scripts automating firmware updates of single or multiple IBM BladeCenter S units.

Note: Install the SAS RAID Controller Firmware Update Package on an Ethernet connected workstation or laptop running a Windows or Linux operating system.

For more information about the RAID controller card, search for the *RAID Expansion Card Installation and User's Guide* at <http://www.ibm.com/systems/support/>.

For additional information about other BladeCenter components, see the instructions in your BladeCenter documentation.

Product description and package contents

The IBM BladeCenter S SAS RAID Controller Module provides fully-integrated RAID Storage Area Network (SAN) functionality, inside your IBM BladeCenter S chassis. Each IBM BladeCenter S SAS RAID Controller Module ships with the following:

- 43W3584 IBM BladeCenter S SAS RAID Controller Module Option
- 46C8000 Publication Package
- 90Y5612 Quick Start Manual
- 90Y5570 Support CD
- 90Y5611 Flyer
- 17P8568 L1 for Battery Backup Unit
- 22R6649 Top Level Assembly Battery Backup Unit
- 43W3604 L1 for IBM BladeCenter S SAS RAID Controller Module
- 17P9375 Aristos EULA
- 17P9277 Top Level Assembly IBM BladeCenter S SAS RAID Controller Module

The IBM BladeCenter S SAS RAID Controller Module consists of an integrated SAS Switch combined with a RAID Controller which provides an embedded RAID storage solution with advanced SAN features to the IBM BladeCenter S chassis. Your IBM BladeCenter S SAS RAID Controller Module features the IBM Storage Configuration Manager which provides end-to-end storage management:

- Fast and easy set up with the Initial Setup wizard
- System health monitoring
- Storage configuration (creates pools, defines volumes, and maps to hosts)
- SAS RAID Module maintenance including firmware updates and device user management
- Troubleshooting

Supported operating systems and drives

The *IBM BladeCenter Interoperability guide* provides a listing of the interoperability between operating systems, drive types, and other components supported for use with the IBM BladeCenter S SAS RAID Controller Module. This guide is updated periodically, so check this location for the latest copy: <https://www.ibm.com/systems/support/supportsite.wss/docdisplay?lnnodocid=MIGR-5073016&brandind=5000020>.

System requirements

The IBM BladeCenter S SAS RAID Controller Module functions only within the IBM BladeCenter S chassis. The following are also required:

- One or two IBM BladeCenter S SAS RAID Controller Modules. If you install two SAS RAID Modules, you must install them in I/O module bay 3 and I/O module bay 4. If you install one SAS RAID Module, you must install it in I/O module bay 3.
- One Battery Backup Unit for each IBM BladeCenter S SAS RAID Controller Module
- At least two hard disk drives for RAID configurations 0 and 1 or three hard disk drives for RAID 5
- An Advanced Management Module
- 2 power supplies per Disk Storage Module (DSM)
- A supported Ethernet switch
 - Nortel 1/10Gb Uplink Ethernet Switch Module (GbESM-1-10U) firmware (1.0.1.0)

Interface choices and functions

After you install the IBM BladeCenter S SAS RAID Controller Module, you can manage and configure it using the following interfaces:

Table 1. Interfaces and functions

Interface	Manage and configure
Use the Advanced Management Module Web interface to manage and configure:	<ul style="list-style-type: none">• IBM BladeCenter S SAS RAID Controller Module IP addresses• SAS Switch IP addresses <p>You can also use the Advanced Management Module to monitor the status of your IBM BladeCenter S chassis and related components</p>
Use the IBM Storage Configuration Manager to:	<ul style="list-style-type: none">• Create storage configuration• Grant host access to storage• Assign storage to hosts• Monitor controller status• Update controller code• Update SAS Switch firmware
Use the RAID Controller command line interface to:	<ul style="list-style-type: none">• Create storage configuration• Grant host access to storage• Assign storage to hosts• Monitor controller status• Update controller code using SAS RAID Controller Firmware Update Package
Use the SAS Switch command line interface to :	<ul style="list-style-type: none">• Monitor SAS Switch status• Update SAS Switch firmware
Use the SAS Switch Web interface to:	<ul style="list-style-type: none">• Monitor SAS Switch components

Workflow notes

There are several different tools and utilities that impact the way you begin using your IBM BladeCenter S SAS RAID Controller Module.

For example, if you are using the IBM Storage Configuration Manager application to configure your storage and data redundancies and maintain your firmware, the steps you take to accomplish this are more automated than if you are using the RAID Controller command line interface and, or the SAS RAID Controller Firmware Update Package to do these things. However, despite the manner in which you choose to accomplish your system storage configurations and maintenance, the IBM BladeCenter S SAS RAID Controller Module enables you configure your integrated storage solutions by performing the following:

- Create storage pools
- Define volumes for those pools
- Receive Logical Unit Numbers (LUNs) for those volumes
- Map those LUNs to hosts (servers) contained in the IBM BladeCenter S chassis.

Important: Before you begin the process of storage configuration, use the RAID Controller command line interface to set up your email to receive system alerts and log output.

Documentation notes

Table 2. Important notes

Summary
Throughout this document, the user name is also known as the login name, user identifier, or user ID for logging into one or more of the following interfaces or programs: <ul style="list-style-type: none">• Telnet interface• Web browser interface• Advanced management module Web interface• IBM Storage Configuration Manager Web interface Note: The IBM Storage Configuration Manager has two login screens: One to the server and the other to the RAID Controller. <ul style="list-style-type: none">• RAID Controller command line interface• SAS Switch command line interface• SAS Switch Web interface•
Requirement: Install two SAS RAID Modules in an IBM BladeCenter S chassis.
Requirement: To use the SAS RAID Modules, Battery Backup Units must be installed in bay 1 and bay 2 of the media tray.
You can obtain up-to-date information about the SAS RAID Modules and other IBM products at http://www.ibm.com/systems/support/

Table 2. Important notes (continued)

Summary
<p>The controller module has the following labels:</p> <ol style="list-style-type: none"> 1. Safety certification label 2. Product name label 3. Serial number label 4. Media access control (MAC) address label 5. SAS ID <p>The major components topic contains an illustration that shows the location of the SAS RAID Modules labels.</p> <p>Note: This information is required when you register the SAS RAID Modules with IBM.</p>

Preinstallation safety information

This topic contains important safety information. Read before installing this product.

Before installing this product, read the safety information (statements)

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 **Safety Information** (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་ཁུངས་འདི་བདེ་སྤྱད་མ་བྱས་གོང་། སྐྱོར་གྱི་ཡིད་གཟབ་
བྱ་འདྲ་མིན་ཡིད་བའི་འོད་ཟེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen
canjbinj soengq cungj vahgangj ancien siusik.

Statement 1



DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet.
- Connect to properly wired outlets any equipment that will be attached to this product.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

To Connect:

1. Turn everything OFF.
2. First, attach all cables to devices.
3. Attach signal cables to connectors.
4. Attach power cords to outlet.
5. Turn device ON.

To Disconnect:

1. Turn everything OFF.
2. First, remove power cords from outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

Statement 2



CAUTION:

When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- Throw or immerse into water
- Heat to more than 100°C (212°F)
- Repair or disassemble

Dispose of the battery as required by local ordinances or regulations.

Statement 21



CAUTION:

Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

Handling static-sensitive devices

Static electricity can damage electronic devices, including your blade server. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

To reduce the possibility of damage from electrostatic discharge, observe the following precautions:

- When you work on a IBM BladeCenter S chassis that has an electrostatic discharge (ESD) connector, use a wrist strap when you handle modules, optional devices, or blade servers. To work correctly, the wrist strap must have a good contact on both ends. It should touch your skin at one end and firmly connected to the ESD connector on the front or back of the IBM BladeCenter S chassis.
- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully: holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to any **unpainted** metal surface of the IBM BladeCenter S chassis or any **unpainted** metal surface on any other grounded component in the rack you are installing the device in for at least 2 seconds. (This drains static electricity from the package and from your body.)
- Remove the device from its package and install it directly into the blade server without setting down the device. If it is necessary to set down the device, place it back into its static-protective package. Do not place the device on your blade server cover or on a metal surface.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Hardware features and specifications

This section provides a summary of the features and specifications for the IBM BladeCenter S SAS RAID Controller Module.

The SAS RAID Modules support the following features:

- 6 internal 1X SAS 3.0 Gb host connectivity to 6 blade slots
- 2 internal 4X SAS 3.0Gb to 2 disk storage module (DSM) systems
- 1.0 Gb Ethernet for RAID management
- 10/100 Ethernet for Switch management
- Serial SAS Protocol
- Serial Management Protocol (SMP) as defined in the SAS specification
- Fourteen internal x1 links to Blade servers

The IBM BladeCenter S chassis takes advantage of the features of the IBM BladeCenter S SAS RAID Controller Module.

The following are standard features of the IBM BladeCenter S chassis:

- An Advanced Management Module
- Two or more power modules
- Four fan modules
- A media tray

You might receive additional features depending on what you ordered.

Table 3. Features

SAS RAID Module features	SAS RAID Module maintainability	SAS RAID Module electrical specifications:
<ul style="list-style-type: none">• SAS RAID Module and SAS expander• Vitesse 7157	<ul style="list-style-type: none">• Diagnostics: Power-on self-test (POST) is performed on all functional components. Port operational tests include internal, external, and online tests.• User interface: Light-emitting diode (LED) indicators	<ul style="list-style-type: none">• Power source loading: 2 amps maximum at 12 V dc• Heat output: 24 watts maximum• Operating voltage: 12 V dc• Circuit protection: Internally fused
Environmental:	Fabric management – methods:	Dimensions

Table 3. Features (continued)

SAS RAID Module features	SAS RAID Module maintainability	SAS RAID Module electrical specifications:
<ul style="list-style-type: none"> Temperature and altitude: <ul style="list-style-type: none"> Operating: <ul style="list-style-type: none"> 10°C to 52°C (50°F to 126°F) at an altitude of 0 to 914 m (0 to 2 998 ft) 10°C to 49°C (50°F to 120°F) at an altitude of 0 to 3 000 m (0 to 9 843 ft) Non-operating: <ul style="list-style-type: none"> -40°C to 65°C (-40°F to 149°F) at an altitude of 0 to 12 000 m (0 to 39 370 ft) Humidity: <ul style="list-style-type: none"> Operating: 8% to 80%, noncondensing Non-operating: 5% to 80%, noncondensing 	<ul style="list-style-type: none"> Advanced Management Module interface IBM Storage Configuration Manager interface Telnet and command line interface (CLI) Web-browser interface SAS connectivity module simple network management protocol (SNMP) agent <p>The SNMP agent enables a network management workstation to receive configuration values and SAS link data through SNMP and the Ethernet interface.</p>	<p>SAS RAID Module</p> <ul style="list-style-type: none"> Width: 112 mm (4.41 in.) Height: 29 mm (1.14 in.) Depth: 260 mm (10.25 in.) Weight: 2 lb (.91 kg) <p>Battery Backup Unit dimensions</p> <ul style="list-style-type: none"> Depth: 16.3 in [414.08 mm] Width: 3.10 in [78.65 mm] Height: 0.88 in [22.4 mm] Weight: 1.32 Kg (2.91 lbs)

Component illustrations

The following illustrations show the front and rear views of an IBM BladeCenter S chassis. Your hardware might have labels not shown in the following illustrations.

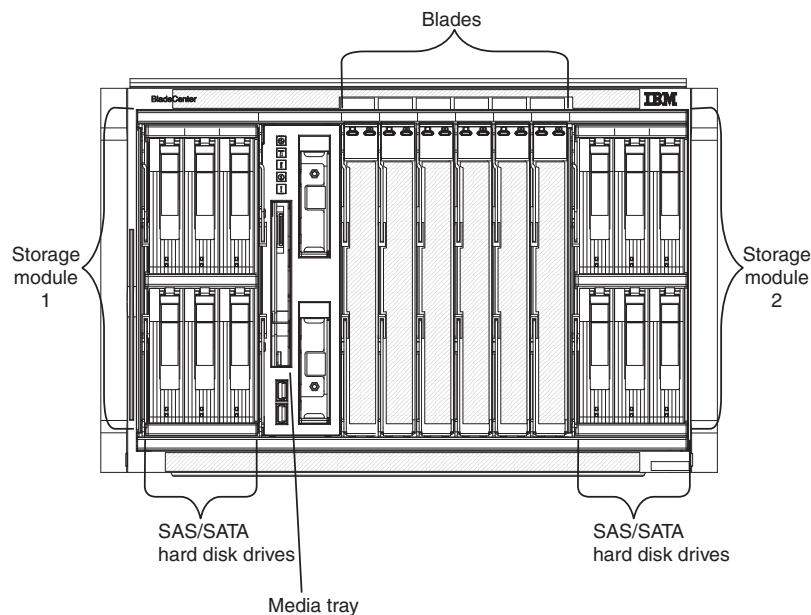


Figure 1. Front view of an IBM BladeCenter S chassis

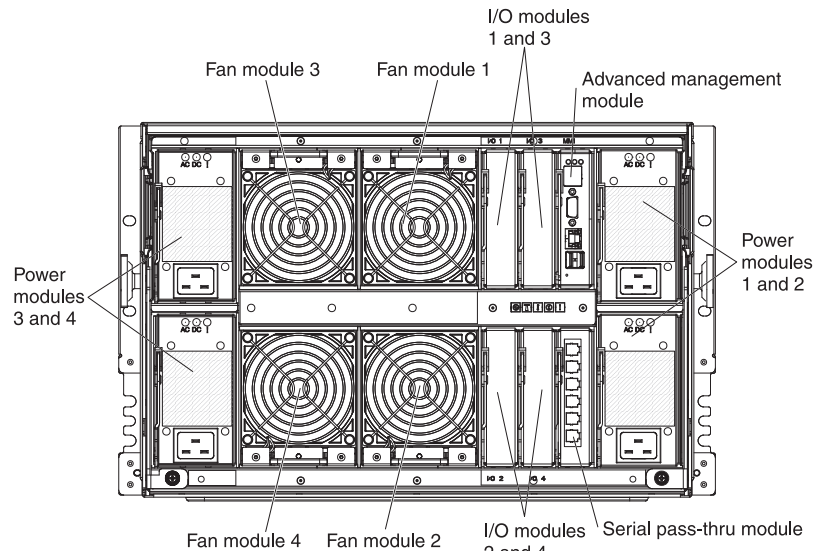


Figure 2. Back view of an IBM BladeCenter S chassis

Logical identifiers and physical location codes

You can use *logical identifiers* and *physical location codes* to locate resources in your system.

Use logical identifiers to identify a specific resource for commands, status, and messages. Use physical location codes to identify a specific resource in the physical world; this helps identify the exact location of a resource when you remove or replace them.

You can see logical identifiers and physical location codes in IBM Storage Configuration Manager by performing the following steps:

1. From the IBM Storage Configuration Manager navigation panel, select **Health > Physical View**. The Physical View page displays a graphical representation of the devices on your server.
2. Hover the mouse cursor over the resources that appear in the Physical View page to display the logical identifiers and physical location codes.

Option package contents

This topic describes the contents of the option package.

The connectivity module option package contains the following items:

- One IBM BladeCenter S SAS RAID Controller Module
- One Battery Backup Unit (45W5002) is bundled with each IBM BladeCenter S SAS RAID Controller Module.
- The RAID Controller Getting Started Guide
- The Support CD, which includes:
 - The RAID Controller and SAS Expansion Card *Installation and User's Guide*
 - The RAID Controller and SAS Expansion Card *Getting Started Guide*
 - IBM BladeCenter Storage Configuration Manager *Planning, Installation, and Configuration Guide*
 - SAS Expansion Card applications
 - MIB files
 - Readme file

Related documentation

This topic details additional documentation sources.

These installation topics are provided in Portable Document Format (PDF) on the support CD that came with your RAID Controller.

Additional related documentation might be included on the support CD or available on the IBM support Web site, <http://www.ibm.com/systems/support/>, along with the following related documentation:

- IBM BladeCenter *Installation and User's Guide* contains setup and installation instructions for your IBM BladeCenter S chassis, including information about getting started and how to install a blade server.
- IBM BladeCenter blade server *Installation and User's Guides*
Each type of blade server has a customized *Installation and User's Guide* that is provided in PDF on the IBM BladeCenter Documentation CD and at the IBM support site .
- The SAS Expansion Card (CFFv) for IBM BladeCenter Installation and User's Guide for IBM BladeCenter products contains installation instructions for the SAS Expansion Card. It also contains information about using the LSI Logic Configuration Utility program to configure the SAS Expansion Card.
- *Multilingual Safety Information*
This multilingual document is provided in PDF on the IBM *BladeCenter Documentation* CD and at <http://www.ibm.com/systems/support/>. It contains translated versions of the caution and danger statements that appear in the documentation for your blade server. Each caution and danger statement has an assigned number, which you can use to locate the corresponding statement in your native language.
- *Rack Installation Instructions*
This document contains the instructions to install your BladeCenter unit in a rack.
- IBM BladeCenter *Hardware Maintenance Manual and Troubleshooting Guide* or *Problem Determination and Service Guide*
Depending on your BladeCenter type, one of these documents is provided in PDF on the IBM *BladeCenter Documentation* CD and at <http://www.ibm.com/systems/support/>. It contains troubleshooting information for yourself or to provide to a service technician.
- IBM BladeCenter S SAS RAID Controller Module *Host System Attachment Guide* contains information on attaching hosts for the IBM BladeCenter S SAS RAID Controller Module.

Depending on your Blade Server model, additional documents might be included on the IBM *BladeCenter Documentation* CD, with the most recent versions of all BladeCenter documents available at <http://www.ibm.com/systems/bladecenter/>.

In addition to reviewing the documentation in this library, make sure that you review the IBM *Planning and Installation Guide* for your BladeCenter unit to help you prepare for system installation and configuration. For more information, see <http://www.ibm.com/systems/support/>.

Chapter 2. Prerequisite hardware

The section highlights the prerequisite hardware required to operate the IBM BladeCenter S SAS RAID Controller Module.

The IBM BladeCenter S chassis requires one Battery Backup Unit, FRU part number 45W5002, for each SAS RAID Module to function.

Understanding Battery Backup Units

Battery Backup Units (BBUs) can provide enough reserve power to store data in your IBM BladeCenter S SAS RAID Controller Module memory cache for 72 hours in the event of an interruption of power.

Battery Backup Units automatically recharge once they are inserted into the IBM BladeCenter S chassis.

Note: Like all batteries, Battery Backup Units degrade over time. You should install Battery Backup Units within 90 days of the date of purchase so that they can begin recharging, and do not take them out of the IBM BladeCenter S chassis for extended periods of time.

The first battery expiration notification is made 90 days before the expiration date listed. Subsequent notifications are made at 30 and 15 days. You must replace the Battery Backup Units before the final expiration date occurs. If the Battery Backup Units expire, the RAID Controller enters into a cache write-through mode until you install new Battery Backup Units. This causes a significant delay in processing speed.

Environmental considerations

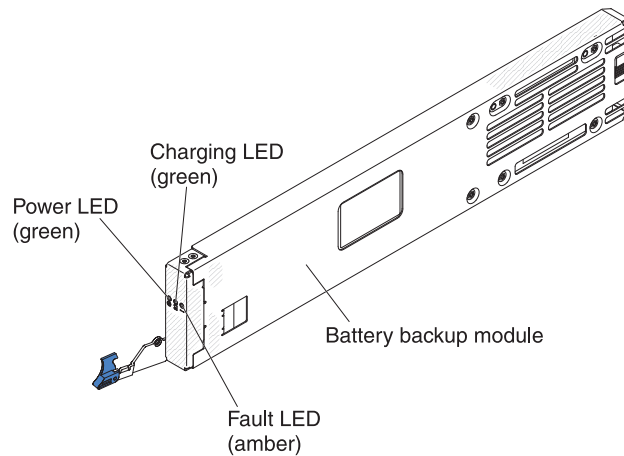
Follow the laws and guidelines for battery and other hazardous waste disposal in your area.

Quick facts about Battery Backup Units

Battery backup units provide backup for SAS RAID controller modules cache.

Battery Backup Units are installed in the battery backup unit bays located in the media tray when you install SAS RAID controller modules. The Battery Backup Unit in battery backup bay 1 provides backup support for the SAS RAID controller module in I/O module bay 3; the Battery Backup Unit in battery backup bay 2 provides backup support for the SAS RAID controller module in I/O module bay 4.

Note: Both Battery Backup Units are required when you install two SAS RAID controller modules.



Controls and indicators

The Battery Backup Units provides the following indicators:

Power Lit (green). Power is being supplied to the Battery Backup Units.

Charging

Lit (green). The Battery Backup Units is being charged.

Off.

Fault Lit (amber). The Battery Backup Units has a failure. If the Fault LED is lit, replace the Battery Backup Units.

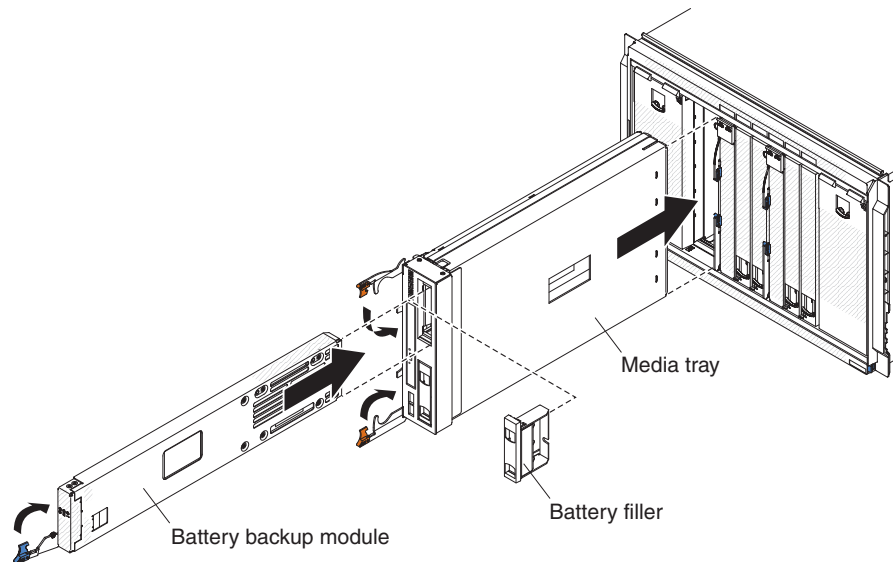
Installing the Battery Backup Unit

To install the Battery Backup Unit, slide the unit into the media tray and close the release handle.

About this task

This topic shows the mechanics of performing a physical installation of the Battery Backup Units. The Replacing a battery section of this document details the steps to take to prepare the IBM BladeCenter S SAS RAID Controller Module for a battery replacement.

Battery Backup Unit installation into the front of the BladeCenter S chassis



Procedure

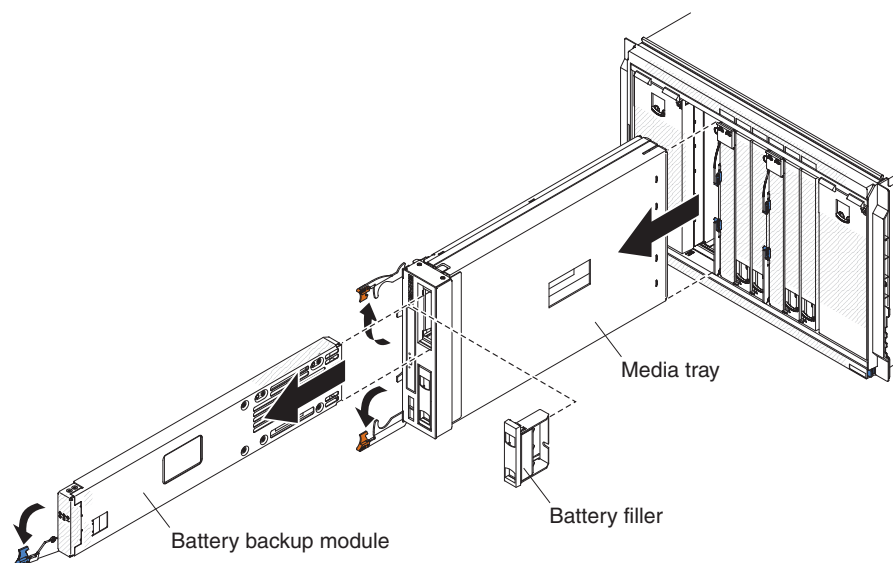
1. Open the release handle (rotate the handle down).
2. Slide the battery backup unit into the media tray.
3. Close the release handle (rotate the handle up)

Removing the Battery Backup Unit hardware

To remove the Battery Backup Unit, open the release handle on the Battery Backup Unit and slide the bBattery Backup Unit out of the media tray.

About this task

Important: If you are removing one or both Battery backup units from a BladeCenter S chassis that contains SAS RAID controller modules, refer to the *IBM BladeCenter SAS RAID Controller Installation and User's Guide* for additional steps that might need to be performed.



Procedure

1. Open the release handle (rotate the handle down)
2. Slide the battery backup unit out of the media tray.

Chapter 3. Understanding the Telnet interface

You can establish a Telnet session to retrieve information or to configure settings using the command line interface.

You can perform a variety of installation and connectivity management tasks through an Ethernet connection using this interface.

You can access the Telnet interface in one of two ways:

- Advanced Management Module
- Use the Command Line Interface on a network management workstation

Establishing a Telnet session to RAID Controller

You can establish a Telnet session using various methods. This topic describes how to establish a Telnet session to the RAID Controller using the Advanced Management Module.

Before you begin

About this task

To establish a Telnet session to the RAID Controller using the Advanced Management Module complete the following steps:

Procedure

1. Point your browser to `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the Advanced Management Module interface. The Enter Network Password window opens.

If you have the Advanced Management Module connected to your network, log in using the network IP assigned to it. If you are using the default IP address your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module .

Note: The default IP address for the Advanced Management Module is 192.168.70.125.

2. Enter the initial default user ID, **USERID** for the **User Name**. The user ID and password are case sensitive.
3. Enter the initial default password, **PASSWORD** (the sixth character is a zero) for the **Password** and click **OK**. The Welcome window opens.
4. Select the timeout value of this Web session for the **Inactive session timeout value** and click **Continue**. The Advanced Management Module window opens.
5. Select **I/O Module Tasks > Configuration**. The I/O Module Configuration window opens.
6. Click the link for either the connectivity module in I/O module bay 3 or in I/O module bay 4.
7. From the **Current IP Configuration for RAID Controller Subsystem** section, click **Advanced Configuration**. The Advanced Configuration window opens.

8. To start a Telnet session, click **Start Telnet Session**. The Login screen opens.
9. At the **Login** prompt, type the initial default user ID, USERID and press Enter. The user ID and password are case sensitive. The Password prompt displays.
10. At the **Password** prompt, type the initial default password, PASSWORD (the sixth character is a zero).
11. Click **OK**. The Command Line Interface Shell screen opens.

Chapter 4. Installing the IBM BladeCenter S SAS RAID Controller Module

This topic details the IBM BladeCenter S SAS RAID Controller Module installation and setup procedures.

Before you begin

Before you begin, do the following:

1. Install a SAS Expansion Card (CFFv) for IBM BladeCenter (Part Number - 39Y9190) into each Blade server that you want to communicate with the RAID Controller. For detailed installation instructions, see The SAS Expansion Card (CFFv) for IBM BladeCenter Installation and Users Guide located in the *Support* directory on the support CD.
2. If you are upgrading ensure that your previously installed Advanced Management Module has the level of firmware that supports the RAID Controller. You can check your firmware level at: www.ibm.com/systems/support/documentation/.

Note: If you log into the Advanced Management Module using the default IP (192.168.70.125), your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module.

3. As part of the setup procedure, obtain four unused IP Addresses on the same subnet from your network administrator.
 - 2 IP Address for the RAID Subsystem
 - 2 IP Address for the SAS Switches
4. Remove the SAS RAID Modules from their shipping packages.

Remember: Follow the guidelines for handling static sensitive devices.

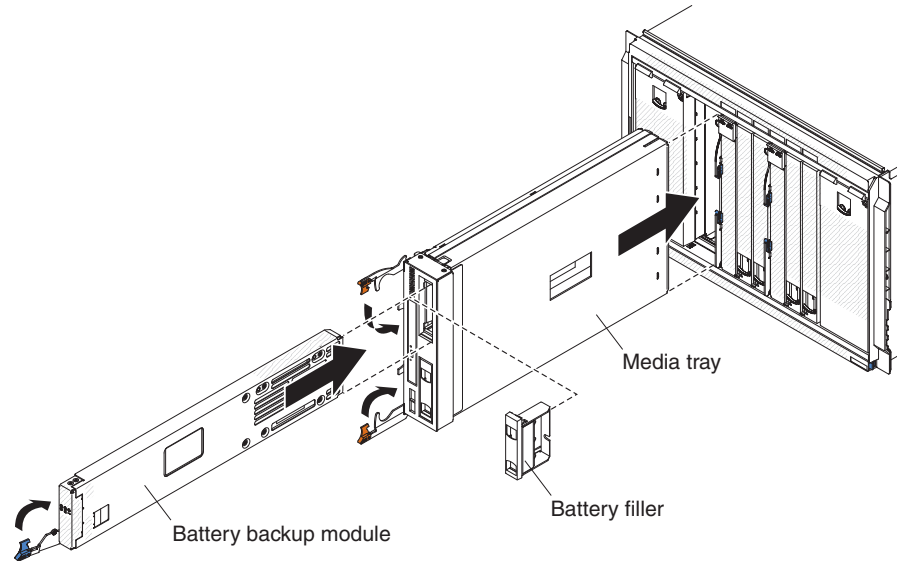
About this task

Once you have finished the prerequisite steps perform the following tasks:

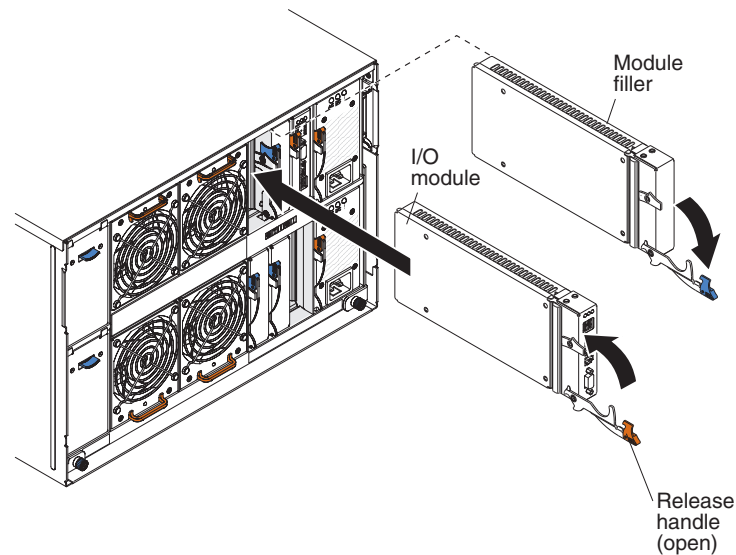
Installation and setup

Procedure

1. Install one Battery Backup Unit in bay 1 of the media tray, and the second Battery Backup Unit in bay 2 of the media tray.



2. Install the first SAS RAID Module in I/O module bay 3, and the second SAS RAID Module in I/O module bay 4.



After you have physically installed the modules, you can configure them in the following ways:

Advanced Management Module

A non-guided manual configuration using a direct connection to the Advanced Management Module.

Log into the Advanced Management Module and perform the rest of the setup tasks.

Note: You will still need to configure integrated storage using the IBM Storage Configuration Manager, or RAID Controller command line interface.

The Advanced Management Module method

About this task

After you install the IBM BladeCenter S SAS RAID Controller Module, you can log into the Advanced Management Module and set the parameters of the modules so that you can begin configuring your integrated storage.

Note: Before you enter the POST and Ethernet switch parameters for your IBM BladeCenter S SAS RAID Controller Module, ensure that if you are running a storage configuration using spares, that spare matches the capacity, speed and type of the drives in the array for which it is used.

Procedure

1. To log into the Advanced Management Module perform the following:

- a. Enter the IP address of the Advanced Management Module into the Web browser URL field.

If you have the Advanced Management Module connected to your network, log in using the network IP assigned to it. If you are using the default IP address your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module .

Note: The default IP address for the Advanced Management Module is 192.168.70.125.

- b. Enter the username and password.
 - The default username is: USERID
 - The default password is: PASSW0RD (the sixth position is the numeral zero)
- c. When prompted for the **Inactive session timeout value**, select **no timeout**.

Note: Remember to log out when you have completed your session. If you do not log out, the system shows an error the next time you try to log in.

2. Click **Continue**.
3. From the **I/O Module Tasks** menu, click **Configuration**.
4. From the **I/O Module Configuration** section, click **Bay 3**
5. Enter the IP settings for the SAS Switch, and RAID Controller.
6. Save the settings.
7. If you have two SAS RAID Modules, repeat these steps to configure the IP settings for the SAS Switch, and RAID Controller in **Bay 4** as well.
8. Verify the IP settings are listed before proceeding to the next step.
9. Enable **Fast POST** and ensure that **External ports** are disabled for each RAID Controller.

Note: The disabled ports are SAS ports, not Ethernet ports.

- a. From the **I/O Module Tasks** menu, click **Admin/Power/Restart**.
- b. Scroll down to the **I/O Module Advanced Setup** section and from the **Select a module** menu, select **I/O module 3**.
- c. Select **Enabled** from the menu for **Fast POST** and **Disabled** for **External ports**.

- d. Click **Save**.
10. If you have two SAS RAID Modules, repeat these steps to enable **Fast POST** and ensure that the **External ports** are disabled for the RAID Controller installed in **I/O module 4** as well.

What to do next

If you experience any problems with setting these parameters, review the advanced verification procedures in the Troubleshooting section of this document.

Installing IBM Storage Configuration Manager

After completing initial configuration of your IBM BladeCenter S SAS RAID Controller Modules, you should install the IBM Storage Configuration Manager. IBM Storage Configuration Manager provides advanced support for management and monitoring of IBM BladeCenter storage. It also provides system health monitoring, device user management, and troubleshooting functions.

About this task

The following is a summary and not meant to be used as primary installation instructions. For complete instructions and important compatibility notices, refer to the *IBM Storage Configuration Manager Planning, Installation and Configuration Guide*.

Procedure

1. Navigate to <http://www.ibm.com/systems/management/director/downloads.html>.
2. From the **Choose Software** list, select IBM Storage Configuration Manager and download the installer file.
3. Unpack the .ZIP or .TAR installation file to a temporary directory or burn the ISO image to a CD.
4. Launch the installer and follow the on screen prompts.
5. When prompted to choose an install type, select **SCM Full Install for all devices**.
6. After you install the IBM Storage Configuration Manager, you are prompted to restart your workstation. The IBM Storage Configuration Manager service starts automatically upon restart.
7. From the Start menu, launch the IBM Storage Configuration Manager.
8. Log in and select Initial Configuration Wizard and follow the on screen prompts.

Important: If you apply a new storage configuration using the IBM Storage Configuration Manager, existing configuration and all data stored on the disks is deleted before new configuration is applied.

User ID and password requirements

The SAS RAID Module has two separate default user IDs and passwords. The first default user, **USERID**, and default password, **PASSWORD** (the sixth character is a zero), is used to access the RAID Controller command line interface. The second default user, **USERID1**, and default password, **PASSWORD** (the sixth character is a zero), is used by the IBM Storage Configuration Manager.

The default user IDs cannot be changed. However, you can change the password for either **USERID** or **USERID1** using the **chpassword** command in the RAID Controller command line interface (see “chpasswd” on page 65). The following rules apply to new passwords:

- Password must contain at least 8 characters
- Password must not exceed 16 characters.
- Password must contain at least one digit (0–9)
- Password must contain at least one alpha character (a–z,A–Z).

If the firmware level of your RAID controllers is older than 1.2.x.xxx, you need to change the password on both SAS RAID Modules at the same time. If the firmware level of your RAID controllers is 1.2.x.xxx or newer, then changing the password on one SAS RAID Module automatically changes the password on the other SAS RAID Module.

Resetting the passwords on an SAS RAID Module

Before you begin

Before resetting the SAS RAID Module passwords, you must end all application I/O processes and shut down any active Blade servers in accordance with the recommended non-concurrent practices. Then, use the **reset to factory defaults** function within Advanced Management Module to reset the passwords.

To reset the passwords on one SAS RAID Module, you must power off both SAS RAID Modules. Perform the following steps to reset the passwords on the SAS RAID Module in bay 3.

Procedure

1. Stop all host I/O applications and power off the Blade servers.
2. Use the Advanced Management Module to reset the passwords.
 - a. Log into the Advanced Management Module.
 - b. Select **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select the checkboxes next to bay 3 and bay 4.
 - d. From the **Available actions** menu, select **Power Off Module(s)**.
 - e. Click **Perform action**.
 - f. Wait until both SAS RAID Modules are powered off. The **Off** message will be displayed in the **Pwr** column.
 - g. Select **I/O Module Tasks > Configuration**.
 - h. In the **I/O Module Configuration** section, select **Bay 3**.
 - i. In the Bay 3 section that displays, select **Advanced Configuration**.
 - j. In the **Advanced Configuration for I/O Module 3** section, select **Restore Factory Defaults**.
 - k. Select **Restore Defaults**.

- l. Select **OK**.
- m. The SAS RAID Module in bay 3 will power on. Wait until the SAS RAID Module in bay 3 successfully powers on. The **On** message will display in the **Pwr** column, and the message **POST results available: Module completed POST successfully** will display in **POST Status** column.
3. Power on the SAS RAID Module in bay 4.
 - a. Select **I/O Module Tasks > Admin/Power/Restart**.
 - b. Select the checkbox next to bay 4.
 - c. From the **Available actions** menu, select **Power On Module(s)**.
 - d. Click **Perform action**.
 - e. The SAS RAID Module in bay 4 will power on. Wait until the SAS RAID Module in bay 4 successfully powers on. The **On** message will be displayed in the **Pwr** column, and the message **POST results available: Module completed POST successfully** will display in **POST Status** column.

What to do next

To reset the passwords for the SAS RAID Module in bay 4, repeat these steps, substituting the opposite bay numbers where appropriate.

Note: Performing the steps to reset the factory defaults does not affect any logical configuration data on the SAS RAID Modules.

Configuring storage through the CLI

Advanced users can also configure their storage through the RAID Controller command line interface – “Using the command line to configure storage” on page 94.

Upgrading from a single to a dual controller configuration

Upgrading from a single RAID Controller configuration to a dual RAID Controller configuration is supported using the RAID Controller command line interface. Perform the following steps to concurrently upgrade from a single to dual controller configuration.

1. Log into the CLI of the RAID Controller.
2. At the <CLI> prompt, enter `list controller` and press Enter to verify the controller is operating in a single controller configuration.

<CLI> `list controller`

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	STANDALONE	1	10
1	Ctlr1	NOT_PRESENT	-	--

3. At the <CLI> prompt, enter `host -get` and press Enter to query the list of host servers.

<CLI> `host -get`

HostWWN 500062b00007e568, HostName Blade_Bay_1 :

LUNs Mapped :

LUN	Permission	Volume
-----	------------	--------

0	ACCESS_READWRITE	Raid10_Pool:r10_vol_1
4	ACCESS_READWRITE	Raid10_Pool:r10_vol_10
3	ACCESS_READWRITE	Raid10_Pool:r10_vol_4
2	ACCESS_READWRITE	Raid10_Pool:r10_vol_3
1	ACCESS_READWRITE	Raid10_Pool:r10_vol_2
5	ACCESS_READWRITE	Raid10_Pool:r10_vol_9
6	ACCESS_READWRITE	Raid10_Pool:r10_vol_8
7	ACCESS_READWRITE	Raid10_Pool:r10_vol_7
8	ACCESS_READWRITE	Raid10_Pool:r10_vol_6
9	ACCESS_READWRITE	Raid10_Pool:r10_vol_5

4. Insert the new RAID Controller into I/O bay 4.
 - a. Open the release handle by rotating the handle down.
 - b. Slide the RAID Controller into the module bay until it stops.
 - c. Close the release handle by rotating the handle up.
 - d. Connect all cables to the module.
5. At the <CLI> prompt, enter alert -get and press Enter. Verify the configuration changed from a single to dual controller by querying the active alert list for alert 706. Alert 706 is automatically cleared from the active alert list after two minutes.

<CLI> alert -get

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
706	61	20100219232029	0	Info	5005076b07441aff	1	Masked
Msg: Controller changed from Single to Dual Controller Mode (SCFG set to 2)							

6. At the <CLI> prompt, enter list controller and press Enter. Verify the controllers are operating in a dual primary-secondary configuration .

<CLI> list controller

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	PRIMARY	1	10
1	Ctlr1	SECONDARY	1	10

7. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list for alert 5600. Record the host port WWN to create host-LUN mappings.

<CLI> alert -get

Current Machine Local Time: 02/19/2010 11:20:36 PM

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
5600	9	20100219162030	1	Info	5005076b07441aff	1	Masked
Msg: Illegal host 0x500062b00007e569 access attempted							

8. At the <CLI> prompt, enter host -add <WWN> and press Enter to add the host WWN to the list of host.

<CLI> host -add 500062b00007e569

Host added with WWN 500062b00007e569 and Name CliHost1

9. At the <CLI> prompt, enter host -get and press Enter to verify the new host was added to the list of host servers.

```
<CLI> host -get
```

```
HostWWN 500062b00007e568, HostName Blade_Bay_1 :
```

```
LUNs Mapped :
```

LUN	Permission	Volume
0	ACCESS_READWRITE	Raid10_Pool:r10_vol_1
4	ACCESS_READWRITE	Raid10_Pool:r10_vol_10
3	ACCESS_READWRITE	Raid10_Pool:r10_vol_4
2	ACCESS_READWRITE	Raid10_Pool:r10_vol_3
1	ACCESS_READWRITE	Raid10_Pool:r10_vol_2
5	ACCESS_READWRITE	Raid10_Pool:r10_vol_9
6	ACCESS_READWRITE	Raid10_Pool:r10_vol_8
7	ACCESS_READWRITE	Raid10_Pool:r10_vol_7
8	ACCESS_READWRITE	Raid10_Pool:r10_vol_6
9	ACCESS_READWRITE	Raid10_Pool:r10_vol_5

```
HostWWN 500062b00007e569, HostName CliHost1 :
```

```
No LUNs Mapped
```

10. At the <CLI> prompt, enter hostlun -map -volume <POOLNAME:VOLNAME> -PERMISSION <RW> -wwn <WWN> -name <HOSTNAME> -lun <LUNNUMBER> and press Enter to map the host to the LUNs using the WWN of the host port . The LUN, volume number, and permissions must be the same.

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_1 -permission rw -wwn 500062b00007e569
-name CliHost1 -lun 0
```

```
Working ...
```

```
Host LUN 0 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_1'
in 'Raid10_Pool'
```

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_2 -permission rw -wwn 500062b00007e569
-name CliHost1 -lun 1
```

```
Working ...
```

```
Host LUN 1 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_2'
in 'Raid10_Pool'
```

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_3 -permission rw -wwn 500062b00007e569
-name CliHost1 -lun 2
```

```
Working ...
```

```
Host LUN 2 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_3'
in 'Raid10_Pool'
```

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_4 -permission rw -wwn 500062b00007e569
-name CliHost1 -lun 3
```

```
Working ...
```

```
Host LUN 3 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_4'
in 'Raid10_Pool'
```

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_10 -permission rw -wwn 500062b00007e569
-name CliHost1 -lun 4
```

Working ...

Host LUN 4 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_10' in 'Raid10_Pool'

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_9 -permission rw -wwn 500062b00007e569  
-name CliHost1 -lun 5
```

Working ...

Host LUN 5 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_9' in 'Raid10_Pool'

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_8 -permission rw -wwn 500062b00007e569  
-name CliHost1 -lun 6
```

Working ...

Host LUN 6 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_8' in 'Raid10_Pool'

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_7 -permission rw -wwn 500062b00007e569  
-name CliHost1 -lun 7
```

Working ...

Host LUN 7 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_7' in 'Raid10_Pool'

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_6 -permission rw -wwn 500062b00007e569  
-name CliHost1 -lun 8
```

Working ...

Host LUN 8 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_6' in 'Raid10_Pool'

```
<CLI> hostlun -map -volume Raid10_Pool:r10_vol_5 -permission rw -wwn 500062b00007e569  
-name CliHost1 -lun 9
```

Working ...

Host LUN 9 for host 500062b00007e569 and host name CliHost1 mapped to volume 'r10_vol_5' in 'Raid10_Pool'

11. Log into the host server and scan for hardware changes to allow for the host to recognized the second path.
12. Log into the host server and verify the second path is operational.
13. At the <CLI> prompt, enter host -get and press Enter to verify the host mappings of the second WWN.

```
<CLI> host -get
```

HostWWN 500062b00007e568, HostName Blade_Bay_1 :

LUNs Mapped :

LUN	Permission	Volume
0	ACCESS_READWRITE	Raid10_Pool:r10_vol_1
4	ACCESS_READWRITE	Raid10_Pool:r10_vol_10
3	ACCESS_READWRITE	Raid10_Pool:r10_vol_4
2	ACCESS_READWRITE	Raid10_Pool:r10_vol_3
1	ACCESS_READWRITE	Raid10_Pool:r10_vol_2
5	ACCESS_READWRITE	Raid10_Pool:r10_vol_9

6	ACCESS_READWRITE	Raid10_Pool:r10_vol_8
7	ACCESS_READWRITE	Raid10_Pool:r10_vol_7
8	ACCESS_READWRITE	Raid10_Pool:r10_vol_6
9	ACCESS_READWRITE	Raid10_Pool:r10_vol_5

HostWWN 500062b00007e569, HostName CliHost1 :

LUNs Mapped :

LUN	Permission	Volume
0	ACCESS_READWRITE	Raid10_Pool:r10_vol_1
1	ACCESS_READWRITE	Raid10_Pool:r10_vol_2
2	ACCESS_READWRITE	Raid10_Pool:r10_vol_3
3	ACCESS_READWRITE	Raid10_Pool:r10_vol_4
4	ACCESS_READWRITE	Raid10_Pool:r10_vol_10
5	ACCESS_READWRITE	Raid10_Pool:r10_vol_9
6	ACCESS_READWRITE	Raid10_Pool:r10_vol_8
7	ACCESS_READWRITE	Raid10_Pool:r10_vol_7
8	ACCESS_READWRITE	Raid10_Pool:r10_vol_6
9	ACCESS_READWRITE	Raid10_Pool:r10_vol_5

If the upgrade did not complete successfully, collect the logs and contact IBM.

Chapter 5. Disconnecting power to the BladeCenter unit

This section describes the power-off sequence for the BladeCenter S chassis with IBM BladeCenter S SAS RAID Controller Module installed.

About this task

If you are disconnecting power from the BladeCenter chassis for more than 72 hours, you must turn off IBM BladeCenter S SAS RAID Controller Module as part of the chassis power-off procedure. This allows the RAID Controller to save the cached data on the disk drives.

Disconnect power from the BladeCenter S chassis by shutting down all blade servers and components and disconnecting the BladeCenter S chassis from all power sources.

Note: A 9401 alert event is logged in the system if one of the following occurs:

- The IBM BladeCenter S SAS RAID Controller Module is not turned off and the chassis is disconnected from the power source for more than 72 hours
- You remove both SAS RAID Controller Modules, both backup battery modules, or the media tray without performing a proper power-off procedure

If the IBM BladeCenter S SAS RAID Controller Module is not turned off and the BladeCenter chassis is disconnected from the power source for more than 72 hours, the backup battery units require a period of charging time before they can provide power for the RAID Controller memory cache. During this charging period, the RAID Controller enters into a cache write-through mode. This causes a significant delay in processing speed.

Before you install or remove any components in the chassis, review and resolve any active alerts for the components. Refer to the related sections in “Non-concurrent repair procedures” on page 158 and “Concurrent repair procedures” on page 168 for more information on repair procedures.

To turn off the BladeCenter S chassis, complete the following steps:

Procedure

1. Turn off the blade servers:
 - a. Stop all blade server I/O applications and shut down the operating systems. See the documentation that comes with your blade server for information about shutting down the operating system on the blade server.
 - b. Log on the Advanced Management Module (AMM).
 - c. Select **Blade Tasks > Power/Restart**.
 - d. Select all blade servers.
 - e. From the **Available actions** list, select **Power Off Blade** and click **Perform action**.
 - f. Make sure that all blade servers are **Off**.
2. Turn off the SAS RAID Controller Modules:
 - a. In the AMM, select **I/O Module Tasks > Admin/Power/Restart**.
 - b. Select the bays in which the SAS RAID Controller Modules are installed.

- c. From the **Available actions** list, select **Power Off Module(s)** and click **Perform action**.
- d. Make sure that both SAS RAID Controller Modules are **Off**.

Note: It may take up to 8 minutes to fully turn off the SAS RAID Controller Modules. If power to the chassis is disconnected before the I/O modules are in the **Off** state and you turn on the chassis after 72 hours, a 9401 alert event will be logged in the system.

- 3. Disconnect power from the chassis:
 - a. Remove all power cords from the power modules.
 - b. Verify that all LEDs are off.

Note: After you disconnect the BladeCenter S chassis from power, wait at least 30 seconds before you connect the BladeCenter S chassis to power again.

Chapter 6. Updating firmware

Several components, including the IBM BladeCenter S SAS RAID Controller Module, require regular firmware updates. This section explains how to find and install the most recent updates.

Note: When replacing BladeCenter components, consider updating the firmware for the Advanced Management Module and any other components to the latest version of firmware.

The SAS RAID Controller Firmware Update Package is a Command Line Interface (CLI) based application package that allows you to automatically upgrade the firmware associated with the IBM BladeCenter S SAS RAID Controller Module and its components. The application must be installed on a computer using Windows or Linux with a network connection to the IBM BladeCenter S SAS RAID Controller Module and the Advanced Management Module.

After completing the installation procedures, check the current firmware level shipped on the IBM BladeCenter S SAS RAID Controller Module and visit the IBM BladeCenter support Web site to ensure that it is operating with the latest version of firmware.

To download the latest firmware update package:

1. Point your browser to <http://www.ibm.com/systems/support/>.
2. From the Product Support section, click the **BladeCenter** link.
3. From the Popular links section, select **Software and device drivers**.
4. From the IBM BladeCenter software and device drivers Web site, select **BladeCenter S**.
5. From the matrix of downloadable files, select the blade servers and other devices that are installed in your BladeCenter S chassis to download the firmware and device drivers for them.

Product documentation for the BladeCenter S system is available at:
<http://www.ibm.com/systems/support/>

From the BladeCenter support page, in the **Support & downloads** section, select **Documentation**.

Note: For information on updating firmware through IBM Storage Configuration Manager, see the IBM Storage Configuration Manager online help.

Note:

1. When updating the RAID Controller firmware from 1.0.x.x to 1.2.x.x, pre-verifying the RAID Subsystem is not supported.
2. The RAID Controller firmware updating through IBM Storage Configuration Manager from 1.3.x.x and above is not supported.
3. The firmware version 1.3.1.010 is the minimum version to support both DSM_SFF (DSM-12) and DSM_LFF (DSM-6) enclosure.
4. The firmware version 1.3.2.002 is the minimum version to support 3TB SAS drives.

Subscribing to notifications

About this task

My Notifications is a service that can automatically email you when new information or code is available for your IBM BladeCenter product. To subscribe, start at the IBM BladeCenter Support web page: <http://www.ibm.com/systems/support/>.

Procedure

1. Locate the **Stay Informed** section of the page and click **Subscribe today**.
2. Click **BladeCenter**
3. From the BladeCenter section of the Support Subscriptions page click **BladeCenter notifications**.

Note: Log in with your IBM ID and password. If you don't yet have an IBM ID, you can register using your email address. You are prompted to create a password, a password hint and to provide your country of residence.

4. At the My subscriptions page, select **BladeCenter S** and click **Submit**
5. From within the **Notify me by** area, select the following: **email, weekly, html**.
6. From within the **Type** area select the machine type of the BladeCenter S (typically 8886).
7. From within the **Operating System** area, select the operating system you use with the BladeCenter SAS RAID Controller Module.
8. From within the **Selections** area, select **Troubleshooting, Download, and Install**, or other items of interest to you.

Installing and configuring firmware updates

To obtain the latest IBM BladeCenter S SAS RAID Controller Module firmware update configuration and installation instructions, visit the IBM Support website at <http://www.ibm.com/support/>. Follow the instructions attached to the code package to install and configure firmware updates.

Chapter 7. Working with storage pools and volumes

You can divide your available storage into storage pools and volumes to customize your configuration.

Understanding storage pools

A storage pool is a collection of disk drives that become a logical entity. When you create a storage pool, you assign a RAID level to it which will provide a redundancy level.

You can create a storage pool using IBM Storage Configuration Manager or by using the **create pool** command in the RAID Controller command line interface (see “create pool” on page 84).

Notes®:

- You should determine the size of your storage pool by the amount of space required by your application. Once you have determined whatever constraints are put in place by the application, then you can weigh the performance enhancement versus cost to determine the RAID level to use.
- All disk drives in a storage pool must be the same type.
- A disk drive can only belong to one storage pool.
- If you use global spares to protect storage pools, ensure that any spare matches the capacity, speed and type of the drives in the storage pool for which it is used.

Understanding volumes

After you create storage pools, you need to break the storage pools into discrete areas of storage, which are called *volumes*. Volumes are the basic unit of storage that are exposed to the Blade server and are created from the available space in a storage pool. A volume is completely contained within a single storage pool, however a storage pool can contain multiple volumes. After you create volumes, you must map them to each individual Blade server. Each Blade server can access one or more of these volumes.

Volumes are typically defined as either data volumes, which are used to store application data, or boot volumes, which are used to store the operating system image. For each volume, you need to determine the following characteristics:

- The size (in GBs)
- The blade server or servers that will have access to the volume
- Any applications on the blade servers that need access to the volume

You define volumes using IBM Storage Configuration Manager or by using the **create volume** command in the RAID Controller command line interface (see “create volume” on page 85).

Notes:

- The minimum size of a volume is 1 MB. The maximum size of a volume is the maximum size of the storage pool in which the volume resides.

- Defining large volumes may take several minutes to complete. An IBM BladeCenter S takes approximately 10 minutes to define an 11 TB volume, and may take longer if the system is performing other tasks.
- The maximum number of volumes on a system is 128. The maximum number of volumes on a host is 16.
- Multiple blade servers can be mapped to a single volume if clustering is configured. See “Configuring blades for Microsoft Cluster Service” on page 38 for more information.
- Mapping a single volume to multiple blade servers can be done using the `hostlun` command through the RAID Controller command line interface. See “hostlun” on page 88 for more information.

Understanding RAID levels

This topic details RAID level characteristics as they relate to the IBM BladeCenter S SAS RAID Controller Module.

A Redundant Arrays of Independent Disks (RAID) is a collection of two or more disk drives that present an image of one or more logical disk drives. In the event of a disk failure, the data can be read or regenerated from the other disk drives in the array due to data redundancy. There are several considerations in deciding which RAID level to choose for your configuration: the amount of storage you have at your disposal, cost, and security requirements.

The IBM BladeCenter S SAS RAID Controller Module supports the following RAID levels:

Table 4. RAID levels and characteristics

RAID levels	Characteristics
0	Striping
1	Mirroring
5	Striping with Distributed Parity
10	Striping across mirrors

RAID 0 uses a process called *striping*, which is the splitting of data across more than one disk. A RAID 0 configuration adds no redundancy and the loss of any one disk in a stripe causes the failure of all the disks in that stripe.

RAID 1 uses a process called *mirroring*. In a RAID 1 configuration, all of the data on a disk is replicated onto a second peer-level disk. If one of the disks in the pair fails, the other continues running unaffected. RAID 1 requires a two-disk configuration.

RAID 5 uses a process called *striped parity*. This process writes data and parity information in stripes along three or more drives. If a drive in the array fails, you do have to replace it, but the array is not destroyed by a single drive failure. If a drive failure occurs, subsequent reads are calculated from the distributed parity. The first predefined configuration file (CannedConfig_RSSM.cfg) sets up a RAID 5 array using six available drives. RAID 5 requires a minimum 3 disk configuration.

RAID 10 uses a process called *striping across mirrors*. This process requires a set of even numbered disks, with four disks being the minimum number required. The

data is organized as stripes across the disks and the striped disk sets are mirrored. This configuration provides fault tolerance and improved performance.

Drive configurations per RAID level

The following table shows the possible drive configurations for each RAID level.

Table 5. Drive configurations per RAID level for DSM_LFF (DSM-6) enclosure

RAID level	RAID characteristics	Minimum drives	Maximum drives	Maximum size of each disk drive	Maximum storage pool capacity
RAID 0	Striping	2	12	3 TB	~36 TB
RAID 1	Mirroring	2	12	3 TB	~3 TB
RAID 5	Striping with Distributed Parity	3	12	3 TB	~33 TB
RAID 10	Striping across mirrors	4. Drives must be added in pairs. (4,6,8,10,12 drives).	12	3 TB	~18 TB

Understanding the predefined storage configuration

When you install your IBM BladeCenter S SAS RAID Controller Module, a predefined configuration is available to get you started. This topic details the specifics of that predefined configuration.

Canned configuration

The predefined configuration packaged with IBM BladeCenter S SAS RAID Controller Module is referred to as a *canned config* within the interface itself. The name of the configuration file is CannedConfig_RSSM.cfg, and the names of the configurations created contain the word *canned* in them. You can use the predefined configuration if you meet the minimum storage requirements for it.

You can load the predefined or canned configuration from the command line interface by running the following command at the RAID Controller command line interface prompt:

```
controller config -load CannedConfig_RSSM.cfg
```

The **controller config** command uses the predefined configuration to create one pool at a RAID 5 level, using port 0, called CannedDG1.

The following example shows a command set that is equivalent to the function of the **controller config** command. The **create pool** command uses five drives in the first storage module to create a RAID 5 array, and the **global spare** command uses another drive to create one global spare. The **create volume** commands then create six volumes of 20 GB in the pool labeled CannedDG1.

Example: Contents of a pool created using the predefined configuration

```
<CLI> create pool -drives 1:3 1:5 1:2 1:1 1:4 -raidtype 5 -port 0 -name CannedDG1
create volume -name CannedDG1:vol1 -size 20480MB -seqpostreadcmdsiz 0 -seqreadaheadmargin 1 -writecachepolicy on
create volume -name CannedDG1:vol2 -size 20480MB -seqpostreadcmdsiz 0 -seqreadaheadmargin 1 -writecachepolicy on
create volume -name CannedDG1:vol3 -size 20480MB -seqpostreadcmdsiz 0 -seqreadaheadmargin 1 -writecachepolicy on
```


- a. From the SCM navigation panel, select **Health > Physical View**, then select the **Controllers** tab. Select each controller and ensure both controllers have a status of Normal (Online).
 - b. From the SCM navigation panel, select **Configuration > Storage**, then select the **Storage Pools** tab. Select a storage pool that you plan to use with VMware, then select **Properties** from the **More Actions** list. From the **General** tab, note the **Primary Controller** which displays the preferred path. All volumes belonging to a storage pool will have the same preferred path as the storage pool.
2. Now that you have identified the preferred path for your volumes, perform the following steps to change the multipath setting within VMware.
- a. Open the VMware Infrastructure Client.
 - b. In the left panel, select the host that you want to change.
 - c. In the right panel, click the **Configuration** tab.
 - d. In the Configuration window, click the **Properties** link next to the **Details** field to open the Datastore properties window.
 - e. Click **Manage Paths** to open the Manage Paths window.
 - f. Near the top of the **Policy** section, click **Change** to open the Manage Paths - Selection Policy window.
 - g. Select **Fixed** and click **OK**.
 - h. Close any windows you opened to return to the main menu. Repeat these steps for all hosts that you want to have this setting.
3. Configure the volumes within the VMware Operating System (OS) configuration to properly failover through the VI client.
- a. Open the VMware Infrastructure Client.
 - b. Select the blades with access to the SAS RAID Modules.
 - c. Under Configuration, select **Storage** from the side panel and select the volume to be changed.
 - d. Click **Properties**, then select **Manage paths**.
There are two paths in the Manage Paths window. The lower numbered path represents controller 0 and the higher numbered path represents controller 1. If the preferred path is same as indicated by the preferred path you investigated in step #1 through CLI or SCM, no action is required. If the preferred path is different from what is indicated in the CLI or SCM display, proceed to the next step.
 - e. Select the device path that you want to change then click **Change**.
 - f. Under preference, select **Preferred** and click **OK**.

Repeat steps 3a through 3f for each of the volumes.

Note: If you change your pool ownership after completing these steps, you may need to re-modify your VMWare configuration.

Configuring blades for Microsoft Cluster Service

This topic describes the steps to configure the SAS Expansion Card (CFFv) for IBM BladeCenter and the SAS Connectivity Card (CIOv) for IBM BladeCenter to support blades that are configured for Microsoft Cluster Service.

If you are configuring a server blade as a node in a Microsoft Windows 2003 clustering environment, you need to configure the SAS Expansion Card or the Onboard SAS Controller BIOS (for configurations with the SAS Connectivity Card) to support blades that are configured for Microsoft Cluster Service. If the SAS Expansion Card and the Onboard SAS Controller BIOS configuration is not set, nodes added to the cluster may fail to boot or hang with the console output as shown in Figure 3.

```
Broadcom NetXtreme II Ethernet Boot Agent v3.4.8  
Copyright (C) 2000-2007 Broadcom Corporation  
All rights reserved.
```

```
Broadcom NetXtreme II Ethernet Boot Agent v3.4.8  
Copyright (C) 2000-2007 Broadcom Corporation  
All rights reserved.
```

```
LSI Corporation MPT SAS BIOS  
MPTBIOS-6.22.00.00 (2008.04.10)  
Copyright 2000-2008 LSI Corporation.
```

```
Searching for devices at HBA 0...  
Searching for devices at HBA 1...  
-
```

Figure 3. Example of a hung boot screen

Important: For blades that have the SAS Expansion Card or a boot disk connected through the SAS Expansion Card, you must apply Microsoft Hotfix 886569 for Microsoft Cluster Service to be able to manage the storage volumes. You can download Microsoft Hotfix 886569 at <http://support.microsoft.com/kb/886569>.

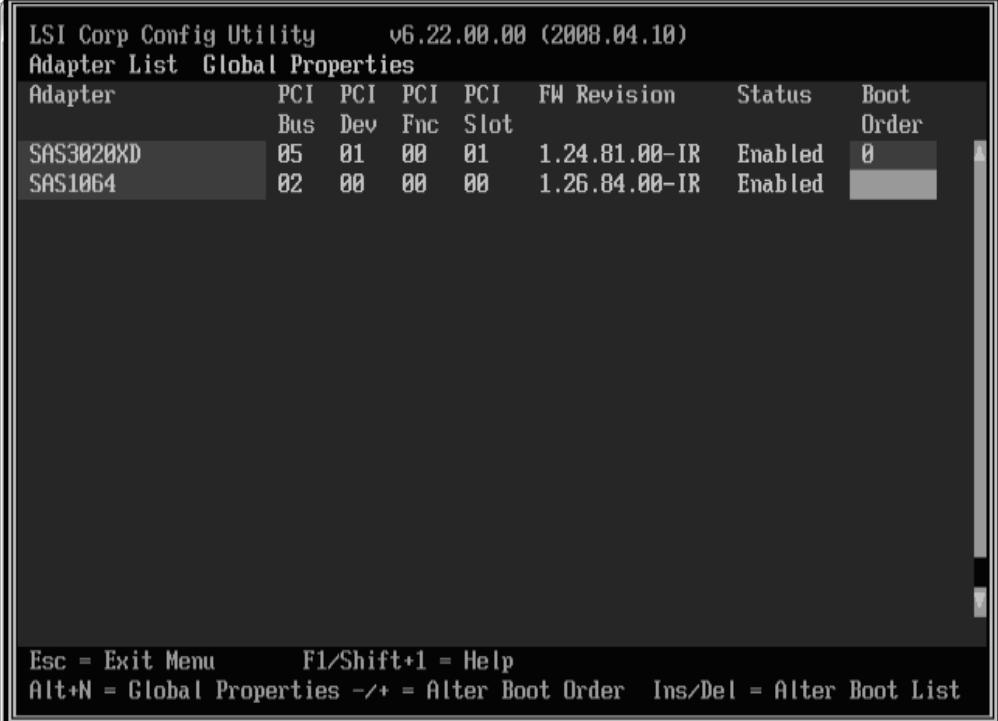
The steps you need to perform to configure the SAS Expansion Card and the Onboard SAS Controller BIOS depend on your boot disk type and external adapter type. Determine which steps you need to follow based on the boot option and the type of external SAS interface card you have installed:

- “Configuring blades with an internal boot disk and SAS Expansion Card” on page 39
- “Configuring blades with a boot disk connected through the SAS Expansion Card” on page 42
- “Configuring blades with the SAS Connectivity Card” on page 46

Configuring blades with an internal boot disk and SAS Expansion Card

Follow these steps when the SAS RAID Module is configured so that only data drives are presented to the blade host, and the host blade uses separate adapters for the internal boot drive and the SAS RAID Module data drives.

1. When the <<<Press Ctrl-C to start LSI Logic Configuration Utility>>> prompt displays during system boot, press Ctrl+C to enter the LSI Logic Configuration Utility. For blades with an enabled Onboard SAS Controller and the SAS Expansion Card, the Adapter List screen will be similar to Figure 4. In Figure 4, the SAS Expansion Card is shown as the first entry **SAS3020XD**. The adapter name may vary depending on the particular blade model and SAS Expansion Card version. To determine which entry is the SAS Expansion Card, you can temporarily disable the Onboard SAS Controller by pressing F1 during the boot; this removes the Onboard SAS Controller from the Adapter List screen and the remaining entry will be the SAS Expansion Card. HS20 and LS20 blade types will have a single SAS entry by default as the internal hard drive is connected using SCSI.



Adapter List Global Properties							
Adapter	PCI Bus	PCI Dev	PCI Fnc	PCI Slot	FW Revision	Status	Boot Order
SAS3020XD	05	01	00	01	1.24.81.00-IR	Enabled	0
SAS1064	02	00	00	00	1.26.84.00-IR	Enabled	

Esc = Exit Menu F1/Shift+1 = Help
Alt+N = Global Properties -/+ = Alter Boot Order Ins/Del = Alter Boot List

Figure 4. Adapter List screen showing Onboard SAS Controller and SAS Expansion Card

2. Use the arrow keys to select the SAS Expansion Card then press Enter to display the Adapter Properties screen. Ensure that **Boot Support** is set to **[Disabled]**, as shown in Figure 5 on page 40. When the boot support is disabled, the LSI Adapter BIOS will not scan the data drives for boot devices.



Figure 5. Disabling boot support for the SAS Expansion Card

3. Press Esc to exit the Adapter Properties screen until the utility asks you to save the configuration as shown in Figure 6. Use the arrow keys to select Save changes then exit this menu, then press Enter. Back on the Adapter List screen, the **Status** of the external adapter now displays as **[Disabled]**.

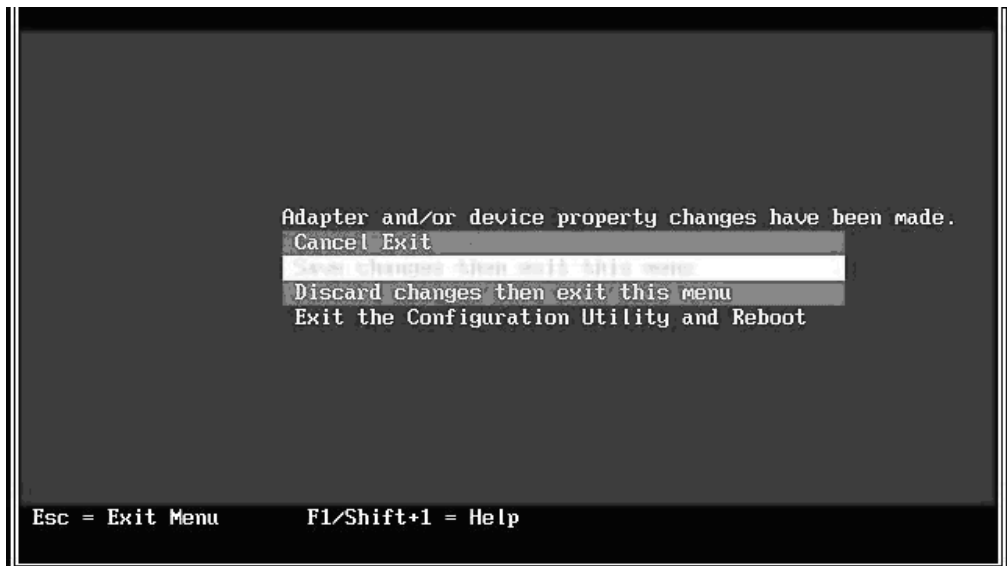
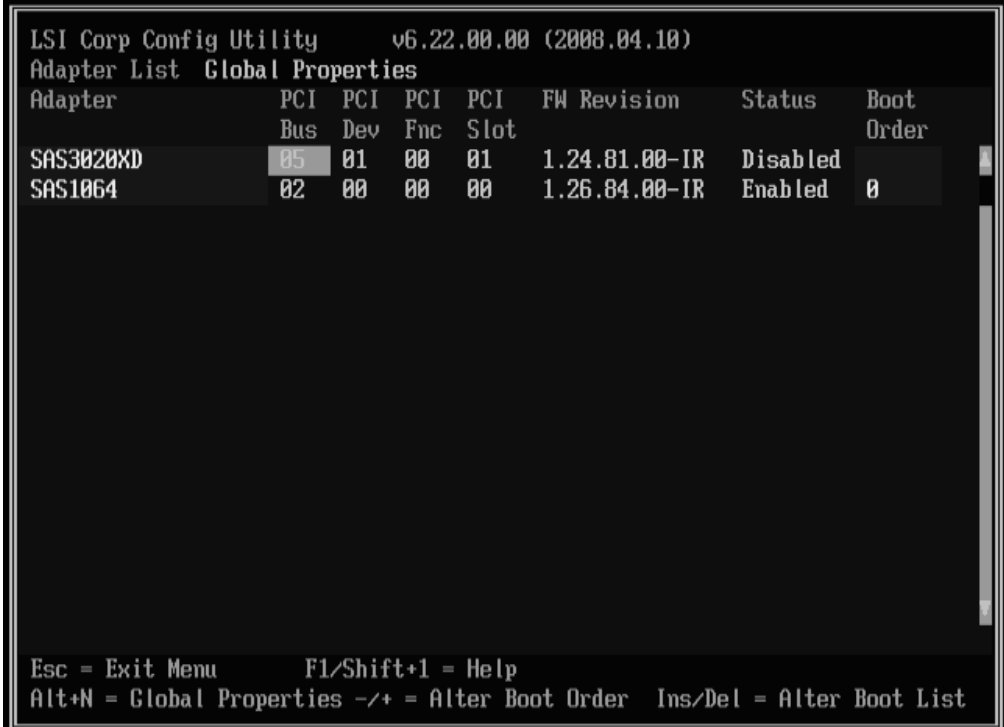


Figure 6. Saving configuration changes for the SAS Expansion Card

4. Change the boot order so that the Onboard SAS Controller is boot device 0. Use the arrow keys to select the **Boot Order** fields, then press Insert and Delete to change the boot order so that the Onboard SAS Controller is set to 0.

Figure 7 shows the correct boot order.



Adapter List		Global Properties					
Adapter	PCI Bus	PCI Dev	PCI Fnc	PCI Slot	FW Revision	Status	Boot Order
SAS3020XD	05	01	00	01	1.24.81.00-IR	Disabled	
SAS1064	02	00	00	00	1.26.84.00-IR	Enabled	0

Esc = Exit Menu F1/Shift+1 = Help
Alt+N = Global Properties -/+ = Alter Boot Order Ins/Del = Alter Boot List

Figure 7. Setting boot order to 0 for Onboard SAS Controller

5. Press Esc to exit the Adapter List screen. Use the arrow keys to select Exit the Configuration Utility and Reboot, then press Enter.



Figure 8. Saving the BIOS setting and rebooting

The blade now boots from the internal disk and will not scan the external drives during the boot. The first boot device is the Onboard SAS Controller.

Configuring blades with a boot disk connected through the SAS Expansion Card

Follow these steps when the SAS RAID Module is configured to boot the host blade, and also for data drives.

Note: The boot drive must be mapped to LUN0, and the data drive mapping can be any drive starting at LUN1. The boot drive must not be shared with other hosts blades on the SAS RAID Module.

1. During the blade boot, press F1 to disable the Onboard SAS Controller. The Devices and I/O Ports screen displays.

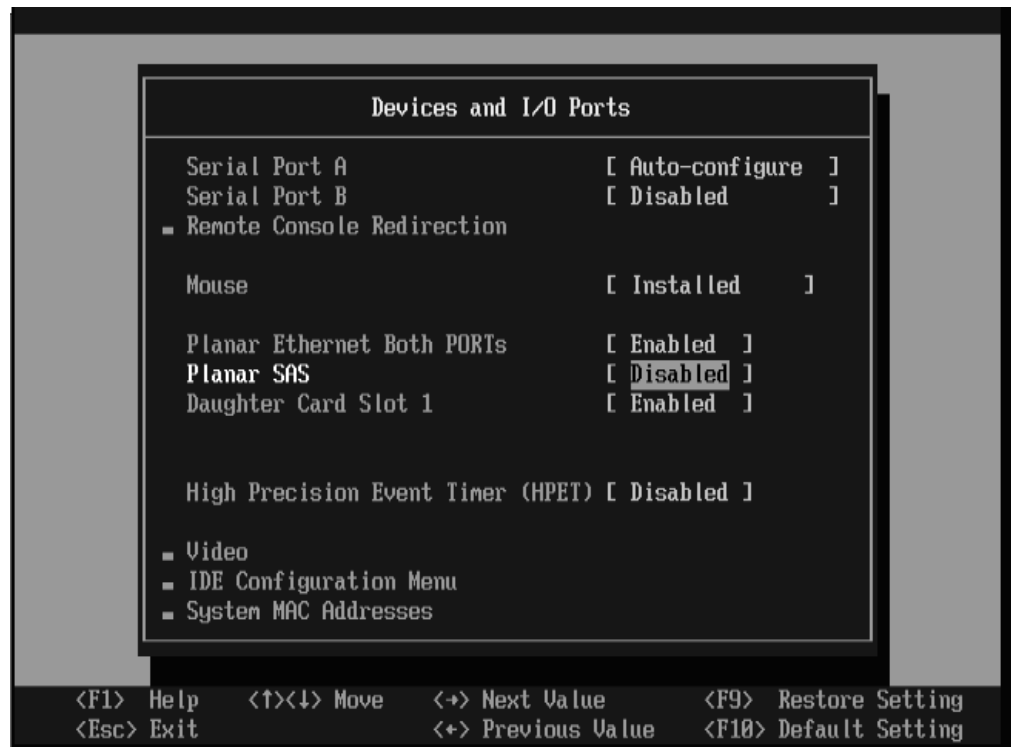


Figure 9. Devices and I/O Ports screen

2. Press Esc to exit the Devices and I/O Ports screen.
3. When the <<<Press Ctrl-C to start LSI Logic Configuration Utility>>> prompt displays during system boot, press Ctrl+C to enter the LSI Logic Configuration Utility. The Adapter List screen displays, similar to Figure 10 on page 43.

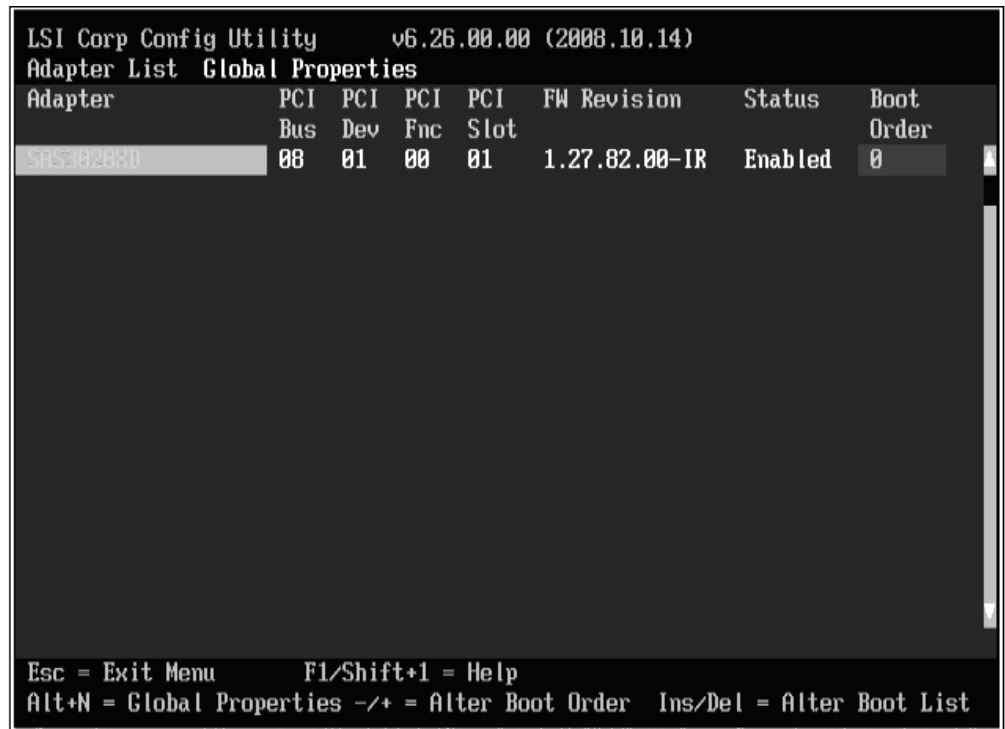


Figure 10. Adapter List screen showing SAS Expansion Card

4. Use the arrow keys to select the external SAS adapter then press Enter to display the Adapter Properties screen. Ensure that **Boot Support** is set to **[Enabled BIOS & OS]**.

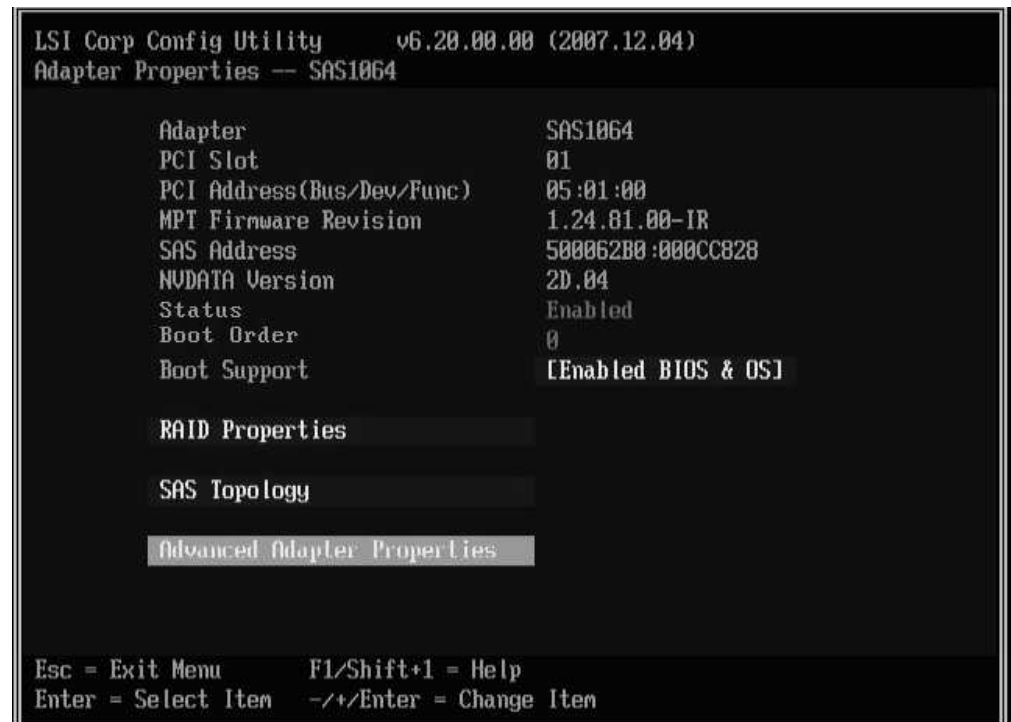


Figure 11. Adapter Properties screen showing enabled BIOS and OS boot support for the SAS Expansion Card

5. Use the arrow keys to select **Advanced Adapter Properties**, then press Enter. The Advanced Adapter Properties screen displays as shown in Figure 12.



Figure 12. Advanced Adapter Properties screen

6. Use the arrow keys to select **Advanced Device Properties**, then press Enter. The Advanced Device Properties screen displays as shown in Figure 13 on page 45.

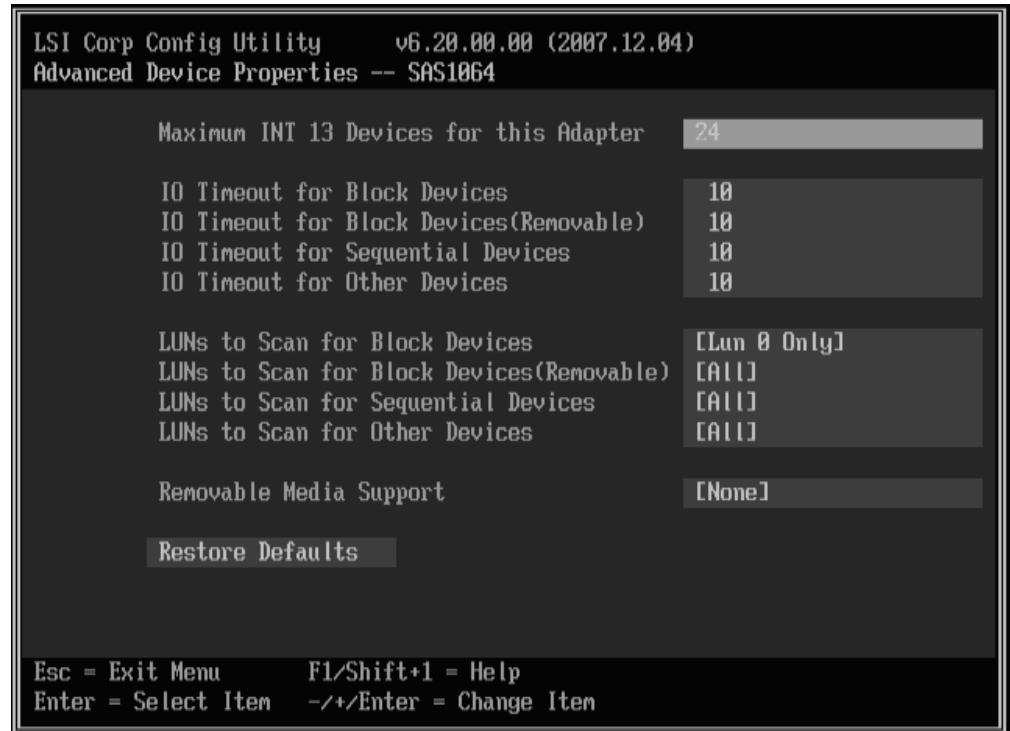


Figure 13. Advanced Device Properties screen

7. Use the arrow keys to navigate to **LUNs to Scan for Block Devices** and set it to **[Lun 0 Only]**.
8. Press Esc to exit the Adapter Properties screen until the utility asks you to save the configuration as shown in Figure 14. Use the arrow keys to select Save changes then exit this menu, then press Enter.

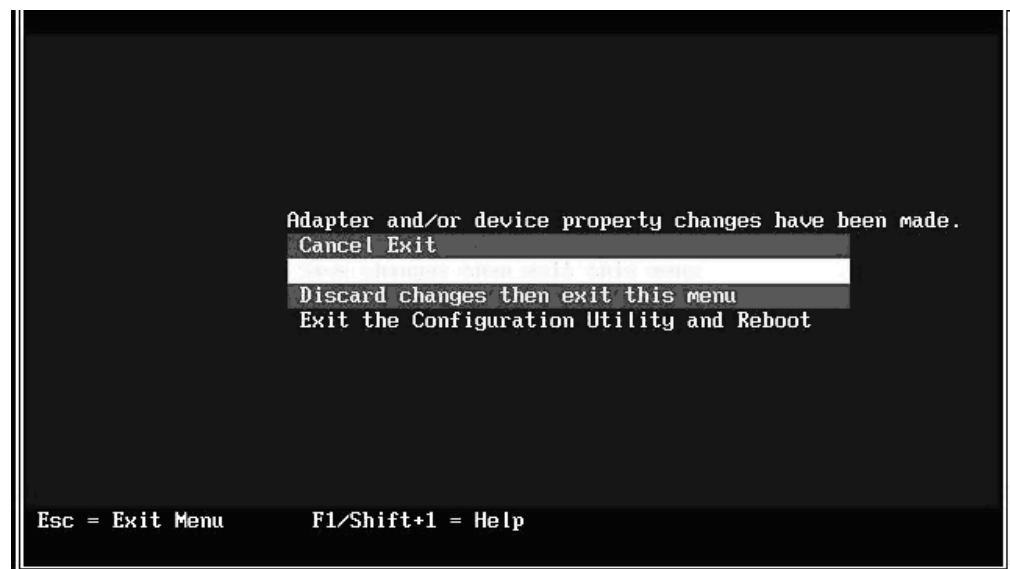


Figure 14. Saving configuration changes for the SAS Expansion Card

9. Press Esc to exit the Adapter List screen. Use the arrow keys to select Exit the Configuration Utility and Reboot, then press Enter.



Figure 15. Saving the BIOS setting and rebooting

Configuring blades with the SAS Connectivity Card

Follow these steps for blades that have the SAS Connectivity Card instead of an SAS Expansion Card. For configurations with the SAS Connectivity Card, the internal hard drive and external drives are on the same storage bus. To configure the blade to operate the SAS Connectivity Card, the Onboard SAS Controller BIOS must be set to scan LUN0 only during the boot and the external drives must be mapped with numbers higher than 0.

Note: If you map drives to the host through the RAID Controller command line interface, you must start the drive mapping with LUN1 or higher. If you start the drive mapping at LUN0, a boot delay will occur.

For blades that have the SAS Connectivity Card and are configured to be booted from an external SAS drive, the internal hard drive must be removed. Except for the requirements to remove the internal disk and to map a boot volume to the blade, the configuration for internal hard drive boot and external SAS boot is identical.

1. When the <<<Press Ctrl-C to start LSI Logic Configuration Utility>>> prompt displays during system boot, press Ctrl+C to enter the LSI Logic Configuration Utility. The Adapter List screen displays, similar to Figure 16 on page 47.

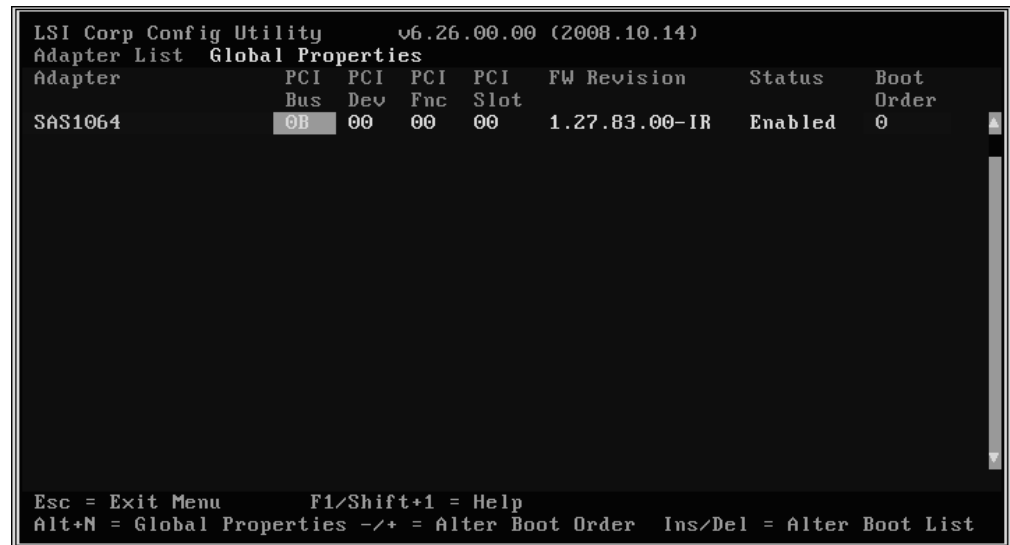


Figure 16. Adapter List screen showing the Onboard SAS Controller.

2. Use the arrow keys to select the Onboard SAS Controller then press Enter to display the Adapter Properties screen.

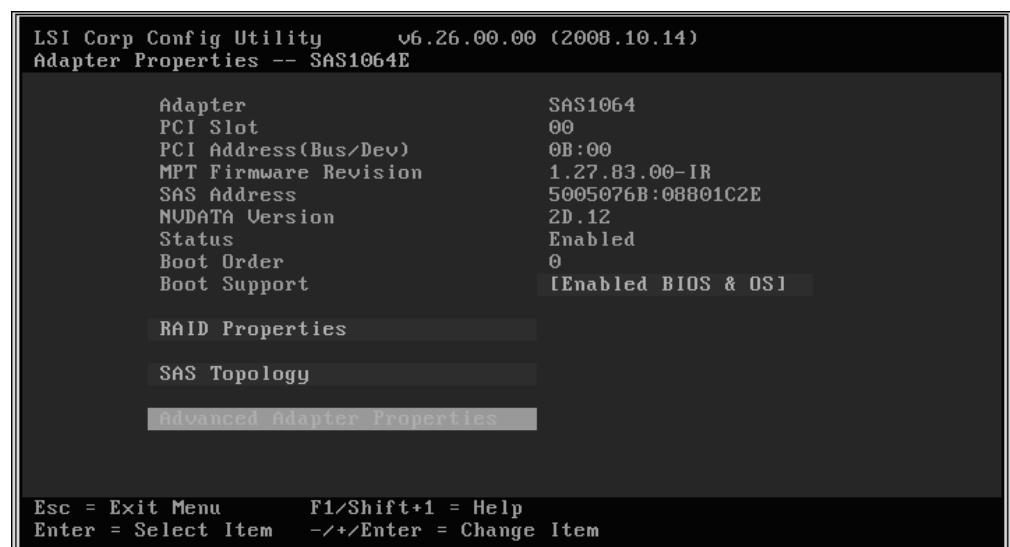


Figure 17. Adapter Properties screen for the Onboard SAS Controller

3. Ensure that **Boot Support** is set to [Enabled BIOS & OS].
4. Use the arrow keys to select **Advanced Adapter Properties**, then press Enter. The Advanced Adapter Properties screen displays as shown in Figure 18 on page 48.

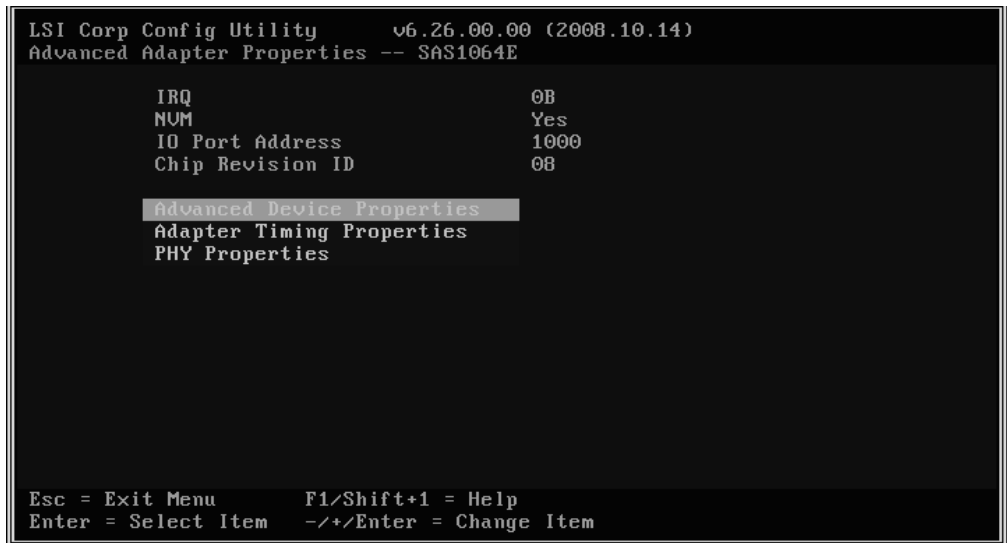


Figure 18. Advanced Adapter Properties screen

5. Use the arrow keys to select **Advanced Device Properties**, then press Enter. The Advanced Device Properties screen displays as shown in Figure 19.

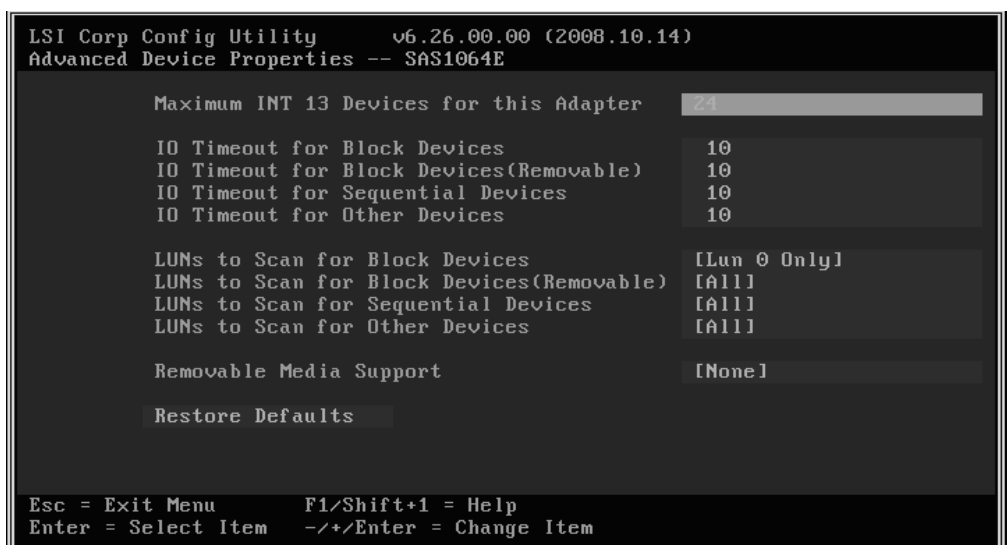


Figure 19. Advanced Device Properties screen

6. Use the arrow keys to navigate to **LUNs to Scan for Block Devices** and set it to **[Lun 0 Only]**.
7. Press Esc to exit the Adapter Properties screen until the utility asks you to save the configuration as shown in Figure 20 on page 49.

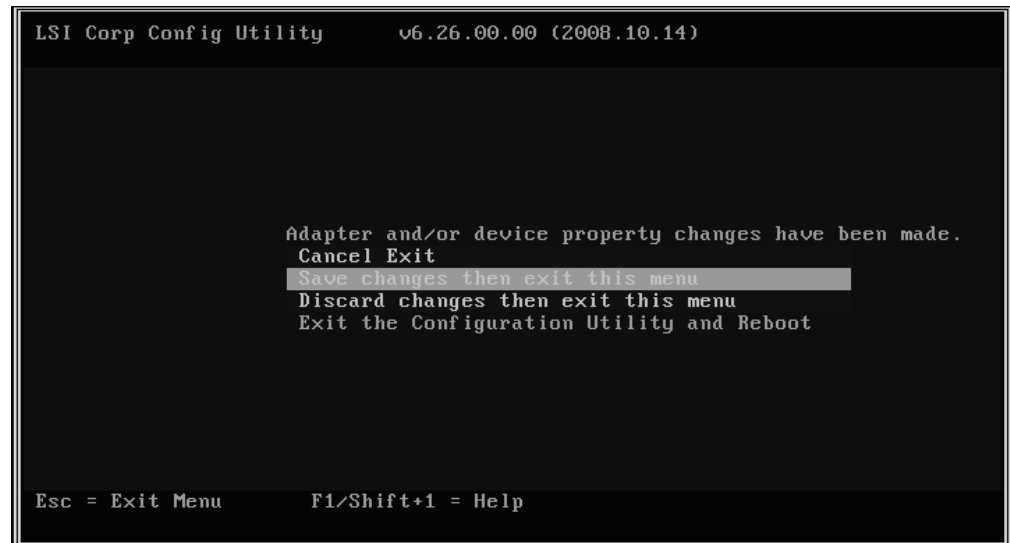


Figure 20. Saving configuration changes for the Onboard SAS Controller

8. Use the arrow keys to select Save changes then exit this menu, then press Enter. The Adapter List screen displays again.
9. Press Esc to exit the Adapter List screen. Use the arrow keys to select Exit the Configuration Utility and Reboot, then press Enter.

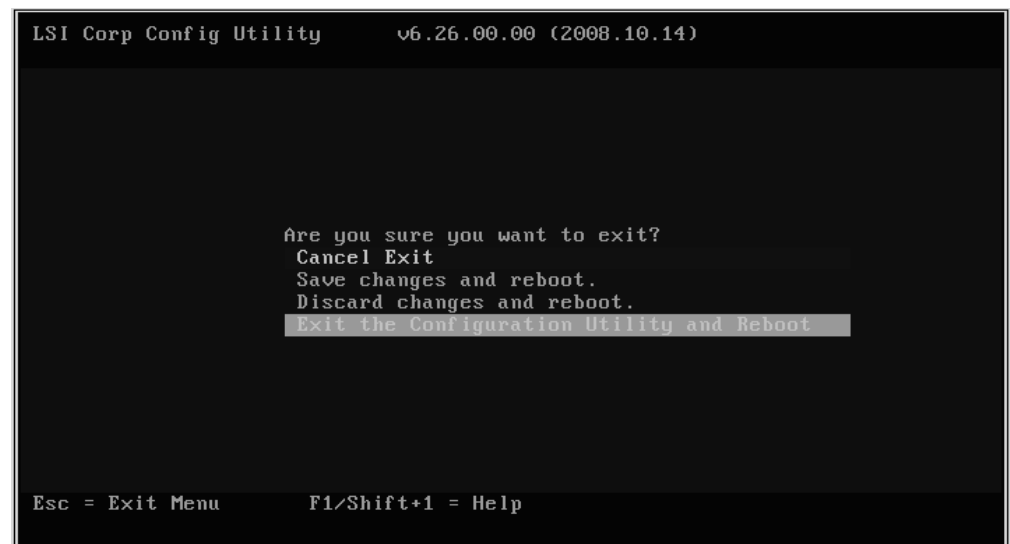


Figure 21. Saving the BIOS setting and rebooting

Disabling IGMP snooping

Internet Group Management Protocol (IGMP) snooping is the process of listening to IGMP network traffic. In a cluster configuration, you should disable IGMP snooping to prevent node failover issues. Perform the following steps to disable IGMP snooping.

Disabling IGMP snooping through Telnet

1. Log into the Advanced Management Module:

- a. Enter the IP address of the Advanced Management Module into the Web browser URL field. If you have the Advanced Management Module connected to your network, log in using the network IP assigned to it. If you are using the default IP address your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module .

Note: The default IP address for the Advanced Management Module is 192.168.70.125.

- b. Enter the username and password.
 - The default username is: USERID
 - The default password is: PASSWORD (the sixth position is the numeral zero)
- c. When prompted for the **Inactive session timeout value**, select **no timeout**.

Note: Remember to log out when you have completed your session. If you do not log out, the system shows an error the next time you try to log in.

2. From the main menu, select the Ethernet module and choose **Advanced Configuration**.
3. Select **Start Telnet Session**.
4. Type `cfg` and press Enter to open the configuration menu.
5. Type `group` and press Enter to open the group menu.
6. Select the appropriate group number at the prompt
7. Type `igmp` at the selected group menu to change the IGMP setting.

```
>> Group 1# igmp
Current Enable/Disable IGMP snooping on current group: enabled
Enter new Enable/Disable IGMP snooping on current group [d/e]:
```
8. Press `d` to disable IGMP snooping.

Disabling IGMP snooping through a web session

1. Log into the Advanced Management Module:
 - a. Enter the IP address of the Advanced Management Module into the Web browser URL field. If you have the Advanced Management Module connected to your network, log in using the network IP assigned to it. If you are using the default IP address your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module .

Note: The default IP address for the Advanced Management Module is 192.168.70.125.

- b. Enter the username and password.
 - The default username is: USERID
 - The default password is: PASSWORD (the sixth position is the numeral zero)
- c. When prompted for the **Inactive session timeout value**, select **no timeout**.

Note: Remember to log out when you have completed your session. If you do not log out, the system shows an error the next time you try to log in.

2. From the main menu, select the Ethernet module from the Advanced Management Module and select **Advanced Configuration**.

3. Select **Start Web Session**.
4. From the navigation panel, select **Miscellaneous settings > Uplink/Group**.
5. For IGMP settings, select **Disable** from the list of options.

Chapter 8. Using the RAID Controller command line interface

This section provides an overview and highlights some of the commands used in the RAID Controller command line interface.

The RAID Controller command line interface (CLI) is an independent program that you can use to operate the RAID controller. You must log in to a Telnet/ssh session using your user ID and password. The RAID Controller command line interface program starts automatically, and a <CLI> prompt appears. When you exit from the RAID Controller command line interface program, the Telnet/ssh session ends simultaneously.

Example of a user ID login:

```
> telnet controllerip
```

```
(none)login: USERID  
password:
```

```
Linux(none) 2.4.20_mv131-alc Rel H-2.4.20.12 Wed Jun 17 15:03:32 PDT 2009 ppc unknown
```

```
MontaVista(R) Linux(R) Professional Edition 3.1
```

```
<CLI>
```

List of commands

Use the commands defined by the RAID Controller command line interface to configuration and maintain the RAID controller. The commands are categorized into the following categories:

1. Display Commands
2. Volume Management
3. Volume Services
4. System Control and Configuration

Size reporting through the CLI

The RAID Controller command line interface (CLI) reports the precision of volume, storage pool, and disk drive sizing to the nearest gigabyte. When adding fractions of a gigabyte, the CLI rounds the result to the nearest gigabyte.

Display help for commands

If any <CLI> command is issued with the -help option, a contextual help page is displayed. Type help at the <CLI> command prompt to display the list of available commands.

Display commands

Use the SAS Switch command line interface for the RAID controller to perform administrative tasks for the device. This topic details the commands that you can use to display information.

detail controller

The detail controller command creates output detailing information about the controller selected.

Command arguments:

<CLI> detail controller -ctlr [0|1]

Where:

- [0|1] - Allows selection of the controller.

Example:

<CLI>detail controller -ctlr [0|1]

Current Machine Local Time: 07/26/2012 00:35:24 AM

Controller Information :

UltraSlice Version	:	ALC3300
Software version	:	H-2.1.2.4
Uboot Version	:	H-1.1.4.6
OS version	:	H-2.4.20.12
SES version	:	0107
BMC version	:	S0BT10A 0121 02/08/2010
FPGA version	:	01.07
CPLD version	:	S0CP00A C00A 01/01/2000
SAS switch version	:	S0SW01D R107 12/17/2009
Chassis Serial Number	:	KQWZZN1
WWN	:	5005076b07402cff

Chassis Machine Type/Model	:	8886AC1
SAS RAID Controller Module Part Number	:	43W3605
SAS RAID Controller Module FRU Part Number	:	43W3630
SAS RAID Controller Module Serial Number	:	YK101279B016
Machine Signature	:	
SAS RAID Controller Module Location	:	IO Bay 3
Manufacturer ID	:	IBM
SAS RAID Controller Module Hardware Revision ID	:	2
SAS RAID Controller Module Hardware Product ID	:	00a5
MAC Address (upto 8)	:	00:1A:64:9E:00:61
Target port WWN	:	5005076b07402ca0
Target port protocol	:	SAS
Target port speed	:	3Gbps

Current Status	:	SECONDARY
System Hardware Configuration Mode	:	Dual
BBU State	:	1 (Working)
BBU Fault Code	:	0 (None)
BBU Part Number	:	45W4439
BBU Serial Number	:	YK10MY2810D2
BBU FRU Number	:	45W5002
BBU Firmware Revision	:	58.0
BBU Expiration Date	:	Sat Jul 23 12:00:00 2016
Charging state information	:	
BBU Charging	:	False
BBU Capacity (Hours)	:	72+

Associated Volumes currently serviced by this controller:

Vol#	VolumeName	Cap	RaidType	Status
0	plr10:plr10_V01	1000GB	10	VBL INI
1	plr10:plr10_V02	2000GB	10	VBL INI TRN
2	plr10:plr10_V03	100GB	10	VBL INI TRN

Usage: VBL=Viable DEG=Degraded INI=Initied
 NVBL=Non-Viable TRN=In-Transition

detail drive

The **detail drive** command creates output detailing information about the drive specified by the bay position.

When the drive is specified by a number, that number refers to the sequence number that appears on the list displayed when issuing the **list drive** command. Issue the **list drive** command before you issue **detail drive** with the **-number** option, so that there is an internal reference list. If you do not issue the **list drive** command first, an error displays.

Command arguments:

<CLI> detail drive [-slot | -number [REFNUM]]

Where:

- [REFNUM] - Refers to the sequence number on the list displayed when you issue the **list drive** command.

Example:

<CLI> detail drive -slot 1:1

Drive#	E:T	SerialNo	Cap	Pool	Usage	State
0	1:1	9QK0SWLM	698GB	raid10pool	GRP	OK

Mount State	Ct10	Ct11	RPM	FW level
Online	1	1	7200	BC1D

Drive SAS Address : 5000c5000d218b73
 Vendor / Manufacturer ID : IBM-ESXS
 IBM Option Number : 42D0546
 IBM FRU Number : 42D0548
 IBM Part Number : 42C0279
 Interface Type : SAS
 Disk Speed : 7200
 Serial Number : 9QK0SWLM
 Code Level : BC1D
 Product Master ID : 41Y8468
 Product Family ID : ST3750630SS

Volume	RaidType	Size
raid10pool:rd10vol1	10	174GB

raid10pool:rd10vol3	10	174GB
raid10pool:rd10vol5	10	174GB
raid10pool:rd10vol4	10	174GB
raid10pool:rd10vol2	10	174GB
raid10pool:rd10vol6	10	174GB
raid10pool:rd10vol8	10	174GB
raid10pool:rd10vol7	10	174GB

detail pool

The **detail pool** command provides detailed information about any pool. The pool can be specified by a name or number. The **-name** option uses the pool name as input.

Command arguments:

```
<CLI> detail pool [-name poolname | -number number]
```

Where:

- *poolname* - Defines the name of the pool.
- *number* - Refers to the sequence number on the list displayed when you issue the **list pool** command.

Example:

```
<CLI> detail pool -name pool1
```

ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
2	DG2	1	IO 3	33GB	28GB	Viable	MV	No

When the pool is specified by a number, that number refers to the sequence number that appears on the list displayed when issuing the **list pool** command. Issue the **list pool** command before you issue **detail pool** with the **-number** option, so that there is an internal reference list. If you do not issue the **list pool** command first, an error displays.

Any volume service currently running on this pool also displays in the status.

The *state* definitions are:

- *UN* - Unmounted, Non-viable
- *MF* - Mounted, Failed
- *UF* - Unmounted, Failed
- *DN* - Dismounted, Non-viable
- *DF* - Dismounted, Failed
- *UV* - Unmounted, Viable
- *DV* - Dismounted, Viable
- *MV* - Mounted, Viable
- *MN* - Mounted, Non-viable

Note: One or more drives are missing in this pool. You must acknowledge an alert pertaining to this state. If the missing drive comes back to make the pool viable, the state automatically changes to *MV*. When you acknowledge the alert, the state of the pool becomes *UN*.

Information about a drive in the primary section is as follows:

Slot	SerialNo	Cap	Grp	Usage	State	Mount State	Ctl0	Ctl1
1:5	DQR9P6C00D3F	33GB	DG2	GRP	OK	Mounted	1	1

Information about a drive in the secondary section is as follows:

Slot	SerialNo	Cap	Grp	Usage	State	Mount State	Ctl0	Ctl1
2:6	DQR9P6C00D8S	33GB	DG2	GRP	OK	Mounted	1	1

Information about existing volumes is as follows:

Volumes	Cap	GrpName	RaidType	Status
DG2:Vol5	690MB	DG2	10	Viable Initd
DG2:Vol6	1GB	DG2	10	Viable Initd
DG2:Vol7	1GB	DG2	10	Viable Initd
DG2:Vol8	1GB	DG2	10	Viable Initd

detail volume

The **detail volume** command creates output detailing information about any volume. The volume can be specified by name or number. The name is specified as a *poolName:volumeName* combination.

When the volume is specified by a number, that number refers to the sequence number that appears on the list displayed when issuing the **list volume** command. Issue the **list volume** command before you issue **detail volume** with the **-number** option, so that there is an internal reference list. If you do not issue the **list volume** command first, an error displays.

The *state* definitions are:

- *UN* - Unmounted, Non-viable
- *MF* - Mounted, Failed
- *UF* - Unmounted, Failed
- *DN* - Dismounted, Non-viable
- *DF* - Dismounted, Failed
- *UV* - Unmounted, Viable
- *DV* - Dismounted, Viable
- *MV* - Mounted, Viable
- *MN* - Mounted, Non-viable

Note: One or more drives are missing in this pool. You must acknowledge an alert pertaining to this state. If the missing drive comes back to make the pool viable, the state automatically changes to *MV*. When you acknowledge the alert, the state of the pool becomes *UN*.

Information about contributing drives is as follows:

Drive#	Slot#	SerialNo	Cap	Pool	Usage	State	Mount State	Ctl0	Ctl1
--------	-------	----------	-----	------	-------	-------	-------------	------	------

0	1:5	DQR9P6C00D3F	33GB	DG2	GRP	OK	Mounted	1	1
1	2:6	DQR9P6C00D8S	33GB	DG2	GRP	OK	Mounted	1	1

Information about an associated controller is as follows:

Controller	Status	Ports	LUNs
Ctrl0	MASTERBOUND	1	1

Command arguments:

<CLI> detail volume [-name poolname:volumename] [-number number]

Where:

- *poolname:volumename* - Allows selection of the volume name as a combination of *poolname* and *volumename*.
- *number* - Refers to the sequence number on the list displayed when you issue the **list volume** command.

Example:

<CLI> detail volume -name pool1:vol1

View Volume Info vol1

VolumeName	Cap	RaidType	Status
pool1:vol1	4GB	0	Viable

HostLUNs mapped:

HostWWN	LUN	Permission
784875485454	3	READWRITE

Pool information:

ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
1	pool1	0	IO 3	33GB	28GB	Viable	MF	No

detail volume verbose

The **detail volume verbose** command creates output detailing information about all of the Logical Unit Numbers (LUNs). A LUN is a number assigned to a logical unit.

Command arguments:

<CLI> detail volume verbose

Example:

<CLI> detail volume verbose

Name	RaidType	HostWWN	LUN	Size	Status
pool1:vol1	0	784875485454	3	4GB	Viable

list controller

The **list controller** command creates output providing summary information about each controller. The status of a controller is the actual running state of the controller.

Command arguments:

<CLI> list controller

Ctlr#	Controller	Status	Ports	LUNs
0	Ctr10	MASTERBOUND	1	1
1	Ctr11	SLAVEBOUND	1	1

Examples:

<CLI> list controller

Ctlr#	Controller	Status	Ports	LUNs
0	Ctr10	STARTING	1	1
1	Ctr11	SHUTDOWN	1	1

list drive

The **list drive** command creates output providing summary information about each drive.

The drive bay number is *E:T*. *E:T* stands for [Enclosure]:[Tray], where *E* is the enclosure number and *T* is the position of the hard drive. These positions/locations begin with 1 and 1 is the uppermost drive.

The *usage* definitions are:

- *UNA* - UnAssigned
- *GRP/SGR* - Current/Stale Group Member
- *FOR* - Foreign
- *GLS/SGS* - Current/Stale Global Spare
- *NQ* - Non-qualified
- *LCS/SLS* - Current/Stale Local Spare
- *CBL/SCL* - Current/Stale Auto-copy-back Local Spare
- *CBG/SCG* - Current/Stale Auto-copy-back Global Spare

The *state* definitions are:

- *OK* - Healthy
- *M* - Missing
- *P* - Predicted Failure (PFA)
- *U* - Unreliable

Note: M P U states can be combined.

- *PM* - Path Missing
- *UP* - UnReliable PFA
- *MP* - Missing PFA
- *MUP* - Missing UnReliable PFA
- *MU* - Missing UnReliable
- *INI* - Initialized
- *UNS* - Unsupported (non-IBM device).
- *PM* - Path Missing The drive is OK, but one or more paths are not usable.
- *IMD* - Incompatible metadata The metadata on the drive is incompatible with the firmware version. Assimilate the drive or upgrade the firmware.
- *UNF* - Unsupported drive firmware version

Important: Drive assimilation a destructive procedure causing complete data loss. Use this command only if your intention is to irrevocably erase all disk data.

Command arguments:

<CLI> list drive

Example:

<CLI> list drive

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ct11	Ct12	RPM
--------	-----	----------	-----	------	-------	-------	-------------	------	------	-----

0	1:4	DQR9P6C00D1H	33GB	--	UNA	U	Dismounted	1	1	0
1	1:5	DQR9P6C00D3F	33GB	DG2	GRP	OK	Mounted	1	1	0
2	2:6	DQR9P6C00D8S	33GB	DG2	GRP	OK	Mounted	1	1	0
3	2:2	DQR9P6C00D8U	33GB	--	UNA	OK	Mounted	1	1	0
4	2:1	DQR9P6C00D8V	33GB	--	UNA	OK	Mounted	1	1	0
5	2:3	DQR9P6C00D9A	33GB	--	UNA	OK	Mounted	1	1	0
6	1:6	DQR9P6C00DBK	33GB	--	UNA	OK	Mounted	1	1	0
7	1:3	J3XU3MVK	33GB	--	UNA	OK	Mounted	1	1	0
8	1:1	J3XU3R0K	33GB	--	UNA	OK	Mounted	1	1	0
9	1:2	J3Y564BK	33GB	--	UNA	OK	Mounted	1	1	0
10	2:4	J3Y8DVLK	33GB	--	UNA	OK	Mounted	1	1	0
11	2:5	J3YWKMJ	33GB	--	UNA	OK	Mounted	1	1	0

list pool

The **list pool** command creates output providing summary information, including the status, about each pool. Any volume service currently running on a pool is also shown in the status. Size displayed is total and available capacity.

The *state* definitions are:

- *UN* - Unmounted, Non-viable
- *MF* - Mounted, Failed
- *UF* - Unmounted, Failed
- *DN* - Dismounted, Non-viable
- *DF* - Dismounted, Failed
- *UV* - Unmounted, Viable
- *DV* - Dismounted, Viable
- *MV* - Mounted, Viable
- *MN* - Mounted, Non-viable.

Note: One or more drives are missing in this pool. You must acknowledge an alert pertaining to this state. If the missing drive comes back to make the pool viable, the state automatically changes to *MV*. When you acknowledge the alert, the state of the pool becomes *UN*.

Command arguments:

<CLI> list pool

Example:

<CLI> list pool

Pool#	ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
0	1	DG1	5	IO 3	267GB	117GB	Degraded-InTransition	MV	Yes

list volume

The **list volume** command creates output providing summary information about all volumes. The volume name displays as poolname:volumename.

The possible states of a volume are:

- Viable
- Degraded
- InTransition
- Initied

An *Initied* state indicates that the volume has been initialized.

Command arguments:

<CLI> list volume

Example:

<CLI> list volume

vol#	VolumeName	Cap	RaidType	Status
0	pool1:vol1	4GB	0	Viable
1	Group0:vol1	183GB	5	Viable
2	ADMIN:v2	197GB	10	Degraded
3	MyData:MyVolume	4GB	0	Initied
4	pl23:volume0	44GB	0	InTransition

System control and configuration commands

Use the RAID Controller command line interface to perform administrative tasks for the device. This topic details commands about system control and configuration.

alert

The **alert** command displays system alerts, changes the state of system alerts, and creates a generic alert. Use the -get option to display alerts generated in the system at any given point. To change the state of the alerts specified by the alert code and alert id, use the -mask, -unmask, or -ack option. Use the -create option to create a generic alert with the alert code specified by the -code option.

Note: Refer to the Troubleshooting section for description and details on the alerts and codes.

Command arguments:

<CLI> alert [-get | -mask | -unmask | -ack | -savehistory | -create | -clear]

-help option

Usage : alert [-get | [-create|-clear] -code genericAlertCode | -savehistory |
-[mask | unmask | ack] -code AlertCode -id Id -ctlr SlotID]
[-get] : Displays the alerts generated in the system at any given point.
[-mask] : When this command is used with mask/unmask or ack options, it can be used to
change the state of the alerts in the system specified by the alert code and
alert id.
[-savehistory] : Saves alert history into a file.
-code : alert code of the alert you want to take action on.

-id : id of the alert message to be taken action on .
 -ctrl : slotID of the controller where you want the action to be taken place on an alert message.
 [-create] : This option can be used to create a generic alert with the alert code specified by '-code' option. The valid range for the alert code is between 10000-19999. The description and details of these codes can be found in RAS user guide.
 [-clear] : This option can be used to clear a generic alert with the alert code specified by '-code' option. The valid range for the alert code is between 10000-19999.

Example:

```
<CLI> alert -get
Current Machine Local Time: 04/02/2009 11:24:34 AM
```

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
5600	2	20090325124508	0	Info	5005076b074059ff	1	Masked
Msg: Illegal host 0x500062b00007ccc0 access attempted							

battery

Use this command to manage the Battery Backup Units.

Command arguments:

```
<CLI> battery -ctrl [0|1] -get
```

Where:

- [0|1] - Allows you to select controller 0 or 1.

When you issue this command with the -get option, the current status of the battery is displayed:

Example:

```
<CLI> battery -ctrl 0 -get
```

Controller 0

Basic battery type and status

```
BBU State : 1 (Working)
BBU Fault Code : 0 (None)
```

```
Part Number : 45W4439
Serial Number : YK10MY2810D2
FRU Number : 45W5002
FirmwareRev : 58.0
Expiration Date : Sat Jul 23 12:00:00 2016
```

Charging state information

```
Charging : False
Capacity (Hours) : 72+
```

```
<CLI>
```

cache settings

Use this command to specify the cache settings.

Command arguments:

```
<CLI> cache -[get | set [-volumesetting -seqpostreadcmdsize [SIZE]
-seqreadaheadmargin [MARGIN] -writecachepolicy [off|on|default]
[-systemdefault] [-volumename [POOL:VOLUME]] | ctrlsetting
-writecachepolicy [on|off] ]
```

Where:

- *[SIZE]* - Indicates maximum sector count of single predictive read ahead.
- *[MARGIN]* - Defines number of sectors in read ahead buffer.
- *[off|on|default]* - Allows you to turn -writecachepolicy off or on or to use with default settings.
- *[POOL:VOLUME]* - Indicates pool name and volume name. If pool name not specified, all system volume settings are modified; if pool name specified but volume name is not specified, cache settings are applied to all volumes in pool.
- *[on|off]* - Allows you to turn -writecachepolicy on or off when -ctrlsetting option is specified.

The maximum sector count of a single predictive read ahead is seqpostreadcmdsize. A value of 0 disables predictive read for this volume. A value of 1-128 overrides the previous setting and represents a command transfer size that is a multiple of 16Kb. A value of (0xFFFF) causes the default value to be used. The number of sectors in the read ahead buffer is seqreadaheadmargin. This parameter is ignored if the seqpostreadcmdsize is zero. The valid range is 1 to 0x7FFF. A value of (0xFFFF) causes the default value to be used. The firmware sets the writecachepolicy to specify the write cache policy. If none of the cache options are provided, the current system default settings are used.

If you do not specify the -poolname, all volumes in the system will have their settings modified. If you specify the -poolname but do not specify the -volumename, the cache settings will be applied to all the volumes in the pool.

If you specify the -systemdefault option, the setting is used to change the system default. System default is used to set the cache policy for a new volume that was created with the cache policy set to default.

If you specify the -get option, the system default setting is displayed.

If you specify the -ctrlsetting option, the write cache settings for the controller are set.

chpasswd

Use this command to change the password for the selected user on an SAS RAID Module. If the firmware level of your RAID controllers is older than 1.2.x.xxx, you need to change the password on both SAS RAID Modules at the same time. If the firmware level of your RAID controllers is 1.2.x.xxx or newer, then changing the password on one SAS RAID Module automatically changes the password on the other SAS RAID Module.

Command arguments:

```
<CLI> chpasswd [-cli | mgmtInterface ] -oldpasswd [OLDPWD] -newpasswd [NEWPWD]
```

-help option

```
Usage          : chpasswd [-cli | mgmtInterface ] -oldpasswd [OLDPWD] -newpasswd [NEWPWD]
-cli           : change the password for the CLI user
-mgmtInterface : change the password for the management interface
OLDPWD         : old password for the user
NEWPWD         : new password for the user - it should be minimum of 8, maximum of 16 characters
                  There should be at least one alphabet and one numeric character in the password
                  Please use a combination of upper and lower case letters and numbers for the
                  password
```

clilog

The **clilog** command prints the log of all CLI commands issued and their timestamps. If you specify the **-save** option with a filename, the log is saved to the file.

Command arguments:

```
<CLI> clilog [-save file]
```

Where:

- *file* - Names the file where the log is saved.

Example:

```
<CLI> clilog -save clilogfile
```

comparams

The **comparams** command is issued by the system administrator to set or display the communication parameter settings. Communication is with outside agencies by using Telnet or one or more Ethernet communication links, and the serial port provided on the microprocessor.

Command arguments:

```
<CLI> comparams [-get -ctrl [0|1] -port [0|1] -ip i.j.k.l -gateway i.j.k.l
-netmask -i.j.k.l [-vlan n -vlaninsert [on|off]]]
```

Where:

- *[0|1]* - Allows selection of the controller or port.
- *i.j.k.l* - Allows selection of the IP address , gateway, or netmask.
- *n* - Allows selection of the VLAN tag.
- *[on|off]* - Allows selection of the VLAN tag insert.

Example:

<CLI> compparams -get

Ctlr0	Port0	Port1
IP ADDRESS	192.168.75.16	192.168.75.17
GATEWAY	192.168.75.1	192.168.75.1
NETMASK	255.255.255.0	255.255.255.0
VLAN tag	0d	0d
VLAN tag insert	0d	0d

Ctlr1	Port0	Port1
IP ADDRESS	192.168.75.18	192.168.75.19
GATEWAY	192.168.75.1	192.168.75.1
NETMASK	255.255.255.0	255.255.255.0
VLAN tag	0d	0d
VLAN tag insert	0d	0d

Switch Ip Address Information :

Switch Ip Address1	:
Switch Ip Address2	:

configure access

Use the **configure access** command to set or display configurable access protocols (SSH and Telnet).

An error occurs if you issue the -set option while the list is empty.

Note: If you disable both SSH and Telnet access protocols, you must reset the RAID controller back to the factory defaults to re-enable both access protocols. For instructions on resetting the RAID controller, see "How to reset the SAS RAID controllers to the factory defaults" on page 187.

Command argument:

configure access -[get | set -enable|disable [SSH|TELNET] | help]

Examples:

<CLI> configure access -get
Current Machine Local Time: 09/16/2011 04:28:38 AM

Access Protocol	Status
TELNET	ENABLED
SSH	ENABLED

<CLI> configure access -set -disable telnet
<CLI> configure access -get

Access Protocol	Status
TELNET	DISABLED
SSH	ENABLED

configure alert

The **configure alert** command selects the alert messages to send by email. Previously configured messages display as *configured* and can be cleared.

Use the **-get** option to display the list of alerts and to build a local list of system alerts before using the **-set** option to configure the alerts. Use the **-set** option to clear the list. An error appears if you issue the **-set** option while the list is empty.

Command arguments:

<CLI> configure alert [-get | -set | -setgenericalerttemplate]

-help option

Usage : configure alert [-get | set [-email | -initiallymasked] -on <RefNum RefNum...> -off <RefNum RefNum...> | setgenericalerttemplate -code <genericAlertCode> -type [persistent|ackable] -initiallymasked [on|off] -email [on|off] -severity [critical|warning|info] -msg "DesiredAlertStringInQuotes"]

[-get] : Displays the email and initiallymasked properties of alerts currently defined in alertTemplates.

[-set] : Enables the user to set the email and initiallymasked attribute for any email.

[-setgenericalerttemplate] : Enables the user to create or replace an entry in alertTemplates for generic alerts.

on : Sets the attribute to 'on' for the alertCode specified by RefNum.

off : Sets the attribute to 'off' for the alertCode specified by RefNum.

email : When email attribute is set for an alert, an email is generated every time that alert is created in the system. When this attribute is set, email is only generated for future events and not for existing alerts.

initiallymasked : When this attribute is set for an alert, initiallymasked LED is lighted every time that alert is created in the system. When this attribute is set, LED is lighted for future events and not for existing alerts.

type : Defines the type of alert for generic alert being specified.

severity : Defines the severity of alert for generic alert being specified.

msg : Defines the message for the generic alert. The string should be specified within quotes for this command. The string is saved in the alertTemplates without the quotes.

Where:

- *number* - Defines the reference number of the alert displayed by using the **-get** option.

Examples:

<CLI> configure alert -get
Current Machine Local Time: 04/08/2009 09:47:11 AM

Ref#	Code	EmailOn State	InitialMask State	AlertMsg
1	0	On	Unmasked	TestAlert %s
2	2	Off	Masked	Compatible drive enclosure %<EnclosureId> found
3	3	Off	Masked	Drive enclosure %<EnclosureId> removed
4	4	Off	Masked	Drive enclosure %<EnclosureId> firmware updated
5	100	On	Masked	Controller firmware updated
6	101	Off	Masked	Disorderly shutdown detected - System restored from battery backup
7	102	On	Unmasked	Controller in survivor mode - Redundant controller %<ControllerId> is offline
8	103	Off	Masked	New controller recognized
9	104	Off	Masked	Replacement media tray %<BackplaneId> detected

10	105	Off	Masked	ArtsTime %<AltString:1=initialized:2=updated> - previous value was %<TimeDate>
11	110	Off	Masked	API requested %<AltString:1=ctlr1:2=ctlr2:3=ctlrs 1&2> to shutdown and %<AltString:1=power off:2=enter service mode>

configure pool

The **configure pool** command allows of user to change the owner controller for a group from CLI. This command must be run on a survivor controller. The other controller must be in service mode.

Command arguments:

```
<CLI> configure pool -name [POOLNAME] -changeowner
```

-help option

```
COMMAND-HELP: configure pool
```

This command is used to change the owner controller for a group from CLI.

This command must be run on a survivor controller. The other controller must be in service mode.

```
Usage          : configure pool -name [POOLNAME] -changeowner.
POOLNAME       : Name of the pool that needs to change the owner controller.
```

Examples:

```
<CLI> configure pool -name plr5 -changeowner
Current Machine Local Time: 02/07/2013 11:04:44 AM
Error : Change pool ownership command failed
Reason: Controller state is not valid for this request
```

Note: One of controller must be in survivor mode.

```
<CLI> shutdown -ctlr 1 -state servicemode
Current Machine Local Time: 03/04/2013 01:22:51 PM
Shutdown Command accepted
```

```
<CLI>configure pool -name plr5 -changeowner
Current Machine Local Time: 03/04/2013 01:45:45 PM
Change pool ownership command successful
```

configure timeout

The **configure timeout** command displays and sets the session timeout for the command line interface. When the configured timeout period is reached, the system automatically closes the CLI session.

By default, CLI session timeout is disabled. The minimum timeout period is two minutes (120 seconds). To disable CLI session timeout after you have configured it, use the **-set** option and specify "00" for HR, MIN, and SEC.

An error appears if you issue the **-set** option while the list is empty or if the timeout value is invalid.

Command arguments:

```
<CLI> configure timeout -[get | set <HR:MIN:SEC> | help]
```

-help option

```
<CLI> configure timeout -[get | set <HR:MIN:SEC> | help]
Usage      : configure timeout -[get | set <HR:MIN:SEC> | help]
[-get]     : Displays the CLI session timeout settings
[-set]     : Sets the CLI session timeout period.
HR         : Number of hours. The number must be less than two digits.
MIN        : Number of minutes. The number must be less than two digits.
SEC        : Number of seconds. The number must be less than two digits.
```

Examples:

```
<CLI> configure timeout -set 00:01:30
Current Machine Local Time: 09/16/2011 03:54:33 AM
Error : configure timeout command failed
```

Note: The timeout period is less than two minutes.

```
<CLI> configure timeout -set 00:02:30
Current Machine Local Time: 11/16/2011 05:07:08 PM
CLI Session Timeout is set to 150 seconds
```

```
<CLI> configure timeout -set 00:00:00
Current Machine Local Time: 11/16/2011 05:07:21 PM
CLI Session Timeout is set to DISABLED
```

controller config

The **controller config** command is used for controller configuration. When this command is issued, a config file is generated where settings are stored or retrieved.

The two sections of the config file are:

- *System configuration* - Contains drive pool, volume, spares, and host configurations.
- *Controller settings* - Contains read write and read only fields. The read write fields contain cache settings (read and write cache enables), redundant mode, port speeds, topology, and IP address/net mask. The read only fields contain the controller World Wide Name (WWN), a unique 64-bit address used for identification.

Issue this command with the **-load** option for the following:

- *Restore factory settings* - This restores the factory default to the controller. Use a file that contains factory settings as the config file. The factory settings are in the *Controller settings* section of the file.
- *Canned Config* - This quickly prepares a system for operation based on predetermined settings. Use a file with a valid server and host configuration as the config file.
- *Clone system* - This uses the saved config file to program another system.

Issue this command with the **-save** option for the following:

- *Clone system* - This uses the saved config file to program another system.
- *Print configuration* - This prints the configuration of the system to the config file. You can read and edit the config file.

Issue this command with the **-get** option to print the config file information on the screen for all config files.

Command arguments:

```
<CLI> controller config [ -save | -load | -get | -delete | -deleteall]
```

Where:

- `[-save]` : Prints the configuration of a system out to a file and be read/edited by user.
- `[-load]` : By issuing this command with `-load.` option, following could be accomplished:
 1. Restore factory settings: A file with factory settings could be given as input filename which restores the factory default to the controller.
This path is mostly used for restoring factory defaults for controller settings (second part of the config file)
 2. Canned Config: A file with a valid back-end and host configuration can be provided to prepare a system for operation based on a pre-decided settings quickly.
 3. Clone system: A file coming from a configured system (generated using `[controller configuration -save filename])` command can be used to program another system.
- `FILENAME` : The filename specifies the name of the file where the settings are stored or retrieved "-" is an invalid character and should not be included in the filename.
- `[-get]` : Executing this command with `'-get'` option prints the config file's header information on the screen for all config files.
- `[-delete]` : Deletes the user generated configuration file(s) specified.
- `[-deleteall]` : Deletes all the user generated configuration file(s).

Example: none

email alert

The **email alert** command selects and sends critical alerts to the your users by email. It allows you to enter an email address configuration and save it. You can do this for up to five email addresses added one at a time. The host name, port number and sender setting overwrites existing settings. The email that is sent out has following format:

```
Alert Code:1300 Drive 3:5000c500003cd4ff failure detected - Previous drive status was spare
Controller WWN: 327654ABE76DD67C Controller SerialNumber : 123abfe56dd
```

Use the `-test` option to configure and send a test communication to a specified email account.

Command arguments:

```
<CLI> email alert [-get | delete -email email | set [-test] -email email -smtpserver server
-smtpport port -smtpsender [SENDER]]
```

-help option

```
<CLI> email alert [-get | delete -email email | set [-test] -email email -smtpserver server
-smtpport port -smtpsender [SENDER]]
```

- `[-set]` : Enables the user to enter an email address configuration and save it.
- `[-test]` : If this option is selected along with `[-set]` option, the email is configured and a test mail is sent. If this option is selected without any other option, the command sends a test alert to the email already configured
- `[-get]` : Displays the current email configuration with emailId , smtp server ,smtp port
- `[-delete]` : Deletes specific email id
- `EMAIL` : EmailId of the person who wants to get the alerts.
- `SERVER` : IP address of the SMTP server .

PORT : Port number on which SMTP server listens .
 SENDER : Sender's full IP address. SMTP domain name is extracted from it so it must be valid for email to work.The format of this input should be in user@domain format.

enclosure reporting

Use this command to get type, version, and status data on enclosures (Disk Storage Modules).

Command arguments:

<CLI> list enclosure

Encl#	Enclosure	Type	Version	Status
0	Encl0	Controller	0004	Good
1	Encl1	DSM	0.42	Good
2	Encl2	DSM	0.42	Good

<CLI> detail enclosure -encl 0

Enclosure Information:

Enclosure Type : Controller
 Package Version : 0100
 SES version : 0100
 Part No : PN
 FRU No : FN

Serial Number : SN
 Slot # : 4294967295
 Controller 1 :
 Voltage : 11.85 Volts
 Controller 2 :
 Voltage : 11.80 Volts
 Status : Good

<CLI> detail enclosure -encl 1

Enclosure Information:

Enclosure Type : DSM
 Package Version : 0.98
 SES version : 0.98
 Enclosure Processor Version : 0.98
 Power Controller Version : 1.13
 Part No :
 FRU No :

Serial Number :
 Slot # : 0
 Status : Good

<CLI> detail enclosure -encl 2

Enclosure Information:

Enclosure Type : DSM
 Package Version : 0.98
 SES version : 0.98
 Enclosure Processor Version : 0.98
 Power Controller Version : 1.13
 Part No :
 FRU No :

```

Serial Number      :
Slot #            : 0
Status            : Good

```

event log

The **event log** command detects and analyzes errors by using a trace capability. Trace information is captured in a file in the controller which the system administrator can browse. Information is displayed or stored for ALSAL, ARTS, or TLC modules. Information can also be displayed or stored for all modules.

Use this command with the **-show** option to display the event log captured by the system for one or all of the modules.

Use this command with the **-save** option to store the event log captured by the system for one or all of the modules. Information is saved to a file named `EVENTLOG_timestamp`. A maximum of three files remains in the system. If you issue **-save** when three files exist in the system, the oldest file is deleted before the new one can be saved. You can retrieve the deleted file with a *getFile* mechanism defined and implemented in external software by using the *gSoap* protocol. You can also retrieve other dump information, such as **cdump** and **controller log**, in the same way.

Command arguments:

```
<CLI> event log [-show [all|arts|alsal|tlc] | -save [all|arts|alsal|tlc] ]
```

Where:

- `[all|arts|alsal|tlc]` - Allows selection of all modules or one module.

Examples:

```
<CLI> event log -show all
.. .. .
```

```
<CLI> event log -save arts
Traces saved to file named EVENTLOG_03312008123456.trace
```

locate

The **locate** command illuminates the information LEDs on the drives corresponding to the objects you select.

Command argument:

```
<CLI> locate
```

```
Please select one of this options
Usage : [ -off | -getobject | -setobject ]
```

```
COMMAND-HELP: locate object
```

```
This command lights up the LED on the drives corresponding to the objects selected
Usage : locate [ -off ] | [ -getobject -[drive | pool | volume | ctrl | bbu | enclosure ] ] |
        [-setobject [ -drive [ slot | all ] | -pool poolname | -volume poolname:volumename |
        -ctrl [0|1] | -bbu [0|1] | -enclosure [0|1|2] | -number objectnumber] ]
```

This command lights up the LED on the drives corresponding to the objects selected.
If only drive object is selected,

```
[-setobject] : This command lights up the LED on the selected objects.
                If the selected object is a drive, the LED on that drive is lit up. If the
                selected object is a pool or a volume, LEDs on all the drives making up that
```


object light up. The object can be specified using either the name or sequence number in the list returned by '-getobject' command.

[**-getobject**] : This command with '-getobject' option is used to get a list of all the objects of that type.

[**-off**] : Turns off the LEDs on all components

Examples:

```
<CLI> locate -setobject -pool group1
```

```
<CLI> locate -setobject -drive 1:1
```

```
<CLI> locate -setobject -bbu 0
```

```
<CLI> locate -setobject -ctrlr 1
```

```
<CLI> locate -setobject -enc1 0
```

```
<CLI> locate -setobject -volume pool1:volume1
```

```
<CLI> locate -setobject -drive all
```

```
<CLI> locate -getobject -volume
```

```
<CLI> locate -setobject -number 2
```

The **locate** command lights up the LED on these objects:

- drive
- pool
- volume
- controller
- bbu
- enclosure

If any of the objects are not supplied, this error returns: cannot find object, name is ambiguous

Use the **-off** option to turn off the LEDs on all objects.

Use the **-getobject** option to list all of a specified object. Specify the object by using either the *identifier* of that object or the *sequence number* in the list returned by the **-getobject** option.

Use the **-drive** option to specify the selected object as a drive and to locate a drive. If the selected object is a drive, the LED on that drive is lit up.

Use the **-pool** option to specify the selected object as a pool and to locate a pool by its name. If the selected object is a pool, the LEDs on all the drives making up that pool are lit up.

Use the **-volume** option to specify the selected object as a volume and to locate drives that belong to a volume by its name. If the selected object is a volume, the LEDs on all the drives making up that volume are lit up.

Use **-bbu**, **-controller**, and **-enclosure** options to identify these objects by their number.

Use the **-setobject** option to turn on the LEDs of the drives indicated by the objects. You can issue the **-setobject** option with the **-number** option to clear a

local list of objects. If you issue the `-setobject` option with the `-number` option while the list is empty, an error generates.

Use the `-number` option only after you have issued the `-getobject` option, which builds a local list of objects.

Command arguments:

```
<CLI> locate [ -off ] | [ -getobject -[drive | pool | volume | ctrl | bbu | enclosure ] ] |
[-setobject [ -drive [ E:T | all ] | -pool poolname | -volume pool:volume | -ctrl [0|1] |
-bbu [0|1] | -tray traylocation | -enclosure [0|1|2] | -number object ] ]
```

Where:

- `[E:T|all]` - Locates a specific drive by name when issued with `-drive E:T`.
Locates all drives when issued with `-drive all`.
- `poolname` - Locates a pool by its name when issued with `-pool poolname`.
- `pool:volume` - Locates drives belonging to a volume by its name when issued with `-volume pool:volume`.
- `[0|1]` - Locates a controller and Battery Backup Unit by their number.
- `[0|1|2]` - Locates a enclosure by its number.
- `object` - Allows selection of the number displayed in the list output.

Examples:

```
<CLI> locate -off
<CLI> locate -getobject -volume
```

vol#	VolumeName	Cap	RaidType	Status
0	pool1:vol1	4GB	0	Viable
1	pool1:vol2	2GB	0	Viable

```
<CLI> locate -setobject -pool group1
<CLI> locate -setobject -drive 0:6
<CLI> locate -setobject -bbu 0
<CLI> locate -setobject -ctrl 1
<CLI> locate -setobject -enclosure 0
<CLI> locate -setobject -volume pool1:volume1
<CLI> locate -setobject -drive all
```

```
<CLI> locate -setobject -pool group1
<CLI> locate -setobject -drive 0:6
<CLI> locate -setobject -bbu 0
<CLI> locate -setobject -ctrl 1
<CLI> locate -setobject -enclosure 0
<CLI> locate -setobject -volume pool1:volume1
<CLI> locate -setobject -drive all
```

```
<CLI> locate -getobject -volume
```

Vol#	VolName#	GrpName#	Capacity#	HostLUN#	Host-WWN
0	testVol0	Grp1	1024	0	23abcd
1	testVol1	Grp2	3590	0	abdef3

```
<CLI> locate -setobject -number 2
```

list features

Use this command to display currently enabled feature fields.

Command arguments:

<CLI> list features

Example:

<CLI> list features
Current Machine Local Time: 08/26/2008 03:25:34 PM

S.No	Features	Availability
0	Base Features	Enabled
1	Bound Mode	Enabled
2	Volume Copy	Disabled
3	Snapshot Copy	Disabled
4	Max Drives Supported	12
5	Max Hosts Supported	6

mountstate

Use this command to query the mount states of drives, pools, batteries, media trays, and enclosures (Disk Storage Modules) in the system.

Command arguments:

<CLI> mountstate

Please select one of the options : [-getobject | -setobject]

COMMAND-HELP : mountstate

This command is used to set and query the mount states of drives, pools, batteries, media trays and enclosures in the system

Usage : mountstate [-getobject -[drive |pool |mediatray |enclosure |bbu] | -setobject -[mount [-drive <E:T> <E:T> ... > [-skipspeed] | -bbu [0|1]

| -mediatray 0 | -enclosure < <num> <num> ...>] | dismount [-drive <E:T> <E:T> ... > | -pool < <poolname> <poolname>...> | -bbu [0|1] | -mediatray 0 | -enclosure < <num> <num>> [-okdegraded]]]]

-getobject : This option is used to query the mount state of the selected object.

-setobject : This option is used to set the mount state of the selected object.

If '-okdegraded' option is not specified while dismounting an enclosure which may result in degraded groups, the command would fail.

If '-skipspeed' option is specified while mounting a dismounted drive which is NQ due to speed criteria, then the drive will be mounted

Where:

- *-getobject* queries the mount state of the selected object
- *-setobject* set the mount state of the selected object

The mount or dismount state of a component tells you if that component is available or unavailable. When querying a system component, some -get options are available but it is important to keep note of the following:

- When pool is the selected object, you can set the -oknonviable option while mounting a nonviable pool.
- If the -reportonly option is specified while dismounting an enclosure, only the affected LUNs are reported without actually dismounting the enclosures.

- If you do not specify the `-okdegraded` option while dismounting an enclosure that might result in degraded groups, the command will fail.

Examples:

```
<CLI> mountstate -getobject -drive
```

Drive#	E:T	State
0	1:4	Online
1	2:3	Online
2	1:6	Online
3	1:2	Online
4	1:1	Online
5	2:6	Online
6	2:2	Online
7	2:4	Online
8	1:3	Online
9	2:5	Online
10	2:1	Online

```
<CLI> mountstate -getobject -mediatray
No trays reported
```

```
<CLI> mountstate -getobject -enclosure
```

Enclosure#	State
0	Online
1	Online
2	Online

```
<CLI> mountstate -getobject -bbu
```

CtlrId#	Battery State
Ctlr 0	Service
Ctlr 1	Service

```
<CLI> mountstate -setobject -dismount -drive 1:1
```

```
<CLI> mountstate -setobject -mount -drive 1:1
```

Note: If a pool has been dismounted, is offline, or in service mode, mounting one or more of the drives will not restore the pool. A dual controller reboot is required to bring the pool back online.

```
<CLI> mountstate -setobject -dismount -pool my_pool
```

Note: Once a pool is dismounted, the pool can not be mounted using the `mountstate -setobject` command. A dual controller reboot is required to bring the pool back online.

```
<CLI> mountstate -setobject -dismount -bbu 1
```

```
<CLI> mountstate -setobject -mount -bbu 1
```

```
<CLI> mountstate -setobject -dismount -mediatray 0
```

```
<CLI> mountstate -setobject -mount -mediatray 0
```

```
<CLI> mountstate -setobject -dismount -enclosure 2
```

Note: If dismounting an enclosure causes a pool to become degraded, this command will fail, unless the `-okdegraded` option is also provided.

```
<CLI> mountstate -setobject -mount -enclosure 2
```

Note: If a pool is completely contained in the enclosure, all drives of the pool are located in the enclosure to be mounted. The pool will not be automatically mounted. A system reboot, both controllers rebooted at the same time, is required to bring the pool online.

post result

The **post result** command shows the result of **post**.

Command arguments:

```
<CLI> post result
```

Example:

```
<CLI> post result
All tests passed for ctrlr 0.
All tests passed for ctrlr 1.
```

service mode

The **service mode** command displays the cause and recovery information when a RAID controller is in service mode.

Some situations and system conditions require you to place the RAID Controller in an offline condition to facilitate a system repair or preserve customer data integrity. You can use the RAID Controller command line interface to put the RAID Controller in a state associated with an offline condition, but remaining active on a level that allows you to continue an interaction. This state is known as *service mode*. A service mode shutdown initiates the orderly shutdown sequence but does not execute the power off phase.

The **service mode** command transitions a controller to service mode when various conditions listed in the following table occur. The controller returns to normal mode after a system administrator or service technician issues one of the controller actions.

Table 6. Service mode conditions

Reason	Description	Controller action
SES_FAILURE	Controller is unable to communicate with SES device	Service Mode - Reboot or Replace
BMC_FAILURE	Controller is unable to communicate with BMC device	Service Mode - Reboot or Replace

Table 6. Service mode conditions (continued)

Reason	Description	Controller action
VPD_NOACCESS	Controller is unable to access VPD data	Service Mode - Reboot or Replace
HW_FAILURE	Unrecoverable hardware error	Service Mode - Reboot or Replace
HW_RECURRING_FAILURE	Recoverable hardware error has caused multiple reboots	Service Mode - Reboot or Replace
SW_RECURRING_FAILURE	Firmware detected error has caused multiple reboots	Service Mode - Reboot or Replace
FORCED_NON_SURVIVOR	Failover condition occurred and other controller was better qualified to become survivor.	Service Mode - Reboot or Replace Error log shows controller, drive, and SES data on which basis a survivor was chosen. (Includes mirror path down, tie breaker cases, host port down, etc.)
DRV_MSMTCH_RB	Rebinder does not see the same drives as survivor.	Service Mode - Reboot or Replace
DRV_MSMTCH_ST	On boot up (warm or cold) both controllers discover a different set of drives and neither controller's discovered drives is a superset of the other's.	Service Mode - Reboot or Replace (Note that both controllers will be in service mode.)
SES_ERRS	The controller detected environmental conditions unsuitable for normal operation.	Service Mode - Reboot after environmentals return to normal
INDETERMINATE_DATA_LOSS	Controller is unable to proceed with out loosing data - PROCEED AT OWN RISK	Service Mode - Reboot, Replace, or Force boot with data loss
BATTERY_LOW, BATTERY_FAILED	If "Writeback mode without battery" is false, enter service mode, else report error in log and continue normally	Service Mode - Reboot when battery OK

Command arguments:

```
<CLI> service mode -getreason
Reason details : string
Recovery Hints : string
```

Where:

- *-getreason* lists any appropriate recovery options.

Example:

```
<CLI> service mode -getreason
Current Machine Local Time: 08/26/2008 03:35:15 PM
```

```
The reason for service mode is "DRV_MISMATCH_RB".
Reason details : "Rebinder does not see the same drives as survivor."
Recovery Hints : "Reboot or Replace the controller"
```

shellscrip

The **shellscrip** command runs a shell script in the RAID controller.

Command arguments:

```
<CLI> shellscrip -file name [-param "ANYSTRING"]
```

Where:

- *-file* is a required parameter that specifies the file to be run.
- *-param* is an optional parameter that is passed to the shell script. *ANYSTRING* must be enclosed in quotation marks, and can contain any printable characters. If the *-param* option is not specified, RAID Controller CLI passes a null string as a parameter to the shell script.

Example:

```
<cli> shellscrip -file somefile.ext
```

show raid levels

The **show raid levels** command displays the list of currently supported raid levels in the system.

Command arguments:

```
<CLI> show raid levels
```

Example:

```
<CLI> show raid levels
Following Raid Levels are supported by the system:
RAID 0
RAID 5
RAID 1
RAID 10
```

shutdown

The **shutdown** command changes the operational state of one or both RAID Controllers.

You can specify these RAID Controller states:

Servicemode

A mode where all processes except command processes are stopped.

Reboot

A mode where all processes are stopped and then started again.

Online

A mode where all processes are active.

This command is used to shutdown RAID Controllers singularly or together. You can specify if the controllers being shutdown enter service mode during the shutdown process.

Note: If the controller to which you have your RAID Controller command line interface session connected is shut down, the CLI session ends. However, if only one controller is selected for servicemode, an optional switch `-ensuresurvivor` can be issued to ensure that the process does not result in non-availability.

With the servicemode option, `-ensuresurvivor` and `-readytoremove` options have to be selected together. `-readytoremove` option illuminates the service LED. A controller in service mode can be brought online by issuing this command with `-state online` option to the active controller.

Command arguments:

```
<CLI> shutdown [-ctrl 0| ctrl 1]-state [servicemode [-readytoremove] [-ensuresurvivor]
| reboot | online]] | [-system -state [servicemode |reboot]]
```

Where:

- `[servicemode|reboot|online]` - Allows selection of the state of the controller.

Example of the shutdown command with the -help option:

```
<CLI> shutdown -help
```

COMMAND-HELP: shutdown

```
Usage          : shutdown -ctrl [0|1] -state [servicemode [-readytoremove -ensuresurvivor]|
                  reboot |online ] | -system -state [servicemode |reboot]
```

This command is used to shutdown either or both the controllers. The user can specify whether the controllers being shutdown enter service mode or shut off their power. If only one controller is selected for servicemode, an optional switch 'ensuresurvivor' can be passed to ensure that it will not result in non-availability. With the servicemode option, ensuresurvivor and readytoremove options have to be selected together. The 'readytoremove' option enables the service LED to be turned on. A powered off controller can be powered on by issuing this command with '-state online' option to the active controller. If the controller to which this CLI session is connected to is being requested to be powered off, the user will lose the CLI session.

swversion

The **swversion** command retrieves and displays the software version.

Command arguments:

```
<CLI> swversion
```

Example:

```
<CLI> swversion
```

Current Machine Local Time: 11/27/2009 11:27:09 PM

Software version	:	H-2.0.2.6	
UBoot version	:	H-1.1.4.5	
OS version	:	H-2.4.20.11	
SES version	:	0105	
BMC version	:	S0BT07c	011A 06/30/2009
FPGA version	:	01.06	
CPLD version	:	S0CP00A	C00A 01/01/2000
SAS switch version	:	S0SW01D	R105 6/8/2009
BBU FirmwareRev	:	53.0	
Package Build No	:	1.2.0.041	

time

The **time** command sets and returns the date and time. It is issued by the system administrator for timestamps in the system, such as logs, alerts, volume creation time, and flashcopy name suffixes. The Linux operating system time is set in the factory and cannot be changed. This factory set Linux time is used for various purposes, such as scheduling tasks and monitoring. A delta is stored from the Linux time in the local flash to remember the changed time.

Command arguments:

```
<CLI> time [-get | set -date mm/dd/yyyy -time hh:mm:ss -[am|pm] ]
```

Where:

- *mm* - Displays the month.
- *dd* - Displays the day.
- *yyyy* - Displays the year.
- *hh* - Displays the hour.
- *mm* - Displays the minutes.
- *ss* - Displays the seconds.

Examples:

```
<CLI> time -set -date mm/dd/yyyy -time hh:mm:ss -am|pm  
Time set to mm/dd/yyyy hh:mm:ss am
```

```
<CLI> time -get  
Current time is mm/dd/yyyy hh:mm:ss am
```

validate key

The **validate key** command sets or displays the license key in the system.

Command arguments:

```
<CLI> validate key [-get | -set <192_bit_key>]
```

Where:

- *-get* - Displays the current license key.
- *-set* - Sets a new 192-bit license key.

Example setting the key:

```
<cli> validate key -set 3a288d5ec2cef28c61510c11f6c64a69afae7e678f6c216f  
Current Machine Local Time: 08/26/2008 03:24:43 PM
```

```
License Key 3a288d5ec2cef28c61510c11f6c64a69afae7e678f6c216f has been set successfully
```

Example getting the current key:

```
<cli> validate key -get  
Current Machine Local Time: 08/26/2008 03:24:43 PM
```

```
License Key : 3a288d5ec2cef28c61510c11f6c64a69afae7e678f6c216f
```

Volume management commands

Use the RAID Controller command line interface for the RAID controller to perform administrative tasks for the device. This topic details the commands you can use to manage your storage volumes.

add mirror

Use this command to add a mirror to an existing drive pool. Mirrors can only be added to a RAID 0 pool. Drives must be added in pairs and must not have a smaller capacity than the existing drives in the RAID 0 pool.

Important: This command requires you to end all application I/O processes and shut down any active Blade servers in accordance with the recommended non-concurrent practices. The add mirror command must complete before you resume any application I/O processes. Depending on the size of the drives, add mirror may take several hours to complete. If one of the Blade servers being shut down is used as the RAID controller management node and has logical unit numbers (LUNs) mapped to it, you must use an external Blade server to manage the RAID subsystem.

Command arguments:

```
<CLI> add mirror -pool [POOL_NAME] -drives [ENCLOSURE]:[TRAY][ENCLOSURE]:[TRAY]..
```

Where:

- *[POOL_NAME]* - Specifies the name of the drive pool.
- *[ENCLOSURE]:[TRAY]* - Specifies the drive bay number by enclosure number and tray number.

Example:

```
<CLI> add mirror -pool Grp1 -drives 1:1 1:3
```

assimilate drive

Use this command with foreign drives, which are drives that were written on another system using the controller software or a system using another vendor's software. By running this command with the -set option, you can record the information pertinent to this controller in the drive region reserved for metadata.

Important: This command produces a destructive procedure causing complete data loss. Use this command only if your intention is to irrevocably erase all disk data.

Command arguments:

```
<CLI> assimilate drive
Please select one of the options: [-get |-set [-slot|-number]]
```

Where:

- *E:T* - Specifies the drive bay number by enclosure number and tray number.
- *number* - Specifies the drive bay number by the sequence number that appears on list displayed when command is run with -get option.

When you run this command with the -get option, a list of all foreign drives is displayed.

Example:

```
<CLI> assimilate drive -get
```

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Ct10	Ct11	RPM
0	2:3	J3YWKGSJ	33GB	D1	CLS	OK	1	1	0

When you run the assimilate drive command with the -set option, the drive is assimilated and becomes available. Specify the drive by bay position or number. When you specify the drive by a number, that number refers to the sequence number that appears on the list displayed on running this command with the -get option. Run this command with the -get option just before running it with the -set option to make an internal reference list. An error message is displayed if you run the assimilate drive command with the -set option without first running it with the -get option. The list is cleared after you run the command with the -set option.

Example:

```
<CLI> assimilate drive -set -slot 2
Drive in Enclosure 2 has been assimilated.
```

```
<CLI> assimilate drive -get
```

Drive#	Enclosure	SerialNo	Cap	Pool	Usage	State	Ct10	Ct11	RPM
0	2	J3YWKGSJ	33GB	D1	CLS	OK	1	1	0

```
<CLI> assimilate drive -set -number 0
Drive is Enclosure 2.
```

copyback

Use this command to copy the data from the source drive to the destination drive. This command can be used to drain a drive or to copy the data from the spare drive to the replaced drive.

Note: For any pool, only one copyback operation is active at a time. A new copyback request will be rejected if a copyback operation is already running in the group.

Command arguments:

```
<CLI> copyback
copyback -source<E:T>-dest<E:T>[-convert]
```

Where:

- *E:T* - [Enclosure]:[Tray] Specifies the drive bay number by enclosure number and tray number.
- *-source* - Specifies the source drive where the data being copied from.
- *-dest* - Specifies the destination drive where the data being copied to.
- *-convert* - Specifies the conversion of the source drive to a global spare when the copyback operation finished.

Example:

```
<CLI> copyback -source 2:6 -dest 1:1
Source drive 2:6
Destination drive 1:1
```

Copyback operation started successfully.

create pool

This command creates a drive pool using drives specified by their bay numbers. The -help option provides more details regarding proper configuration of drives in particular RAID levels.

This command creates a drive pool using drives specified by their bay numbers. The -help option provides more details regarding proper configuration of drives in particular RAID levels.

Example of the create pool command with the -help option

```
<CLI> create pool -help
```

```
COMMAND-HELP: create pool
```

This command is used to create drive groups.

```
Usage : create pool -drives [DRIVE][DRIVE].. -raidtype [RAID_LEVEL] -port [PORT]
       -name [POOL_NAME]
```

```
DRIVE : [ENCLOSURE]:[TRAY] format for one drive.
```

```
RAID_LEVEL : Possible RAID_LEVEL values are '0','1','5','10'.
```

```
0 - RAID 0, 1 - RAID 1, 5 - RAID 5, 10 - RAID 10
```

```
RAID 5 - For RAID 5 configuration, specify at least 3 drives
```

```
RAID 10 - For RAID 1+0 configuration, the number of drives specified should
         be a multiple of 2
```

```
RAID 1 - For RAID 1 configuration, the number of drives specified should
         be 2
```

```
PORT : Port value can be either '0' or '1'.
```

```
POOL_NAME : Pass a unique name for this Drive Pool
```

```
Pool name is maximum of 12 characters and contains only alphanumeric and
underscores.
```

Where:

- *[ENCLOSURE]:[TRAY]* - Specifies the drive bay number by enclosure number and tray number.
- *[0|1|10|5]* - Allows selection of raid type.
- *[0|1]* - Allows selection of port.
- *[POOL_NAME]* - Defines the name of the pool.

A drive pool is a defined set of drives. Each volume that is exposed to host systems is completely contained within a drive pool. It is important to note that a drive can only be a member of one drive pool.

This command creates a pool using drives specified by their bay numbers. You can specify the -raidtype and the owner controller bay number. The pool name can be a maximum of 12 characters long and can contain alphanumeric and underscores. Make the pool name unique across the system.

Example:

```
<CLI> create pool -drives 1:4 1:1 1:3 -raidtype 10 -port 0 -name Group10
```

Drive Group created with total capacity of 46 GB.

create volume

This command creates a volume of a specified size on a particular pool.

Command arguments:

```
<CLI> create volume -name poolname:volumename -size number
[%|MB|GB] -seqpostreadcmdsize size -seqreadaheadmargin margin
```

Where:

- *poolname:volumename* - Specifies pool name and volume name. Volume name can be up to 12 characters long and contain alphanumeric and underscores; it must be unique across pool on which it is created.
- *number* - Number indicating size of the pool.
- [%|MB|GB] - Allows you to specify size in percentage of total pool capacity, MB, or GB.
- *size* - Specifies maximum sector count of a single predictive read ahead.
- *margin* - Indicates number of sectors in the read ahead buffer.
-

create volume -help

```
<CLI> create volume
```

Too many/few parameters for -name option

COMMAND-HELP: create volume

This command is used to create a volume.

```
Usage : create volume -name [POOLNAME]:[VOLUMENAME] -size [SIZE][UNIT]
        [-seqpostreadcmdsize [READCMD_SIZE] -seqreadaheadmargin [MARGIN] ]
```

POOLNAME : Pool's name on which the volume is going to be created

VOLUMENAME : Volume's name to create. It has to be associated with poolname as a pool:volume pair. Volume name is maximum of 12 characters and contains only alphanumeric and underscores.

SIZE : Size may be passed in different units.

If % is used, then SIZE value should not be more than '100%' .

If MB or GB is used, then it should not be more than available size of Drive Group. e.g. if available size of Drive Group(DRIVEGRPNAME) is 2346MB it should be less than or equal to '2346MB' or '2GB'. The SIZE specified should be whole numbers i.e. 236.54MB is not a valid number.

UNIT : Unit of the size can be GB or MB or %

READCMD_SIZE : Sequential Post Read Command Size is the maximum sector count of a single predictive read ahead. A value of 0 disables predictive read for this volume. A value of 1-128 will override the previous setting and represents a command transfer size that is a multiple of 16Kbytes. A value of (0xFFFF) will cause the default value to be used.

MARGIN : Read Ahead Margin is the number of sectors in the read ahead buffer. This parameter is ignored if the Sequential Post Read Command Size is zero. The valid range is 1 to 0x7FFF. A value of (0xFFFF) results in the default value being used.

In other words, specify size in MB, GB or percentage of the total pool capacity.

Specify the name as *poolname:volumename*. The volume name can be a maximum of 12 characters long and can contain alphanumeric and underscores. Make the volume name unique across the pool on which it is being created. The maximum sector count of a single predictive read ahead is seqpostreadcmdsize. A value of 0 disables predictive read for this volume. A value of 1-128 overrides the previous setting and represents a command transfer size that is a multiple of 16Kb. A value of (0xFFFF) causes the default value to be used. The number of sectors in the read

ahead buffer is seqreadaheadmargin. This parameter is ignored if the seqpostreadcmdsiz is zero. The valid range is 1 to 0x7FFF. A value of (0xFFFF) results in the default value.

Example:

```
<CLI> create volume -name Grp1:volume1 -size 10 %  
Volume 'volume1' created on pool 'Grp1' with capacity 15 GB.
```

delete pool

This command deletes a drive pool.

Command arguments:

```
<CLI> delete pool -name poolName
```

Where:

- *poolName* - Specifies name of pool to be deleted.

When you issue this command, the following warning is appears:

Example:

```
<CLI> delete pool -name Group0
```

```
All volumes in this Pool and hostluns mapped to them will be  
unavailable (deleted). The data for these volumes will be deleted.  
Do you want to continue? Type L to delete or any other key to cancel.  
L  
Pool Group0 has been deleted.
```

An error message is displayed if the target pool is not found.

Example:

```
<CLI> delete pool -name Group0  
No such drive pool  
Please re-execute the command with valid pool name available
```

delete volume

This command deletes a master volume.

Command arguments:

```
<CLI> delete volume -name poolname:volumename
```

Where:

- *poolname:volumename* - Specifies pool name and volume name. Volume name can be up to 12 characters long and contain alphanumeric and underscores; it must be unique across the pool on which it is created.

When you issue the delete volume command, the following warning appears:

Example:

```
<CLI> delete volume -name raid1:vol88  
All hostluns mapped to this volume will be unavailable (deleted).  
The data for this volumes will be deleted. Do you want to continue?  
Type 'L' to delete or any other key to cancel.  
L  
Volume vol88 on pool raid1 has been deleted
```

global spare

Use this command to manage global spares. Global spares are drives that can be used to rebuild a degraded pool that has no local spares.

Command arguments:

```
<CLI> global spare -[add -slot E:T | get | delete  
-[slot E:T |number number]]
```

Where:

- *E:T* - Specifies the drive bay number by enclosure number and drive position.
- *number* - Specifies the drive bay number by the sequence number that appears on list displayed when command is run with -get option.

You can use a drive from the global spares to rebuild a degraded pool that has no local spares, but can only add global spares to the global spare pool if their state is unassigned. Run the **list drive** command defined earlier to obtain a list of unassigned drives. If a drive being deleted from the global spare pool has already been chosen for a rebuild, it will produce an error.

Running the global spare command with the -get option returns a list of all the global spares in the system.

Example:

```
<CLI> global spare -get
```

Drive#	Slot	SerialNo	Cap	Pool	Usage	State	Ct10	Ct11	RPM
1	1:5	3LM269P3	279GB	--	GLS	online	1	1	0

Running this command with the -add option adds a global spare.

Example:

```
<CLI> global spare -add -slot 1:5  
Global spare added
```

Running the global spare command with the -delete option deletes a global spare. Specify the drive by bay position or number. When you specify the drive by a number, that number refers to the sequence number that appears on the list displayed on running this command with the -get option. Run this command with the -get option just before running it with the -delete number option to make an internal reference list. An error message is displayed if you run the global spare command with the -delete option without first running it with the -get option.

Example:

```
<CLI> global spare -delete -slot 1  
Global spare deleted from Controller Enclosure 1.
```

```
<CLI> global spare -get
```

Drive#	Enclosure	SerialNo	Cap	Pool	Usage	State	Ct10	Ct11	RPM
0	2	J3YWKGSJ	33GB	--	GLS	OK	1	1	0
1	1	J3YXDVJJ	33GB	--	GLS	OK	1	1	0
2	1	JBV1HE7J	33GB	--	GLS	OK	1	1	0

```
<CLI> global spare -delete -number 2  
Global spare deleted from Controller Enclosure 1.
```

host

Use this command to add a host World Wide Name (WWN) to the controller list of hosts or to get the list of hosts added to the controller .

Command arguments:

<CLI>host -[add WWN| get]

Where:

- *WWN* - Specifies host WWN to add to controller list of hosts or host WWN for which logical unit numbers (LUNs) will be mapped.

Examples:

```
<CLI> host -add 1234567890abcdef
Host added with WWN 1234567890abcdef.
```

```
<CLI> host -get
HostWWN 784875485454 : LUNs Mapped
```

LUN	Permission	Volume
3	ACCESS_READWRITE	pool1:vol1

```
HostWWN 1234567890abcdef0 : No LUNs Mapped
HostWWN 1234567890abcdef1 : No LUNs Mapped
```

hostlun

Use this command to map or unmap a volume to a host using the specified LUN number or to get a list of all host LUNs.

Important: When using this command with the -unmap argument to unmap a volume to a host, the command requires you to end all application I/O processes on the LUN that is being unmapped and to shut down any active Blade servers in accordance with the recommended non-concurrent practices.

Command arguments:

```
<CLI> hostlun -[get -wwn WWN | map -volume poolname:volumeName -permission
[ro/rw] -wwn WWN -lun number | unmap -wwn WWN -lun number]
CLI> host
Please select one of the below options
Usage : [ -add | -delete | -get ]
```

```
COMMAND-HELP: host
Usage          : host -[get |delete WWN | add WWN]
This command is used to add/delete a host WWN to/from the controller list of hosts or get
the list of hosts added to the controller.
WWN           : The WWN name of the host (16 hexadecimal digits).
```

Where:

- *WWN* - Specifies host World Wide Name for which LUNs will be mapped or unmapped.
- *poolname:volumeName* - Specifies pool name and volume name. Volume name can be up to 12 characters long and contain alphanumeric and underscores; it must be unique across pool on which it is created.
- *[ro/rw]* - Specifies whether permission is read only or read-write.
- *number* - Specifies LUN number to be mapped or unmapped.

Running the `hostlun` command with the `-map` option maps any volume to any host using the specified LUN number. This command adds the host if it has not already been added. It returns an error message if the specified volume is already mapped to the specified host.

Example:

```
<CLI> hostlun -map -volume Grp1:vol1 -permission RW
-wwn 500062b00008ace9 -lun 6
Host Lun 6 for host 500062b00008ace9 mapped to volume 'vol1' in pool 'Grp1'.
```

Running this command with the `-get` option returns a list of all host LUNs.

Example:

```
<CLI> hostlun -get -wwn 500062b00008ace9

HostWWN 500062b00008ace9 : LUNs Mapped
```

LUN	Permission	Volume
2	ACCESS_READWRITE	raid1_1:vol01
3	ACCESS_READWRITE	raid1_1:vol02
0	ACCESS_READWRITE	raid0_0:vol01
1	ACCESS_READWRITE	raid0_0:vol02
6	ACCESS_READWRITE	raid10_1:vol01
7	ACCESS_READWRITE	raid10_1:vol02
4	ACCESS_READWRITE	raid5_0:vol01
5	ACCESS_READWRITE	raid5_0:vol02

Running this command with the `-unmap` option unmaps the host LUN from a volume.

Example:

```
<CLI> hostlun -unmap -wwn 500062b00008ace9 -lun 4
Lun 4 for host 500062b00008ace9 unmapped.
```

Volume services commands

Use the SAS Switch command line interface for the RAID controller to perform administrative tasks for the device. This topic details commands related to volume services.

add capacity

The **add capacity** command expands the capacity of a drive pool by adding a new unassigned drive or drives to the pool. The number of drives you add to the pool is dependant on the RAID level configured on your system. For RAID levels 1 and 10, you add two drives to the pool at a time. If you are operating a RAID level of 0 or 5, you add one at a time. If the capacity of the new drive is less than the capacity of the smallest drive in the pool, the system generates an error. However, if the capacity of the new drive is more than the capacity of the smallest drive in the pool, the system generates a warning.

Command arguments:

```
<CLI> add capacity -pool name -drivelist <[ENCLOSURE]:[TRAY]>  
<[ENCLOSURE]:[TRAY]> .. <[ENCLOSURE]:[TRAY]>
```

Where:

- *name* - Defines the pool name.
- *[ENCLOSURE]:[TRAY]* - Specifies the drive bay number by enclosure number and drive position (tray) number. You can add one or more drives to the pool.

Example:

```
<CLI> add capacity -pool Group0 -drivelist 1:3  
Capacity added successfully
```

datascrub

The **datascrub** command views or sets the **datascrub** policy.

The -auto flag specifies whether background scrub should be enabled. If a problem is found, the policy to fix it or create bad blocks is defined in the flash configuration file.

Command arguments:

```
<CLI> datascrub -[get | set -auto [on|off]
```

Where:

- *[on|off]* - Enables or disables data scrubbing.

Example:

```
<CLI> datascrub -get  
Data Scrub Policy is off
```

delete all

Important: This command produces a destructive procedure causing complete data loss. Use this command only if your intention is to irrevocably erase all disk data.

The **delete all** command deletes all pools, volumes, and host LUNs in a bound controller system. Use this command to delete an existing configuration before loading a new configuration manually or from a configuration script.

Command arguments:

```
<CLI> delete all
```

Example:

```
<CLI> delete all
All volumes in the system and hostluns mapped to them will be unavailable
(deleted). The data for these volumes will be deleted. Do you want to
continue? Type 'L' to delete or any other key to cancel.
L
Started deleting all...
Delete All Successful
```

expand -volume

Use the **expand -volume** command to expand the capacity of a volume. The new capacity of a volume is equal to the added capacity increment plus the old volume. The incremental capacity can be defined in MB, GB or the percentage (%) of the total remaining drive pool capacity.

Note: If the remaining capacity on the pool is less than the requested expansion, an error occurs.

Command arguments:

```
<CLI> expand -volume poolname:volumename -add capacityIncrement [MB|GB|%]
```

Where:

- *poolname:volumename* - Allows selection of the volume name as a combination of *poolname* and *volumename*.
- *capacityIncrement* - Specifies the number for the incremental capacity.
- *[MB|GB|%]* - Defines incremental capacity in MB, GB, or as % of total remaining drive pool capacity.

Example:

```
<CLI> expand -volume Grp1:vol1 -add 10%
Volume 'vol1' on pool 'Grp1' has been expanded. The new capacity is 34 GB.
```

initialize

The **initialize** command performs a task that overwrites and formats the metadata area on the drive before removing the drive from the system.

Important: This command produces a destructive procedure causing complete data loss. Use this command only if your intention is to irrevocably erase all disk data.

Command arguments:

<CLI> initialize -drive slotnumber

Where:

- *slotnumber* - Specifies the drive bay by enclosure number.

Example:

<CLI> initialize -drive 1:3

list killedpaths

The **list killedpaths** command displays the killed drive paths information from the persistent memory. If both paths to a drive are killed, the drive will not show up in the list drive response.

Command arguments:

<CLI> list killedpaths [-ctlr [0|1]]

Where:

- *-ctlr* specifies the path to act on. The default is both the *ctlr 0* and *ctlr 1* paths.

Example:

<cli> list killedpaths [-ctlr [0|1]]

Current Machine Local Time: 08/26/2008 03:20:14 PM

E:T:S	DriveDN	Word-Wide Node Name	Word-Wide Port Name
1:2:0	3:5000c5000a832023	5000c5000a832021	5000c5000a832021
1:4:0	3:500000e0177202d0	500000e0177202d2	500000e0177202d2
1:3:0	3:5000c5000a83b72f	5000c5000a83b72d	5000c5000a83b72d
1:2:0	3:5000c5000a832023	5000c5000a832022	5000c5000a832022
1:4:0	3:500000e0177202d0	500000e0177202d3	500000e0177202d3
1:3:0	3:5000c5000a83b72f	5000c5000a83b72e	5000c5000a83b72e

synchronize volume

The **synchronize volume** command synchronizes a volume immediately to ensure that redundant information is valid. You can also use this command to perform a parity check on RAID 5 volumes and a mirror consistency check on mirrored volumes. Any errors found during the check are handled according to the defined **datascrub** policy found in the flash configuration file. The progress of **datascrub** is shown along with other volume services.

If the background **datascrub** is enabled (**datascrub** is disabled by default) and running when you issue **synchronize volume**, the background task enters into a suspended state. After **synchronize volume** finishes, the background task automatically resumes. The status of **synchronize volume** reports, but the status of the background task does not report.

Command arguments:

```
<CLI> synchronize volume [-name pool[:volume]]
```

Where:

- *pool[:volume]* - Defines the pool name, the volume name, or the pool name and volume name.

If the pool name is not specified, all the volumes in the system will be synchronized. If the pool name is specified and the volume name is not specified, all the volumes in that pool will be synchronized.

Example: none

view long running tasks

The **view long running tasks** command displays all of the long running tasks that have been initiated and their status. The following long running tasks can have their status displayed:

- *Volume based tasks:*
 - initialize
 - synchronize volume
- *System level tasks:*
 - synchronize volume
- *Pool based tasks:*
 - synchronize volume
 - addmirror
 - addcapacity

Command arguments:

```
<CLI> view long running tasks
```

Example:

```
<CLI> view long running tasks
```

Status of long running tasks:

Volume based tasks:

Pool name	Volume name	Task name	% complete	Status
Group0	vol1	migrate	80%	running
Grp1	volume12	init	50%	running

Grp1	Volume1	init	0%	scheduled
Group based tasks:				
Pool name	Task name	% complete	Status	Tray
Grp2	Rebuild	30%	running	1:2
Group34	AddMirror	24%	running	N/A
System tasks:				
Task name		% complete	Status	
Synchronize volume		80%	running	

Using the command line to configure storage

The recommend method of configuring storage is the IBM Storage Configuration Manager, but storage configuration can also be done using the RAID Controller command line interface.

Example of a RAID 5 configuration

About this task

The following shows an example the commands used to create a RAID 5 configuration.

Procedure

- Before you begin, ensure that all of your drives are in an unassigned and online state.
- Run the **list drive** command
list drive
- Issue the commands to create your pools and a global spare (GLS)
create pool -drives 1:1 1:2 1:3 -raidtype 5 -port 0 -name A1R5
create pool -drives 2:1 2:2 2:3 2:4 2:5 -raidtype 5 -port 1 -name A2R5
global spare -add -slot 2:6
- Verify pools and global spare
list pool
list drive
- Create your volumes
create volume -name A1R5:V1 -size 1GB
create volume -name A1R5:V2 -size 1GB.
create volume -name A2R5:V1 -size 4GB
create volume -name A2R5:V2 -size 4GB
- Verify your volumes
list volume
- Map the volumes to hosts
hostlun -map -volume A1R5:V1 -permission rw -wwn 500062B000030D4C -lun 0
hostlun -map -volume A1R5:V1 -permission rw -wwn 500062B000030D4D -lun 0
hostlun -map -volume A1R5:V2 -permission rw -wwn 500062B000030D4C -lun 1
hostlun -map -volume A1R5:V2 -permission rw -wwn 500062B000030D4D -lun 1

hostlun -map -volume A2R5:V1 -permission rw -wwn 500062B00007E0D0 -lun 0
hostlun -map -volume A2R5:V1 -permission rw -wwn 500062B00007E0D1 -lun 0
hostlun -map -volume A2R5:V2 -permission rw -wwn 500062B00007E0D0 -lun 1
hostlun -map -volume A2R5:V2 -permission rw -wwn 500062B00007E0D1 -lun 1
- Verify host mapping

```
host -get
```

Chapter 9. Configuring zones

Zoning for your integrated storage is configured automatically for the IBM BladeCenter S SAS RAID Controller Module.

The IBM BladeCenter S chassis has a default zoning configured allowing all blades to communicate with all disks. In some cases, isolating one or more disks can be useful in problem determination procedures so it is possible to adjust the zoning. It is recommended however, that you maintain the default zoning settings for regular operations.

Note: Zoning for the RAID Controller is set up automatically. Because the RAID Subsystem acts as one unit, altering the zoning disables communication between the storage modules and blade servers.

Understanding the predefined zone

There is only one predefined zone for use with the RAID Controller.

Due to the nature of RAID technology, the default predefined zone used with the IBM BladeCenter S chassis is set so that all the Blade Servers can communicate with all of the disk storage. In the course of troubleshooting, you might want to isolate a Blade Server as a diagnostic tool, but it is recommended that you maintain the default zoning settings for regular operations.

Chapter 10. Attaching an external tape device to the SAS RAID Module

The SAS RAID Module has four 3.0 GB external SAS Ports that you can use to attach an external SAS storage tape device. This chapter describes the installation process for the following supported tape devices:

Table 7. Tape devices supported by the IBM BladeCenter S SAS RAID Controller Module

Supported tape devices
IBM System Storage TS2230 Tape Drive Express Model
IBM System Storage TS2240 Tape Drive Express Model
IBM System Storage TS2340 Tape Drive Express Model
IBM System Storage TS2900 Tape Autoloader Express
IBM System Storage TS3100 Tape Library Express Model

Tape device considerations

To create a successful backup solution using SAS storage tape devices, consider the following:

- The backup software that you use must support the operating environment, including connectivity topologies, tape devices, and operating systems.
- The SAS RAID Module does not support configurations where multiple servers are able to access the same tape device simultaneously. However, this type of configuration may be supported by application software offered from third parties.
- For optimal backup performance, do not mix tape devices with disk storage devices on the same HBA port.
- Use zoning to isolate different types of traffic when you use an SAS connectivity module for both disk and tape operations for different servers. For information on modifying the SAS zoning, see the IBM Storage Configuration Manager online help.
- LAN-free drive sharing is not supported for the SAS-based tape libraries covered in this section. Instead, use dedicated backup servers or LAN-based backup operations.
- The predefined zones that ship with the SAS switch have external ports enabled. Ensure that only one application is accessing the tape device at a time.

Updating firmware prior to connecting a tape device

Before you connect a tape device to your SAS RAID Module, make sure you have the latest firmware updates. Perform the following steps to prepare your IBM BladeCenter S for the installation of the tape device.

1. Update the firmware on the Advanced Management Module to a version that supports the SAS RAID Module.
2. Update the SAS RAID Module firmware to the latest supported version. For detailed instructions, see Chapter 6, “Updating firmware,” on page 31.
3. Ensure you have the latest version of IBM Storage Configuration Manager. For instructions on installing IBM Storage Configuration Manager, see the *IBM Storage Configuration Manager Planning, Installation, and Configuration Guide* at <http://www.ibm.com/support>.

Installing and configuring a tape device

Perform the following steps to connect a tape device to the SAS RAID Module.

1. Make sure that both SAS RAID Modules and the tape device are powered on.
2. Download and install the tape device drivers for the supported operating system platform. For a list of supported tape devices, see the *BladeCenter-S Interoperability Guide* at <http://www.ibm.com/support>.
3. Attach the host end of the SAS interface cable to the SAS connector on the tape device.
4. Attach the other end of the host SAS interface cable to one of the four ports on the SAS RAID Module.
5. Enable the external ports on the SAS RAID Module via the Advanced Management Module.
 - a. Log into the Advanced Management Module.
 - b. Select **I/O Module Tasks > Admin/Power/Restart > I/O Module Advanced Setup**.
 - c. Select **I/O Module 3** from the **Select a Module** menu.
 - d. Select **Enabled** from the **Fast Post** menu.
 - e. Select **Enabled** from the **External ports** menu.
 - f. Click **Save**.
 - g. Repeat these steps for **I/O Module 4**.
6. Verify the tape device is visible to your operating system platform. For information on device management, consult the documentation supplied with your operating system.
7. Verify the tape device is visible to IBM Storage Configuration Manager.
 - a. Log into IBM Storage Configuration Manager.
 - b. Select **BC-S SAS RAID Module > Configuration > SAS Ports**.
 - c. Verify the status of the port to ensure the tape device is visible.
8. If the tape device is not visible after completing these steps, contact IBM support.

For additional information about the supported tape devices, go to <http://www.ibm.com/support>.

Chapter 11. Troubleshooting

This topic contains scenarios and solutions to common RAID Controller troubleshooting issues. To help you understand, isolate, and resolve problems with your RAID Controller, the troubleshooting and support information also contains instructions for using the problem-determination resources that are provided with your IBM products.

You can use the information here to resolve a technical issues on your own, by identifying the source of a problem, gathering diagnostic information, and knowing how to search knowledge bases to get online fixes. If you need to contact IBM Support, you can find out what diagnostic information the service technicians need to help you address your technical issue.

Attention: Back up the data before servicing or replacing components.

Putting the IBM BladeCenter S SAS RAID Controller Module into service mode

service mode

The RAID Controller command line interface includes a **service mode** command that you can use to put the RAID Controller in a state associated with an offline condition, but remaining active on a level that allows you to continue an interaction. For more information on the **service mode** command, see “service mode” on page 77.

For information on using IBM Storage Configuration Manager to a RAID Controller into service mode, see the "Shutdown and Recover" topic in the IBM Storage Configuration Manager online help.

Understanding LEDs

This topic describes what the LED lights on your IBM BladeCenter S SAS RAID Controller Module signify.

Power – OK LED

Power Indicators are used on each component to indicate the status of the power distribution network within that component. A single indicator is utilized to indicate the various power conditions of the component by utilizing the different indicator states to differentiate the different power conditions.

Activity – ACTIVITY LED

Activity LEDs are implemented on various components to provide an indication of the level of utilization of a component. The LED state is internally controlled by the component and will utilize the FLASHING indicator state as internally defined by the component to manage the state of the indicator.

Identify – IDENTIFY LED

A blinking Alert/Fault led can be used to identify a component.

System Information – INFORMATION LED

The IBM BladeCenter S SAS RAID Controller Module system information indicator is used to provide a user notification that the storage system is in a state that requires attention. The system information LED is also used to provide an external indication that the SAS RAID Module storage system has an activity in progress might prevent you from accessing the SAS RAID Module management facilities through the user interfaces.

Alert / Fault – ALERT / FAULT LED

Alert / Fault indicators are used to provide an external indication that a condition has been detected within a component that requires service or repair. Alert / Fault indicators are also be used to identify a particular component and, or indicate that a particular condition is present within a component.

Alert / Fault LED SOLID state

A component Alert / Fault LED that is in a SOLID state indicates externally that there has been a condition detected in the component that requires either service, repair, and or replacement. It also indicates that the component is in a condition or state where it is ready to be removed from the system.

Alert / Fault LED BLINK state

A component Alert / Fault LED that is in a BLINK state indicates that the storage system has identified this component in response to a request. The request can originate from a user interface or as an automated response to a defined set of system conditions.

Note: An LED test occurs whenever the SAS RAID Module is turned on. All LEDs are lit and remain lit for approximately 10 seconds during POST and then return to a normal state.

Table 8. Light path diagnostics LED details

CRU	Indicator Name	Color
IBM BladeCenter S SAS RAID Controller Module	OK	Green
	Activity	Green
	Information	Amber
	Alert/Fault	Amber
	Data In Cache	Green
	iPass Port Activity (1 per Port)	Green
	iPass Port Alert/Fault (1 per Port)	Amber
Disk subsystem	Fault	Amber
Battery Backup Unit	Power	Green
	Battery Charging	Green
	Fault	Amber

SAS RAID Module light path indicators and valid states

System Information LED (Amber)

The SAS RAID Module system information indicator is used by the Light Manager to provide a notification that the storage system is in a state that requires attention. The system information LED is also used by the Light

Manager to provide an external indication that the SAS RAID Module storage system has an activity in progress that might prevent access to the SAS RAID Module management facilities through the user interfaces.

Valid States: OFF, SOLID, SLOW BLINK

OFF – There are no conditions that require attention.

SOLID – The system requires attention that requires you to use the user interface.

SLOW BLINK – The storage system is in a condition where it might not be available through the user interfaces.

Controller Card Fault/Alert LED (Amber)

The SAS RAID Module Controller Fault / Alert LED is used by the Light Manager to indicate the state of the two cards in the SAS RAID Module. The local Baseboard Management Controller is the Light Controller of the SAS RAID Module Card Fault / Alert LED.

Valid States: OFF, SOLID, BLINK

OFF – There have been no faults or conditions detected by either card of the SAS RAID Module that can be serviced using the light path diagnostics indicators. The SAS RAID Module is not in a condition that permits a repair or replacement activity.

SOLID – There has been a fault and or condition detected by the storage system with the SAS RAID Module that can be serviced using the light path diagnostics indicators. The SAS RAID Module is in a condition that permits repair or replacement activity.

BLINK – The SAS RAID Module has been identified in response to a request to identify itself.

Data in Cache LED (Green)

The Data in Cache LED is used by the Battery Backup Unit to indicate that there is data present in the system cache memory.

Valid States: OFF, FLASHING

FLASHING – There is information in system cache memory that must be preserved to ensure customer data integrity. It also indicates that the Battery Backup Unit is providing power to the system memory.

OFF – Indicates that AC power is present or the system cache memory does not contain any information required to ensure customer data integrity.

OK LED (Green)

The OK LED is used by the Light Manager to indicate the power state and or condition of the SAS RAID Module.

Valid States: OFF, SOLID, SLOW BLINK, FAST BLINK

OFF – Power domain two is off or the unit is not operational as determined by boot diagnostics.

SOLID – The SAS RAID Module has been powered on, POST has completed and the SAS RAID Module is fully operational.

SLOW BLINK – Used to indicate POST is running. This indicator also blinks during extended POST.

FAST BLINK – Fast Blink can be preformed only by the Baseboard Management Controller.

SAS RAID Module Activity LED (Green)

The SAS RAID Module Activity LED is used by the SAS RAID Module to indicate that the status of system activity on the storage system.

Valid States: OFF, SOLID, FLASHING

OFF – Indicates main DC power is not present

SOLID – There is no SAS RAID Module storage system activity.

FLASHING – The flash rate of the Activity LED indicates SAS RAID Module a rate proportional to the level of SAS interface (host and/or device) activity as determined by the SAS Bridge Device.

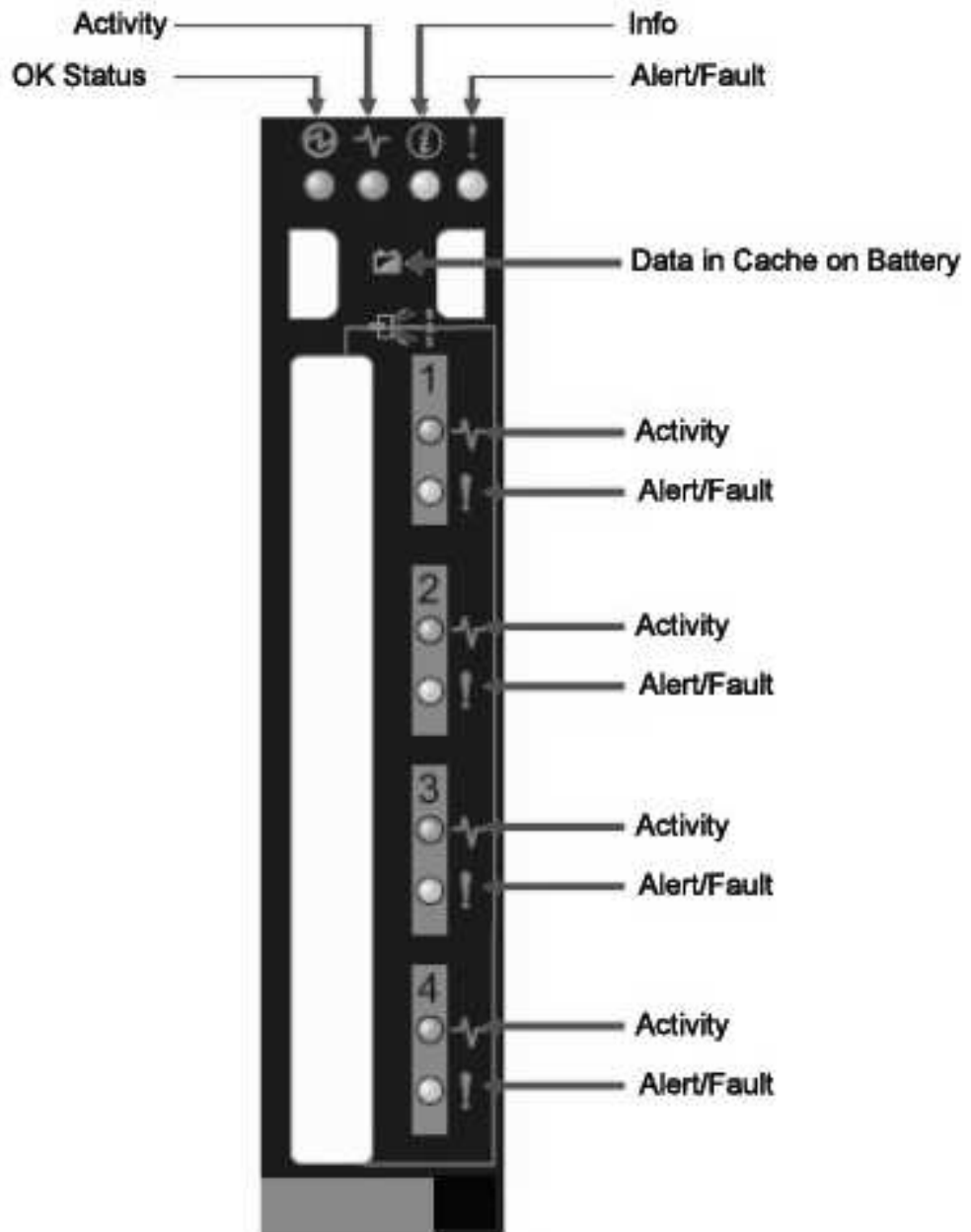


Figure 22. SAS RAID Module light path indicators

Battery backup unit light path indicators and valid states

The SAS RAID Module relies on each battery backup unit to provide power to preserve its respective SAS RAID Module cache memory. Each battery backup unit supports the following light path indicators and valid states.

Battery Backup Unit Charging LED (Green)

The battery backup unit charging indicator provides indication of the charging state.

Valid States: OFF, FLASHING, SOLID

OFF – The DC output is off or out of tolerance.

FLASHING – The battery is in a charging state.

SOLID – The battery is charged to a capacity state that will support battery backup power mode for seventy-two (72) hours.

Battery Backup Unit Fault / Alert LED (Amber)

The battery backup unit fault / alert indicator provides information about the state of the battery.

Valid States: OFF, SOLID, FLASHING, BLINK

OFF – There have been no faults or conditions detected by the SAS RAID Module with the battery that can be serviced using the light path diagnostics indicators. The battery is not in a condition that permits a repair or replacement activity.

FLASHING – There is a battery firmware upgrade in progress.

SOLID – A fault / condition detected by the SAS RAID Module with the battery that can be serviced using the light path diagnostics indicators. The battery is in a condition that permits repair or replacement activity.

BLINK – The battery has been identified in response to a request to identify the battery.

Battery Backup Unit Power LED (Green)

The battery backup unit power indicator provides information about the state of power to the battery.

Valid States: OFF, SOLID

OFF – Standby power is not available to the battery.

SOLID – DC power is applied to battery backup unit.



Figure 23. Battery Backup Unit light path indicators

Disk Storage Module light path indicators and valid states

The Disk Storage Module (DSM) light path indicators describe the state of the DSM.

DSM Fault / Alert LED (Amber)

Each DSM supports the following light path indicators and states.

Valid States: OFF, SOLID, BLINK

OFF – There have been no faults or conditions detected by the SAS RAID Module with the DSM that can be serviced using the light path diagnostics indicators. The DSM is not in a condition that permits a repair/replacement activity.

SOLID – There has been a fault / condition detected by the SAS RAID Module with the DSM that can be serviced using light path diagnostics indicators. The DSM is in a condition that permits repair / replacement activity.

BLINK – The DSM has been identified in response to a request to identify the DSM.



Figure 24. Disk Storage Module (DSM) Light Path Indicators

SAS RAID Module External SAS Port indicators and valid states

There are four SAS RAID Module external port activity LEDs to indicate the status of a SAS port.

SAS RAID Module Activity LED (Green)

Valid States: OFF, SOLID, FLASHING

OFF – There is no activity on this port.

SOLID – Link has been established normally.

FLASHING – Blinks as a result of SAS activity

SAS RAID Module External Port LED (Amber)

There are four SAS RAID Module external port alert LEDs to indicate the state of a port.

Valid States: OFF, SOLID

OFF – There is no link on this port or no error on the link.

SOLID – A fault exists in this link.

Performing advanced verification procedures

Verifying connectivity between your components using the Advanced Management Module graphical user interface (GUI) helps to ensure proper setup and troubleshoot any abnormal events.

Before you begin

About this task

To verify connectivity between your components perform the following for each SAS RAID Module:

Procedure

1. From the **I/O Module Tasks** menu, click **Configuration**.
2. From the **I/O Module Configuration** section, click **Bay 3**.
3. Click **Advanced Configuration**.
4. Ensure POST is successful
In the POST Results section of the page, The success message reads: POST results available: Module completed POST successfully.
5. From the **Advanced Setup** section, ensure that **External management over all ports** and **Preserve new IP configuration on all resets** are set to **Enabled** in the menus.
6. Click **Save**.
7. From the **Send Ping Requests** section, click **Ping SAS Module** to verify network connectivity for the SAS Switch.
8. Click **Cancel** to return to the previous screen.
9. From the **Send Ping requests to the RAID Subsystem** section, click **Ping RAID Subsystem** to verify network connectivity for the RAID Subsystem.
10. Click **Cancel** to return to the previous screen.
11. Repeat all of the above steps, to verify the advanced setting for the SAS RAID Module in I/O module bay 4.
12. From the **Monitors** menu, click **System Status**.
13. Click **I/O Modules** to verify that the **System Status Summary** indicates that the SAS RAID Modules in bays 3 and 4 are operating normally. System is operating normally. All monitored parameters are OK. If you do not see this message, use the anchor links to examine each component.
If you do not see this message indicating normal operation, then proceed to the following step. If you perform this step and find that the SAS RAID Modules are not operating in a dual-active primary-secondary environment, then utilize the alert information in this document and begin your problem determination and repair procedures.
14. Log into the RAID Subsystem and verify the controllers are operating in a dual-active primary-secondary environment.
 - a. Using a secure shell, log into the RAID Controller.
 - The default username is: USERID

- The default password is: PASSWORD (the sixth position is the numeral zero)
 - b. Verify the status of the RAID Controller. Type `list controller`. Ensure that the status is **PRIMARY** and **SECONDARY**.
 - c. To verify that no RAID Controller critical alerts exist. Type `alert -get`. If a critical alert exists in the active alert list, go to the alert section of this document to begin your problem determination and repair procedure.
15. Verify the visual indicators on each RAID Controller, ensuring the amber **System Information** and **Fault** LEDs are off.

Understanding IBM BladeCenter S SAS RAID Controller Module alerts

This topic details how to read alerts you might see while administering your RAID Controller.

The IBM BladeCenter S SAS RAID Controller Module displays alert information that keeps you informed as to the state of your system while providing for advanced diagnosis and guidance to correct errors and device failures. The alert function creates a requirement making it necessary for you to interact with the system to acknowledge critical errors and confirm actions taken in the course of system debug and repair. All of which are logged and creates a history that can be used to maintain the system and troubleshoot any future system events.

Active Alerts

Active alerts are created by events or state changes in the RAID Controller and are uniquely identified by instance ID, alert code, and primary ID parameter.

Every alert created remains active until cleared in one of the following ways:

- Timeout
- User acknowledgement
- Change in controller state

Once an alert is cleared, the alert is recorded in two places: The alert history buffer, and the alert history log file. You can also use the RAID Controller CLI to record alerts into the history log file and download them from the RAID Controller.

Note: The RAID Controller automatically updates the alert history log upon shut down.

If your RAID Controllers are in a redundant configuration, an active alert causes the information indicators on both RAID Controllers to light up, however each RAID Controller generates and maintains its own active alerts and alert history independent of the other. When the RAID Controllers are not in a bound configuration, or are not able to communicate through a serial port interconnect, you have to retrieve the active alerts from each RAID Controller separately.

Note: The mechanism for downloading the alert history logs is not inherently bound, and must always be executed separately for each RAID Controller.

Alert Types

The following is a list of alert types:

Table 9. Alert types generated by the RAID Controller

Type	Description
Persistent	Alerts that relay critical system state and remain active until corrected
Ackable	Alerts that report important conditions and remain active until corrected or acknowledged by the user or until an optional timeout expires
Maskable	Alerts that remain active until corrected. The user has the ability to mask the alert, which prevents the alert from asserting the information indicator.
Self Clearing	Generally informational with no specific user action required. These alerts are never included in the active alert list and therefore do not assert the information indicator.

System Information LED and Alert States

Active alerts have two default state attributes that are used to define how the end-user is notified of system state changes. The first attribute is the email alert attribute, which is used to notify the user of system state changes via email. The second is the maskable state attribute, which is used to notify the user of system state changes via light path diagnostics. If one or more alerts are in the unmasked state, both the SAS RAID Module system information LED and the IBM BladeCenter S chassis system information LED will illuminate.

Alert Masking

All alerts can be masked. The mask state of an alert determines if the alert contributes to the overall state of the SAS RAID Module system information LED. If an alert is masked, it does not contribute to the system information LED. Consequently, if an alert is unmasked, then it contributes to the system information LED status. The mask state of an alert may be toggled any number of times through the RAID Controller command line interface or IBM Storage Configuration Manager.

The default mask state of each alert is defined in the alert templates file, and can be set to either masked or unmasked for the initial creation state of the alert. You can use the “configure alert” on page 67 command to modify the initial mask state of the alert; this is only supported through the RAID Controller CLI. Modifying the default state does not affect any current instances of alerts (those currently displayed in the active alert list). However, any new instances of an alert after the modification are affected.

Alert Code Numbering Conventions

The following conventions have been applied in determining alert code numbering.

- 0xxx – System Status Information Alert Codes
- 1xxx – Failure Detected or Predicted Alert Codes
- 2xxx – Ready for Service Alert Codes

- 4xxx – Warning – Action Required Alert Codes
- 5xxx – Warning – Possible Action Required Alert Codes
- 9xxx – Critical Status Notification Alert Codes

Note: The thousands digit indicates the severity and user action.

The hundreds digit indicates the RAID Subsystem component associated with the alert:

- 0xx Enclosure
- 1xx Controller HW-FW
- 2xx Battery
- 3xx Drive HW-FW-Tray
- 4xx Drive Group
- 5xx Volume-FlashCopy-VolCopy
- 6xx Connectivity Host-Ethernet-Disk
- 7xx Config-Settings-Metadata

Alert Attributes

Each alert has the following attributes:

Table 10. Alert Attribute descriptions

Attribute	Description
Instance ID	32-bit per controller alert sequence number
Severity	Informational, Warning, or Critical
Timestamps	Time Created, Time Cleared / Acked
Controller ID	Unique controller ID
State	The current state of the alert. They can be as follows: <ul style="list-style-type: none"> • Masked – Alert is maskable and has been masked • Unmasked – Alert is maskable but is not masked • Unmaskable – Alert is persistent • Unacked – Alert can be cleared by user ack
Message	Descriptive string

System enclosure alerts

The alerts in this section are related to the system enclosure housing the redundant SAS RAID controller modules.

4001 System enclosure *enclosure_ID* product data memory inaccessible

Explanation: The controller cannot read or write data to the nonvolatile memory device associated with each system enclosure. This device contains vital configuration data and system identification necessary for normal functioning of the system. In the system enclosure, the memory device is located in the media tray and is accessed by the RAID controller via its onboard Baseboard Management Controller subsystem.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. The alert clears when the media tray becomes functional or when the controller is rebooted.

Operator response:

1. If either controller has active alerts indicating a failure in the Baseboard Management Controller subsystem, perform the associated diagnosis procedure for those alerts.
2. If alert 4001 is active after other alerts are cleared, remove and reinsert the media tray. Doing so might clear the alert.
3. If the alert persists, replace the media tray (see “Replacing a media tray” on page 166).

Note: The media tray contains information unique to each system, and must be configured specifically to replace the previous media tray. Failure to use a preconfigured media tray intended for the target system might result in additional system errors, including potential indeterminate data loss.

4. If the alert persists, replace the controller. If doing so does not resolve the alert, reinstall the original controller.
5. If the problem still persists, the blade chassis might be the cause.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5000 Controller warning - temperature out of range

Explanation: Elevated temperature has been detected in the controller generating the active alert.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The controller continues normal operation unless the temperature climbs to a critical level. The alert clears automatically when the temperature of the controller falls below the warning level threshold.

Operator response:

1. Make sure the room environment is within specification for the Blade Center. Check the fans used to cool the controller to see if they are operating correctly.
2. If no cooling problem exists, the temperature sensor in the controller might be malfunctioning. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5001 Controller warning - power supply voltage out of range

Explanation: Power supply voltage is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and controller sensor failure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the voltage returns to the normal operating range.

Operator response:

1. Perform a concurrent power supply replacement.
2. If the problem persists, the controller sensor might be failing. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5002 Controller warning - power supply current out of range

Explanation: Power supply current is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and controller sensor failure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the current returns to the normal operating range.

Operator response:

1. Perform a concurrent power supply replacement.
2. If the problem persists, the controller sensor might be failing. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

9000 Controller critical - temperature out of range

Explanation: The temperature detected in the controller is outside the normal operating range. The controller is initiating an orderly shutdown.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If both controllers or the survivor controller has generated this alert, the system is automatically taken offline to preserve data integrity. If only one controller in a redundant system is generating this error, that controller shuts down and the remaining controller assumes control of all volumes. The alert clears automatically when the controller temperature returns to the normal operating range.

Operator response:

1. Make sure the room environment is within specification for the Blade Center.
2. Check the fans used to cool the controller to see if they are operating correctly.
3. If no cooling problem exists, the temperature sensor in the controller might be malfunctioning. Replace the controller.

9001 Controller critical - power supply voltage out of range

Explanation: The voltage detected in the controller is outside the normal operating range. Potential causes are power supply failure and controller sensor failure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If both controllers or the survivor controller has generated this alert, the system is automatically taken off line to preserve data integrity. If only one controller in a redundant system is generating this error, that controller shuts down and the remaining controller assumes control of all volumes. The alert clears automatically when the controller voltage returns to the normal operating range.

Operator response: If this alert is generated by only one of the controllers, the voltage sensor in the controller might be malfunctioning. Replace the controller.

9002 Controller critical - power supply current out of range

Explanation: The current detected in the controller is outside the normal operating range.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If both controllers or the survivor controller has generated this alert, the system is automatically taken off line to preserve data integrity. If only one controller in a redundant system is generating this error, that controller shuts down and the remaining controller assumes control of all volumes. The alert clears automatically when the controller current returns to the normal operating range.

Operator response: If this alert is generated by only one of the controllers, the current sensor in the controller might be malfunctioning. Replace the controller.

Drive enclosure alerts

The alerts in this section are related to the drive enclosure (also known as the DSS module).

0002 Compatible drive enclosure *enclosure_ID* found

Explanation: A disk drive enclosure has been discovered, either at boot-up or during normal controller operation (because a disk enclosure was connected to the system). This alert is generated for informational purposes only, and does not indicate any error condition.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail..Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0003 Drive enclosure *enclosure_ID* removed

Explanation: A drive enclosure was disconnected during normal controller operation. This alert is generated for informational purposes only, and does not indicate any error condition.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0004 Drive enclosure *enclosure_ID* firmware updated

Explanation: Drive enclosure firmware has been successfully updated. The controller updates drive enclosure firmware as part of the controller firmware update process initiated by the user or automatically whenever a non-matching drive enclosure firmware revision is detected during controller system boot.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

1002 Drive enclosure *enclosure_ID* failure - Redundant SES device is non-functional

Explanation: Two controllers are operating redundantly and the SES device in the drive enclosure is discoverable and functioning for one controller, but not for the other. The controller that cannot communicate with the SES device generates alert 1002. This condition could result from a number of potential root causes.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response:

- If a drive enclosure firmware upgrade is in progress, ignore the alert until the firmware upgrade is successfully completed.
- If no drive enclosure firmware upgrade is in progress (including the case where a previous firmware upgrade was unsuccessful), retry the operation using the non-concurrent drive enclosure firmware upgrade procedure.
- If the firmware upgrade procedure is successful, but alert 1002 persists, perform an Asymmetrical Disk Connectivity Diagnosis. You may have to replace the controller reporting the alert or replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165)..

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4010 No viable drive groups available in system

Explanation: At least one configured drive group member drive is discovered, but no viable drive groups exist in the system. Non-viable drive groups cannot expose LUNs to any host because the controller cannot create a complete data set from the drives that are present.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when at least one viable drive group is discovered or created, or when no drive group member drives are present.

Operator response: Perform the following steps:

1. Insert any missing drives.
2. If the drives appear to be inserted but are not discovered by the system, perform a Disk Connectivity Diagnosis.
3. If the controller correctly reports the number of drives, but the missing drives are unavailable, you can either remove the drives that represent the non-viable drive groups or assimilate those drives so that they can be reused to create new spares or new drive groups.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5008 Previously connected drive enclosure *enclosure_ID* not found during startup

Explanation: A drive enclosure containing one or more previously configured drives is not discovered in the system.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. If the missing drive enclosure is an expected condition, ignore the alert. If the reported enclosure is not missing, perform a Disk Connectivity Diagnosis.

5010 Drive enclosure *enclosure_ID* - no drives detected

Explanation: A drive enclosure is detected, but no drives are discovered in the enclosure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears when drives are discovered in the enclosure or the enclosure is removed.

Operator response:

- If no drives are present in the enclosure, insert one or more drives.
- If drives are present in the enclosure but are not discovered, reseal the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165). If the problem persists, perform a Disk Connectivity Diagnosis.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5011 Drive enclosure *enclosure_ID* warning - temperature out of range

Explanation: Elevated temperature has been detected in the drive enclosure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. The alert clears automatically when the temperature of the enclosure falls below the warning level threshold.

Operator response:

1. Make sure the room environment is within specification for the Blade Center. Check the fans used to cool the controller to see if they are operating correctly.
2. If no cooling problem exists, the temperature sensor in the enclosure might be malfunctioning. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

5012 Drive enclosure *enclosure_ID* warning - power supply voltage out of range

Explanation: Drive enclosure power supply voltage is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and voltage sensor failure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the voltage returns to the normal operating range.

Operator response:

1. Replace the drive enclosure power supply.
2. If the problem persists, the voltage sensor in the enclosure might be failing. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5013 Drive enclosure *enclosure_ID* warning - power supply current out of range

Explanation: Drive enclosure power supply current is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and current sensor failure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the current returns to the normal operating range.

Operator response:

1. Replace the drive enclosure power supply.
2. If the problem persists, the current sensor in the enclosure might be failing. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5014 Drive enclosure *enclosure_ID* firmware mismatch exists. Reboot system or execute controller firmware update.

Explanation: The controller queries the firmware revision level of each drive enclosure in the system. During system boot up or as part of controller firmware upgrade, the controller automatically updates all connected drive enclosures. However, connecting a drive enclosure to a system that is already operational does not trigger a firmware update. If the drive enclosure firmware revision does not match the current controller firmware level, alert 5014 is generated.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the firmware in the drive enclosure is updated.

Operator response: You can correct the firmware mismatch by performing either of the following tasks:

- If the firmware revision of the drive enclosure is compatible with the procedure, perform a concurrent controller firmware update..
- Reboot the system. The controller automatically updates the drive enclosure firmware as part of the boot-up procedure.

Note: The drive enclosure firmware update process can take minutes to complete. During that time, the system will be offline and unavailable.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

9004 Drive enclosure *enclosure_ID* firmware update failed

Explanation: A drive enclosure firmware update has failed. The firmware update happens either automatically at system boot-up (because the firmware revision level of the drive enclosure does not match the current controller firmware level) or as part of a controller firmware update procedure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the enclosure is removed or another firmware update is initiated.

Operator response:

1. Acknowledge to clear the alert immediately.
2. Try again to update the drive enclosure firmware.
3. If this update is unsuccessful, perform a non-concurrent controller firmware update.
4. If the problem persists, perform a Disk Connectivity Diagnosis.
5. If no other solution has worked, replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

9005 Drive enclosure *enclosure_ID* fault condition - temperature out of range

Explanation: The temperature detected in the enclosure is outside the normal operating range.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the enclosure temperature returns to the normal operating range.

Operator response:

1. Make sure the room environment is within specification for the Blade Center.
2. Check the fans used to cool the enclosure to see if they are operating correctly.
3. If no cooling problem exists, the temperature sensor in the enclosure might be malfunctioning. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

9006 Drive enclosure *enclosure_ID* fault condition - power supply voltage out of range

Explanation: The voltage detected in the enclosure is outside the normal operating range. Potential causes are power supply failure and voltage sensor failure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the enclosure voltage returns to the normal operating range.

Operator response: Replace the drive enclosure power supply. If the problem persists, the voltage sensor in the enclosure might be malfunctioning. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

9007 Drive enclosure *enclosure_ID* fault condition - power supply current out of range

Explanation: The current detected in the enclosure is outside the normal operating range.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the enclosure current returns to the normal operating range.

Operator response: Replace the drive enclosure power supply. If the problem persists, the current sensor in the enclosure might be malfunctioning. Replace the drive enclosure (see “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165).

9008 Drive enclosure *enclosure_ID* fault condition - critical fan failure

Explanation: The drive enclosure cooling fan is contained in the power supply modules directly behind each drive enclosure. Alert 9008 is generated when no fan directly behind the corresponding drive enclosure is functioning.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The drive enclosure automatically powers down the drives after a five-minute delay. The controller performs an orderly system shutdown and then waits for the condition to be cleared before rebooting and restarting the system.

Operator response: Ensure that at least one working power supply is installed behind each drive enclosure. If the fan on an installed power supply is not working, perform a concurrent power supply replacement.

You can choose to run the system without the drive enclosure that is reporting the problem. To do so, perform the following steps:

1. Wait for the shutdown to complete.
2. Remove the drive enclosure.
3. Reboot the system.

Note: If the controller was unable to complete the orderly shutdown before the drive enclosure removed power from the drives, data might be stuck in cache. To avoid indeterminate data loss, ensure that the “data in cache” indicator is *not* illuminated before removing any controller or battery. Do not restart the system with any previously connected drive missing.

Controller informational alert history log events

The alerts in this section are generated for logging controller status. These operator never sees them as active alerts.

0101 Disorderly shutdown detected - System restored from battery backup

Explanation: The controller backup battery system allows for recovery of cached write data when power fails unexpectedly. This alert indicates completion of the data recovery. It is generated for logging purposes only.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0105 ArtsTime *new_time* - previous value was *old_time*

Explanation: The controller maintains a operator-settable time and date that is also synchronized when two controllers bind. This time is used when creating alerts and controller log entries.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0110 API requested *controller_ID* to shutdown and [power off|enter service mode]

Explanation: The controller supports several cases for shutting down from normal operation. This alert creates a log indicating the type of shutdown requested, which controllers are being shut down, and the source of the shutdown request.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0111 BMC requested *controller_ID* to shutdown and power off

Explanation: The controller supports several cases for shutting down from normal operation. This alert creates a log indicating the type of shutdown requested, which controllers are being shut down, and the source of the shutdown request.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

Controller informational alerts

The alerts in this section are generated as controller state warning messages.

0100 **Controller *controller_ID* firmware updated**

Explanation: The controller firmware has been updated successfully.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0103 **New controller recognized**

Explanation: A surviving controller generates this alert when a factory replacement controller is recognized in the other slot.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0104 **Replacement media tray *backplane_ID* detected**

Explanation: The controller generates this alert when a factory replacement media tray is installed and recognized. The media tray contains the system identity information that is normally associated with the chassis or backplane.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

2100 **Controller ready for service *controller_ID***

Explanation: A previously bound controller is ready for removal. Possible causes:

- Unrecoverable controller failure.
- Operator requested offline condition (part of the concurrent controller replacement procedure).

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The controller fault light turns on, indicating "ready to remove" state. Alert clears if controller is rebooted.

Operator response: Replace the controller.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator. Masking the alert does not prevent the controller fault light from illuminating.

Controller warning alerts

The alerts in this section are generated as controller state warning messages.

0102 Controller in survivor mode - Redundant controller *controller_ID* is offline

Explanation: In a redundant controller system, if one controller enters service mode and the other survivor controller assumes ownership of all LUNs, the surviving operational controller generates this alert. This alert is generated as part of the normal concurrent controller replacement procedure.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds. The condition is resolved when the controller rebinds.

Operator response: Acknowledge to clear the alert immediately. Insert the other controller or diagnose the health of the other controller by evaluating the active alerts for that controller.

1100 Controller non-critical failure detected - Ethernet port *port_ID* failed

Explanation: The controller Ethernet port is not functioning properly. Generally, this alert can be reported only when two controllers are operating in a bound configuration and the user administrative interface (CLI or GUI) is connected to the other controller.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears when the controller is rebooted. The controller with the failed Ethernet port can continue to provide redundancy to the system and service host I/O requests. However, if the controller with the working Ethernet port fails and the other controller becomes survivor, you will have no administrative communication path with the system.

Operator response: Replace the controller reporting this alert. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1101 Controller non-critical failure detected - RTC battery failed

Explanation: The controller real time clock (RTC) battery is not functioning properly.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears when the controller is rebooted. The controller with the failed RTC battery can continue to provide redundancy to the system and service host I/O requests. However, if the other controller fails and this controller becomes survivor, the system time might be reported incorrectly.

Operator response: Replace the controller reporting this alert. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1102 Controller non-critical failure detected - RTC failed

Explanation: The controller real time clock (RTC) is not functioning properly.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears when the controller is rebooted. The controller with the failed RTC can continue to provide redundancy to the system and service host I/O requests. However, if the other controller fails and this controller becomes survivor, the system time might be reported incorrectly.

Operator response: Replace the controller reporting this alert. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

3100 Controller entering service mode to maintain volume availability.

Explanation: The non-survivor controller generates this alert when a failover has occurred because this controller was providing access to volumes mapped to a non-redundant disk drive and has lost the ability to communicate with that drive. The other controller does have access to the non-redundant disk drive and can provide access to the host as a survivor controller. The root problem is asymmetric drive connectivity.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If connectivity to all drives is restored, this controller rebinds with the surviving controller and redundant operation resumes. Alert clears when bound controller state is achieved.

Operator response: Perform an Asymmetrical Disk Connectivity Diagnosis. If the non-redundant drive is replaced, restart this controller to return to redundant controller operation.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

3101 Controller entering service mode to maintain volume availability.

Explanation: The survivor controller generates this alert when a failover has occurred because the other controller has lost connectivity to a non-redundant disk drive and can no longer provide access to the associated volumes. This controller does have access to the non-redundant disk drive and can provide access to the host as a survivor controller. The root problem is asymmetric drive connectivity.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If connectivity to all drives is restored, the controller in service mode rebinds with the surviving controller and redundant operation resumes. The alert clears when bound controller state is achieved.

Operator response: Perform an Asymmetrical Disk Connectivity Diagnosis. If the non-redundant drive is replaced, restart this controller to return to normal operation.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4100 ZSS waiting for specified drive configuration

Explanation: RAID Zero Step Setup is a mechanism by which the controller detects that it has never before been configured in a system, finds that no drives in the system contain configuration information (metadata), and is enabled to run a factory installed configuration script when a minimum number of drives have been installed. This alert is generated when the controller is ready to run the script, but has not yet discovered the minimum physical configuration of drives required.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. In most cases, installing additional drives causes the controller to clear this alert and proceed to automatically configure the system as per the Zero Step Setup feature.

Note: Because you might want to add more than the minimum number of drives, the controller does not initiate Zero Step Setup configuration immediately after discovering a sufficient number of drives. Instead, the controller waits for predefined period (the default is 60 seconds) after each drive insertion so that you have time to add more drives. If that period elapses without further drive insertions, Zero Step Setup configuration begins.

Operator response: Use manual to determine proper drive configuration for Zero Step Setup. If the alert is still active more than 60 seconds after you ensure that the correct drive configuration exists, perform a Disk Connectivity Diagnosis.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4101 Controller diagnostic information available. Please collect controller logs.

Explanation: Uncollected cdump image exists and overwrite protection delay has not expired.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when overwrite protection delay has expired or data has been collected.

Operator response: None.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5000 Controller warning - temperature out of range

Explanation: Elevated temperature has been detected in the controller generating the active alert.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The controller continues normal operation unless the temperature climbs to a critical level. The alert clears automatically when the temperature of the controller falls below the warning level threshold.

Operator response:

1. Make sure the room environment is within specification for the Blade Center. Check the fans used to cool the controller to see if they are operating correctly.
2. If no cooling problem exists, the temperature sensor in the controller might be malfunctioning. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5001 Controller warning - power supply voltage out of range

Explanation: Power supply voltage is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and controller sensor failure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the voltage returns to the normal operating range.

Operator response:

1. Perform a concurrent power supply replacement.
2. If the problem persists, the controller sensor might be failing. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5002 Controller warning - power supply current out of range

Explanation: Power supply current is not yet critical, but is out of the normal operating range. Potential causes are power supply failure and controller sensor failure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the current returns to the normal operating range.

Operator response:

1. Perform a concurrent power supply replacement.
2. If the problem persists, the controller sensor might be failing. Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5101 Controller in survivor mode - Redundant controller *controller_ID* failed or missing

Explanation: The surviving controller generates this alert when the other controller is undetectable or unresponsive. This alert occurs when the other controller is removed for service.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the survivor rebinds.

Operator response: Insert the missing controller or replace the failed controller.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5102 Controller in survivor mode - Redundant controller *controller_ID* ready for removal

Explanation: The survivor controller generates this alert in conjunction with alert 2100 being generated by the other controller.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the other controller is removed or restarted.

Operator response: Remove or reboot the other controller.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

Controller critical alerts

The alerts in this section are generated when a critical failure has occurred.

1103 Controller critical failure detected - baseboard management controller failed

Explanation: The controller continually monitors the health of the Baseboard Management Controller subsystem and controls the power for the controller. If this subsystem fails, the controller might not be able to control indicator lights, check environmental conditions, store critical state information, and retrieve system identity data. When this alert is generated, the controller can no longer continue normal operation.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If the failure occurs in a redundant controller, the remaining controller enters survivor mode and assumes control of all disk drives and associated LUNs while the failed controller enters service mode. If this failure occurs on a controller that is already in survivor mode, the controller attempts to flush all dirty cache and orderly dismount all volumes prior to entering service mode.

Operator response: Reboot the controller. All alerts are cleared. The controller reevaluates the system health status and regenerates all alerts that apply. If alert 1103 is generated again after the reboot, replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

1104 Controller critical failure detected - SES/SAS expander failed

Explanation: The controller continually monitors the health of the SES (System Enclosure Services) controller / SAS expander subsystem. If this subsystem fails, the controller might not be able to control indicator lights, check environmental conditions, and access drives. When this alert is generated, the controller can no longer continue normal operation.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If the failure occurs in a redundant controller, the remaining controller enters survivor mode and assumes control of all disk drives and associated LUNs while the failed controller enters service mode. If this failure occurs on a controller that is already in survivor mode, the controller attempts to flush all dirty cache and orderly dismount all volumes prior to entering service mode.

Operator response: Reboot the controller. All alerts are cleared. The controller reevaluates the system health status and regenerates all alerts that apply. If alert 1104 is generated again after the reboot, replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

1105 Controller *controller_ID* critical failure detected - Unrecoverable HW error

Explanation: An unrecoverable hardware error has been detected in the controller. The controller continually monitors the health of the RAID Storage Processor and microprocessor subsystem. When this alert is generated, the controller can no longer continue normal operation.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If the failure occurs in a redundant controller, the remaining controller enters survivor mode and assumes control of all disk drives and associated LUNs while the failed controller enters service mode. If this failure occurs on a controller that is already in survivor mode, the controller attempts to flush all dirty cache and orderly dismount all volumes prior to entering service mode.

Operator response: Reboot the controller. All alerts are cleared. The controller reevaluates the system health status and regenerates all alerts that apply. If alert 1105 is generated again after the reboot, replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

1106 Controller *controller_ID* critical failure detected - Recurring system error

Explanation: The controller attempts to automatically recover from unexpected system errors, including both software and hardware errors. If, after repeated recovery attempts (during which the controller might perform multiple restarts), the failure persists or reoccurs within a predetermined time window, the controller aborts further recovery attempts and generates this alert. When this alert is generated, the controller can no longer continue normal operation.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If the failure occurs in a redundant controller, the remaining controller enters survivor mode and assumes control of all disk drives and associated LUNs while the failed controller enters service mode. If this failure occurs on a controller that is already in survivor mode, the controller attempts to flush all dirty cache and orderly dismount all volumes prior to entering service mode.

Operator response: Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

1107 Controller critical failure detected - Serial port failed

Explanation: The system uses a dedicated serial port to exchange status and control between redundant controllers. If this port fails, each controller might attempt to become the survivor controller and reset the other controller. Thus, the other controller might actually reset the controller that reports alert 1107 before you can take additional corrective action. When this alert is generated, the controller can no longer continue normal operation.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. If the failure occurs in a redundant controller, the remaining controller enters survivor mode and assumes control of all disk drives and associated LUNs while the failed controller enters service mode. If this failure occurs on a controller that is already in survivor mode, the controller attempts to flush all dirty cache and orderly dismount all volumes prior to entering service mode.

Operator response: Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

1108 Controller critical failure detected - Mirror bus failed

Explanation: The system uses a dedicated high-speed dual lane mirror bus to maintain redundant controller operation. If this bus fails, each the controllers use the serial port interconnect to determine the controller most qualified to enter survivor mode and the other controller enters service mode. Both controllers might report alert 1108, and it can be difficult to determine which controller is at fault.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert cannot be masked or cleared and persists until one controller is removed or until the mirror bus becomes functional.

Operator response: Perform the following troubleshooting procedure:

1. Remove and reinsert the controller in service mode. If the reinserted controller boots up and binds with the survivor controller, either the controller was not well inserted before, or the connector between the controller and the backplane might have intermittent connectivity.
2. If the reinserted controller again reports alert 1108, shut down the system and reseal the survivor controller (see “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159).
3. If reseating the survivor controller does not clear the conditions, replace the controller in service mode with a new controller.
4. If the problem persists, replace the other controller with the removed original service mode controller.
5. If the problem is still not resolved, either the remaining controller needs to be replaced or the backplane is defective and needs to be replaced.

1109 Controller *controller_ID* critical failure detected, replace controller

Explanation: The path used to communicate with disk drives is nonfunctional.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when a different controller rebinds with the survivor controller or the system is rebooted.

Operator response: Replace the controller. See “Replacing a single controller using the CLI” on page 158 or “Replacing a single controller using the SCM” on page 159.

5100 Controller unable to continue redundant operation

Explanation: This alert is generated by a controller in service mode in conjunction with when two controllers are unable to bind. In order to bind, both controllers must be able to communicate properly via the dedicated mirror bus, the list of drives discovered by each controller must match, and the firmware revisions must match.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears automatically when the controller enters redundant operation or reboots as a survivor controller.

Operator response: Look for additional alerts to determine the reason why the controllers cannot bind.

9100 Controller *controller_ID* FW update failed

Explanation: The controller firmware update process has failed.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when a firmware update completes successfully.

Operator response: Perform the following steps:

1. Reboot the controller.
2. Try again to perform a concurrent controller firmware update. You might have to use a different firmware set.

9101 Controller incompatible with survivor controller - Unable to bind

Explanation: Normally, if a redundant controller attempts to enter redundant operation with another controller currently in survivor mode, the survivor controller will ensure that the firmware revision level of the redundant controller matches the survivor firmware revision level. If the firmware does not match, the survivor controller transfers its own firmware to the redundant controller to correct the mismatch. However, if the redundant controller hardware is not compatible with the survivor firmware, the operation is aborted and the redundant controller reports alert 9101.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the controller is rebooted.

Operator response: Correct the firmware version mismatch. Possible solutions:

- Obtain a replacement redundant controller that is compatible with the survivor controller.
- Replace the survivor controller with hardware that is compatible with the redundant controller (see “Replacing a single controller using the CLI” on page 158).

9103 Unable to determine machine identity - machine initialization is required

Explanation: On boot-up, the controller detected that the backplane has not been initialized with Enclosure IDs and the controller identities or states do not match or are not initialized.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The controller enters service mode. The alert clears after the operator loads the genesis file via FTP and reboots.

Operator response: Load genesis file via FTP and then reboot.

Battery informational alert history log events

The alerts in this section are generated for logging battery status. These operator never sees them as active alerts.

0200 Battery *battery_ID* started charging

Explanation: Battery has started charging.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0201 Battery *battery_ID* stopped charging

Explanation: Battery has stopped charging.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0202 Battery *battery_ID* started conditioning

Explanation: Battery has started conditioning.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0203 Battery *battery_ID* stopped conditioning

Explanation: Battery has stopped conditioning.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0204 Battery *battery_ID* started discharging

Explanation: Battery has started discharging.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0205 Battery *battery_ID* stopped discharging

Explanation: Battery has stopped discharging.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0206 Battery *battery_ID* connected to memory

Explanation: Battery has been connected to memory and will provide some amount of battery backup.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0207 Battery *battery_ID* disconnected from memory

Explanation: Battery has been disconnected from memory and no longer provides any battery backup. This event is part of an orderly shutdown process.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0208 Battery change notification received (*present*=[0|1], *swapped*=[0|1])

Explanation: A battery change notification has been received.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0209 Battery *battery_ID* non-volatile memory read

Explanation: Battery has non-volatile memory that was read during BBU detection.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None

0210 Battery *battery_ID* non-volatile memory written

Explanation: Battery has non-volatile memory that was written during BBU detection.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None

Battery alerts

The alerts in this section are generated to inform the operator of changes in battery status.

0215 Battery *battery_ID* firmware update complete

Explanation: When the system boots up or a battery is inserted, the controller checks the battery firmware level. If the firmware does not match the expected version, the controller automatically performs a firmware update and then generates this alert to indicate that a firmware mismatch was detected and corrected.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

1200 Battery *battery_ID* nearing expiration date (*date*)

Explanation: The battery has expiration date tracking, and the expiration date is between 14 and 90 days from now.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when battery is removed or battery status changes to “expiration imminent” (alert 1201).

Operator response: Replace the battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1201 Battery *battery_ID* expiration date (*date*) imminent

Explanation: The battery has expiration date tracking, and the expiration date is less than 15 days from now.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the battery is removed or battery status changes to “expired” (alert 1202).

Operator response: Replace the battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1202 Battery *battery_ID* expired (*date*)

Explanation: The battery has expiration date tracking, and the battery expiration date has passed.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the battery is removed.

Operator response: Replace the battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1203 Battery *battery_ID* failed (*code failure_code*)

Explanation: No working battery is detected. Possible causes include:

- Battery communication error or timeout
- Missing battery
- Charging system failure
- Battery has passed its expiration date
- Battery temperature out of Spec range

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the battery is removed.

Operator response: Correct the problem. Ensure that a working battery is in place (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4200 Battery missing

Explanation: Configuration supports a battery, but no battery is detected by the SES controller.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when a battery is inserted.

Operator response: Insert a battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4201 Battery *battery_ID* product data memory inaccessible

Explanation: BBU flash device is inaccessible

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. This alert persists until BBU flash device is functional.

Operator response: Replace the battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5200 Controller *controller_ID* reports RAID system 72-hour battery reserve unavailable

Explanation: No single controller-battery pair available with 72-hour capacity and controller write cache policy is enabled.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when a controller-battery pair with 72-hour capacity or controller write cache policy is enabled.

Operator response: Do either of the following:

- Replace the battery (see “Replacing a Battery Backup Unit” on page 181).
- Wait for the battery to charge.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5201 Battery *battery_ID* firmware mismatch exists

Explanation: When the system boots up or a battery is inserted, the controller checks the battery firmware level. If the firmware does not match the expected version, the controller automatically performs a firmware update. This alert indicates that a firmware mismatch was detected, but was not corrected because the battery firmware update failed.

System action: the operator is notified of this alert by e-mail. Alert clears if the battery is removed.

Operator response: Reinsert or replace the battery (see “Replacing a Battery Backup Unit” on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

9200 Battery *battery_ID* firmware update failed

Explanation: When the system boots up or a battery is inserted, the controller checks the battery firmware level. If the firmware does not match the expected version, the controller automatically performs a firmware update. This alert indicates that a firmware mismatch was detected, but the battery firmware update failed.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears if the battery is removed or a firmware update is initiated.

Operator response: Acknowledge to clear the alert immediately. Initiate another firmware update by removing and reinserting the battery. If multiple attempts to update the firmware are unsuccessful, replace the battery (see “Replacing a Battery Backup Unit” on page 181).

Disk drive informational alerts

The alerts in this section are generated as disk drive state warning messages.

0300 Spare drive *drive_ID* reassigned

Explanation: Rebuild operation has been started on the drive group and the spare drive has been selected for rebuild.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0303 Spare drive *drive_ID* copyback complete

Explanation: The copyback operation has completed and the spare drive is now available.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0304 Drive *drive_ID* position has been updated

Explanation: By default, the SAS RAID Module system information indicator is not turned on and

System action: the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0307 Drive *drive_ID* firmware upgraded

Explanation: Drive firmware upgrade has completed successfully.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0308 Replacement drive *drive_ID* detected, and assigned as global spare

Explanation: A new replacement drive has been detected and assigned as a spare.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0310 Drive *drive_ID* mounted as global spare

Explanation: The drive has been mounted as a global spare.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0311 Global spare drive *drive_ID* dismounted

Explanation: Orderly dismount of a global spare completed successfully. May be invoked explicitly as dismount spare or as part of dismount enclosure.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears if the drive is removed or a mount command is issued. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0315 Drive *drive_ID* removed

Explanation: Detected missing drive drive removal via SES.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0316 Drive *drive_ID* inserted

Explanation: Detected new drive via drive login after boot time discovery.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

2000 Dismounted drive enclosure *enclosure_ID* ready to remove

Explanation: Orderly dismount of all mounted drives in an enclosure has completed successfully.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Drive enclosure light indicates "ready to remove" state. Alert clears when the enclosure is removed.

Operator response: Remove the enclosure.

2100 Controller ready for service *controller_ID*

Explanation: A previously bound controller is ready for removal. Possible causes:

- Unrecoverable controller failure.
- Operator requested offline condition (part of the concurrent controller replacement procedure).

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The controller fault light turns on, indicating "ready to remove" state. Alert clears if controller is rebooted.

Operator response: Replace the controller.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator. Masking the alert does not prevent the controller fault light from illuminating.

2101 Controller ready for service. RAID System is down due to *service_mode_reason*

Explanation: The controller was in Survivor/Standalone state and has entered offline state due to a unrecoverable error or by operator request. The controller is now ready for service. This alert is triggered by any of the following events:

- SES not accessible
- BMC not accessible
- VPD not accessible
- Battery backup is low or has failed
- SES is reporting critical environmental
- User requested service mode case

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The controller fault light turns on, indicating "ready to remove" state.

- If battery backup was low, the alert clears when charge returns to sufficient.
- If SES reported critical environmental, the alert clears when SES environmentals return to normal.
- For other problems, the alert clears after the problem is corrected and the controller is rebooted.

Operator response: Correct the problem. Reboot the controller. If the problem persists, replace the controller.

2200 Battery *battery_ID* **ready for service**

Explanation: The battery is detected present by SES, but has failed or expired. It is ready to be removed.

System action: Battery fault light turns on, indicating "ready to remove" state. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the battery is removed.

Operator response: Replace the battery (see "Replacing a Battery Backup Unit" on page 181).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

2300 Drive *drive_ID* ready for service

Explanation: Drive is ready for removal. Possible causes:

- Dismount request from operator
- Presence of an unreliable drive (failed or undiscoverable yet detected by SES)
- Presence of an unsupported drive

System action: Drive fault light turns on, indicating "ready to remove" state. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed or the drive mount state changes (to unmounted or mounted).

Operator response: Remove the drive.

2320 Drive carrier *tray_ID* ready for service

Explanation: Tray contains no mounted drives and at least one dismounted drive

System action: Tray fault light turns on, indicating "ready to remove" state. Drive fault lights of any associated failed drives turn on, indicating "ready to remove" state. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when tray is removed.

Operator response: Remove the tray

2322 Drive carrier *tray_ID* ready for service

Explanation: The operator set the tray mount state to DISMOUNTED.

System action: Tray fault light turns on, indicating "ready to remove" state. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when tray is removed or mount state changes to MOUNTED.

Operator response: Acknowledge to clear the alert immediately. Remove the tray.

Disk drive alerts

The alerts in this section are generated to inform the operator of changes in drive status.

0317 Unresponsive drive inserted in location *drive_ID*

Explanation: SES detects drive presence, but no target port login detected after appropriate delay.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when drive connectivity is established or the drive is removed.

Operator response: Check drive connections or replace drive (see "Replacing a failed drive" on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

0325 Drive carrier *tray_ID* removed

Explanation: A drive carrier tray that was previously known to exist was detected as missing by SES.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0326 Drive carrier *tray_ID* inserted

Explanation: Detected new tray via SES.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0328 Tray spare drive *drive_ID* discovered in drive carrier *tray_ID* with one or more assigned drives - Drive converted to global spare

Explanation: Drive in tray is tray spare drive, but tray is not a spare tray.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0330 Drive *drive_ID* containing stale metadata has been discovered after initial system boot. This drive is a member of drive group *group_ID*, a RAID *raid_level* group containing drive(s) *drive_list*.

Explanation: The controller allows missing member drives of groups discovered at boot up and spare drives to be hot plugged into the system after initial boot up. However, if a hot plugged drive's metadata indicates that the drive is part of a drive group that was not discovered during system boot up, no group is listed, the drive is reported as assigned, and this alert is generated. The arguments in this alert indicate the group to which the drive belongs. To mount the drive as is, a controller restart is required. The alert persists until acknowledged by the user or the drive is removed.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears when the drive is assimilated or removed.

Operator response: Acknowledge to clear the alert immediately. Assimilate or remove the drive.

1300 Drive *drive_ID* failure detected- Previous drive status was [inuse|spare]

Explanation: Drive failure condition caused controller to fail a drive group member or spare drive.

System action: Drive mount state is set to DISMOUNTED. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. This alert (and all other 13xx alerts) is cleared when the drive is removed.

Operator response: Replace the failed drive (see "Replacing a failed drive" on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1301 Drive *drive_ID* failure detected - Previous drive status was unassigned

Explanation: Drive failure condition caused controller to fail an unassigned, foreign, or IM drive.

System action: Drive mount state is set to DISMOUNTED. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears when the drive is removed.

Operator response: Replace the failed drive (see “Replacing a failed drive” on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1303 Drive *drive_ID* reports predicted failure - Current drive status is [inuse | spare]

Explanation: PFA detected.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed.

Operator response: Replace the drive (see “Replacing a failed drive” on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1304 Drive *drive_ID* reports predicted failure - Current drive status is unassigned

Explanation: PFA detected.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed.

Operator response: Replace the drive (see “Replacing a failed drive” on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1305 Drive *drive_ID* failure detected - Primary disk port unusable, previous drive status was [inuse | spare]

Explanation: Drive failure process initiated on a drive because of unreliable connectivity on servicer drive port of assigned drive. Possible causes:

- Unusable error threshold exceeded.
- Persistent logged out condition.

System action: If drive is redundant or spare, the drive is failed and alert 1300 is generated. By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed.

Operator response: Replace the failed drive (see “Replacing a failed drive” on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1307 Drive *drive_ID* error condition detected - Secondary disk port unusable, current drive status [inuse | spare | unassigned]

Explanation: Drive failure process initiated on a drive because of unreliable connectivity on servicer drive port of assigned drive. Possible causes:

- Unusable error threshold exceeded.
- Persistent logged out condition.

The drive is not failed or dismounted based on secondary port status.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed.

Operator response: Replace the drive (see “Replacing a failed drive” on page 171)..

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1309 Drive *drive_ID* failure detected - Drive failed to reassign sector, current drive status is [inuse | spare]

Explanation: Drive failure process initiated because the drive returned an error on a reassign sector command.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert 1300 or 1301 is also generated. Alert clears when the drive is removed.

Operator response: Replace the failed drive (see “Replacing a failed drive” on page 171).

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

1310 Drive *drive_ID* status has been changed from unassigned to unreliable

Explanation: Due to metadata read from a newly discovered drive, a previously unassigned drive has been marked unreliable. Possible causes:

- Drive reports reassign block failure.
- Drive exceeded configured maximum media error threshold per drive.

System action: Drive mount state is set to DISMOUNTED. By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears immediately if the drive is removed. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Replace the drive (see “Replacing a failed drive” on page 171).

2300 Drive *drive_ID* ready for service

Explanation: Drive is ready for removal. Possible causes:

- Dismount request from operator
- Presence of an unreliable drive (failed or undiscoverable yet detected by SES)
- Presence of an unsupported drive

System action: Drive fault light turns on, indicating "ready to remove" state. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed or the drive mount state changes (to unmounted or mounted).

Operator response: Remove the drive.

4300 Unsupported drive *drive_ID* detected

Explanation: Drive lockout active due to unsupported drive.

System action: Controller rejects all configuration commands until the unsupported drive is removed. By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the unsupported drive is removed.

Operator response: Remove the unsupported drive.

4301 Unmasked drive firmware level is unsupported

Explanation: A disk drive with an unsupported firmware level is detected by the controller.

System action: The controller will not configure the disk drive.

Operator response: Remove the disk drive with the unsupported firmware level, or upgrade the disk drive firmware level.

4302 Drive *drive_ID* specifies one or more missing drives already determined to be missing from a previously discovered drive group. This drive is a member of drive group *group_ID*, a RAID *raid_level* group containing drive(s) *drive_list*.

Explanation: A drive group has been discovered that specifies one or more member drives that are missing from the system and already described as members of a previously discovered drive group. The previously discovered drive group need not be mounted to cause this alert.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the affected drives are assimilated or removed from the system.

Operator response: Assimilate or remove the affected drives.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4303 Drive *drive_ID* specifies a group whose identity conflicts with an existing group. This drive is a member of drive group *group_ID*, a RAID *raid_level* group containing drive(s) *drive_list*.

Explanation: A drive group is discovered whose GUID conflicts with an already recreated group. The previously discovered group need not be mounted to cause this alert.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the affected drives are assimilated or removed from the system.

Operator response: Assimilate or remove the affected drives.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4304 Drive *drive_ID* cannot be mounted without exceeding controller resource limits. This drive is a member of drive group *group_ID*, a RAID *raid_level* group containing drive(s) *drive_list*.

Explanation: A drive group is discovered that, if mounted, would cause one or more controller resource limits to be exceeded (max volumes, max hosts, max terabytes, etc.).

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the affected drives are assimilated or removed from the system.

Operator response: Assimilate or remove the affected drives.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4322 **Drive carrier *tray_ID* contains one or more unreliable or unsupported drives and cannot be mounted. Please remove drive(s) *drive_list* and reinsert.**

Explanation: Cannot mount tray due to unreliable or unsupported drives

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the tray is removed.

Operator response: Remove unsupported or unreliable drives from system.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5300 **Drive *drive_ID* firmware update failed**

Explanation: Attempted drive firmware update operation was unsuccessful.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Retry the firmware update.

5301 **Surplus capacity of replacement drive *drive_ID* will not be utilized**

Explanation: Drive in replacement tray has too much capacity.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Replacement drive detection treats this as a qualified replacement drive and automatically uses the spare. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5302 **Drive *drive_ID* cannot be used as a replacement.**

Explanation: Replacement drive is not qualified. This alert indicates that replacement drive detection has been disabled for this group.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Assign a replacement spare drive manually.

5303 **No drives discovered**

Explanation: No drives were discovered during system boot-up. RAID Zero Step Setup is disabled.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears automatically when at least one drive is discovered.

Operator response: Acknowledge to clear the alert immediately.

5305 Unreliable drive *drive_ID* detected.

Explanation: Unreliable drive discovered.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when the drive is removed.

Operator response: Acknowledge to clear the alert immediately. Remove the drive.

5306 Global spare drive *drive_ID* is not qualified for any currently mounted drive group

Explanation: Possible causes:

- A global spare is mounted, but is not usable by any drive group in the system.
- The last drive group for which the global spare qualifies is dismounted.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the affected spare is deleted or dismounted

Operator response: Configure one or more groups for which the drive can be a spare or configure a larger spare drive.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5310 Drive *drive_ID* missing from drive group *group_ID*. Group is not viable due to missing drive(s) and associated volumes are not mounted.

Explanation: Drive group is non-viable due to missing drives as detected each time metadata processing is invoked.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when one of the following events occurs:

- The drive is inserted.
- The drive group is deleted.
- All member drives are removed.
- Enough member drives are inserted to restore viability.

Operator response: Add drives to make the group viable. If no automount occurs, reissue the mount command.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5311 Drive *drive_ID* metadata unusable and drive was not found to be part of any existing drive group. Drive state set to unassigned.

Explanation: This alert is caused by drive metadata errors. Possible errors include:

- Anchor error
- Both sections unreadable
- One section open and the other unreadable

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5322 **Drive carrier *tray_ID* is not qualified as a replacment. No spare tray assignment will be performed.**

Explanation: Replacement tray is not qualified. This alert indicates that replacement drive detection has been disabled for this group.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Assign a replacement spare drive manually.

9300 **RAID system down - Unsupported drive *drive_ID* detected**

Explanation: The system entered service mode because unsupported drives were detected on boot-up.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the unsupported drive is removed.

Operator response: Remove the unsupported drive.

9302 **Drive *drive_ID* not accessible, please restore connectivity or acknowledge drive group *group_ID* disorderly dismount with potential indeterminate data loss.**

Explanation: The specified drive has no usable paths and is contributing to the specified mounted drive group not being viable.

Note: If this condition is detected in power fail recovery and Auto Ack Pending Non-Viable is enabled, alert 9406 is generated for the group and this alert is not generated for each missing drive group member drive.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when one of the following events occurs:

- The specified drive is discovered in the system. (It might not be usable by the group.)
- Enough drives are discovered to make group viable (not including this drive).
- The drive group is deleted.
- One or more drive group members are failed as unreliable such that the group cannot become viable even if this drive is reconnected.

Operator response: Acknowledge to clear the alert immediately. Restore the missing drive.

9303 **Global spare drive *drive_ID* has been orderly dismounted due to enclosure *enclosure_ID* fault condition.**

Explanation: Forced orderly dismount due to enclosure critical environmentals.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

9304 **One or more outstanding alert 9302 conditions exist. Acknowledge to proceed with shutdown.**

Explanation: System shutdown initiated with outstanding 9302 alerts.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when all 9302 alerts are cleared. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Restore the missing drive.

9308 **Drive *drive_ID* contains metadata protocol violation. Drive state set to incompatible metadata.**

Explanation: Read errors existed in both metadata copies during drive discovery.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the drive is removed or assimilated.

Operator response: Remove or assimilate the drive.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

9310 **Drive *drive_ID* not accessible during power fail recovery, please restore connectivity or acknowledge to skip power fail recovery for drive group *group_ID* with potential indeterminate data loss.**

Explanation: A non-redundant drive was missing during power failure recovery. Auto Ack Pending Non-Viable is disabled.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. The alert clears when the missing drive is inserted or the drive group becomes viable. After a predefined delay, the controller initiates RAID Zero Step Setup configuration.

Operator response: Acknowledge to clear the alert immediately. Insert the missing drive (or enough drives to make the drive group viable).

Note: Because you might want to add more than the minimum number of drives, the controller does not initiate Zero Step Setup configuration immediately after discovering a sufficient number of drives. Instead, the controller waits for predefined period (the default is 60 seconds) after each drive insertion so that you have time to add more drives. If that period elapses without further drive insertions, Zero Step Setup configuration begins.

Drive group alerts

The alerts in this section are generated to inform the operator of changes in drive group status.

0400 **Long-running task started: *task_info***

Explanation: Volume service started.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds. Alert clears immediately when volume service is suspended or cancelled.

Operator response: Acknowledge to clear the alert immediately.

0401 Long-running task suspended: *task_info*

Explanation: Volume service has been suspended.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0402 Long-running task completed: *task_info*

Explanation: Volume service has completed.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0403 Drive group *group_ID* redundancy restored

Explanation: The redundancy of the drive group has been restored after successful completion of rebuild on the drive group.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0410 Stale Drive group *group_ID* mounted

Explanation: Stale drive group mounted.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0411 Drive *drive_ID* mounted as local spare for group *group_ID*

Explanation: Local spare mounted.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0412 Drive group *group_ID* dismounted

Explanation: Orderly dismount of drive group *group_ID* completed successfully.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears when a mount command is issued or the last drive associated with the drive group is removed.

Operator response: This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

4010 No viable drive groups available in system

Explanation: At least one configured drive group member drive is discovered, but no viable drive groups exist in the system. Non-viable drive groups cannot expose LUNs to any host because the controller cannot create a complete data set from the drives that are present.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when at least one viable drive group is discovered or created, or when no drive group member drives are present.

Operator response: Perform the following steps:

1. Insert any missing drives.
2. If the drives appear to be inserted but are not discovered by the system, perform a Disk Connectivity Diagnosis.
3. If the controller correctly reports the number of drives, but the missing drives are unavailable, you can either remove the drives that represent the non-viable drive groups or assimilate those drives so that they can be reused to create new spares or new drive groups.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

3400 Degraded drive group *group_ID*

Explanation: Failure of a redundant drive caused the drive group to become degraded, but the drive group is still viable (a spare is available).

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears when either of the following events occurs:

- Rebuild operation has been completed and redundancy of the drive group has been restored.
- The drive group is deleted.

Operator response: None.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5400 Degraded drive group *group_ID* - No spare available for rebuild

Explanation: Drive group has become degraded due to failure of a redundant drive. The drive group is viable, but no usable spare is available for rebuildDrive.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when a spare becomes available.

Operator response: Assign a spare drive or insert a qualified replacement drive.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5403 Previously mounted drive group *group_ID* comprised of drives *drive_list* was not found and has been removed from mounted group list.

Explanation: Entire drive group found missing on cold boot.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Add drives to make the group viable. If no automount occurs, reissue the mount command. (In release 1, you must reboot the system to mount the group when available.)

5405 **Drive group *group_ID* has been degraded due to enclosure *enclosure_ID* fault condition. Drive(s) *drive_list* removed from drive group.**

Explanation: Forced orderly dismount due to enclosure critical environmental conditions caused one or more "dropped" drives, but the group is still viable.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

5406 **Long-running task canceled prior to completion: *task_info***

Explanation: Volume service permanently aborted.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5410 **Stale drive group conflicting group name *group_ID1* has been renamed to group name *group_ID2***

Explanation: Group rename occurred during discovery.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5413 **Previously mounted drive group *group_ID* comprised of drives *drive_list* does not match current controller ID and has been removed from mounted group list.**

Explanation: MGL group found but does not match the ID of this controller on cold boot.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

5414 **Drive group *group_ID* is offline due to one or more missing drives.**

Explanation: This alert is generated when a group becomes non-viable due to one or more missing drives. This can occur at system startup if the group cannot be mounted due to missing non-redundant drives, or during normal operation if the group was previously mounted and connectivity to one or more non-redundant drives is lost.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Reinsert the missing drives.

Note: In the R1 release, you must reboot the system with the missing drives in place in order to return the group and its associated volumes to the mounted viable state with mapped LUNs online and accessible.

5720 Spare drive carrier *tray_ID* has been disqualified, drive carrier spare drives converted to global spares

Explanation: A group is created such that an existing spare tray is no longer qualified as a spare tray.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Assign a new spare drive or tray if required.

9401 Drive group *group_ID* has been mounted with indeterminate data loss

Explanation: This alert is caused by either of the following events:

- With the "force disorderly mount" controller setting is enabled, a mount operation was performed on a drive group that was not orderly dismounted.
- All drives in the group are from the same controller and were mounted regardless of automount setting and "force disorderly mount" setting.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9403 Drive group *group_ID* was not orderly dismounted - Acknowledge to mount with indeterminate data loss

Explanation: With the "force disorderly mount" controller setting disabled, a mount operation was attempted on a drive group that was not orderly dismounted.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the affected drive group is removed.

Operator response: Acknowledge to clear the alert immediately. Remove the affected drive group.

9405 Drive group *group_ID* has been orderly dismounted due to enclosure *enclosure_ID* fault condition.

Explanation: Due to enclosure critical environmental, a forced orderly dismount was performed.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9406 Drive group *group_ID* missing during powerfail recovery has been disorderly dismounted

Explanation: With "Auto Ack Pending Non-Viable" enabled, a PFR drive group was not found during PFR drive discovery.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9408 **Drive group *group_ID* unavailable during powerfail recovery - Reconnect drive(s) *drive_list* if missing or acknowledge indeterminate data loss to proceed.**

Explanation: With "Auto Ack Pending Non-Viable" disabled, a PFR drive group was not found during PFR drive discovery because all drives were missing or defunct.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when at least one member drive of the missing drive group is discovered.

Operator response: Acknowledge to clear the alert immediately. Insert one or more of the missing drives.

9409 **JBOD pass-through drive missing during powerfail recovery. To proceed, acknowledge indeterminate data loss for Host:LUN *LUN*, or insert missing drive *drive_ID*.**

Explanation: With "Auto Ack Pending Non-Viable" disabled, a PFR JBOD drive was not found during PFR drive discovery. Dirty cache exists for the corresponding volume.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the missing JBOD drive is discovered.

Operator response: Acknowledge to clear the alert immediately. Insert the missing JBOD drive.

9410 **Drive group *group_ID* was disorderly dismounted during power fail recovery due to unavailable drive(s) *drive_list*.**

Explanation: Drive group is non-viable during PFR due to missing or defunct drives. "Auto Ack Pending Non-Viable" is enabled.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9411 **Drive group *group_ID* is non-viable due to unusable drive(s) *drive_list*. Acknowledge to dismount associated volumes.**

Explanation: System is operational (not in warm boot) and this group is on the MG list but is not viable due to one or more unreliable drives.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

Note: Acknowledging the alert causes the affected drive group to be removed from the MG list.

9412 **Drive group *group_ID* volume migration in progress and destination group is missing. Volumes not completely migrated to destination have been deleted.**

Explanation: Volume migrate was suspended or interrupted, and the destination group is not available at system reboot time.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9413 **Drive group *group_ID* encountered indeterminate data loss**

Explanation: The controller was running with write cache disabled due to user setting (batteryless mode enabled) and power was lost. On the next boot this RAID 5/6 group was marked uninitialized, but became degraded before the init completed.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

Volume alerts

The alerts in this section are generated to inform the operator of changes in volume status.

0500 **Volume *volume_ID* unrecoverable media error - One or more bad blocks created in LBA range *LBA1* to *LBA2***

Explanation: Due to unrecoverable media errors, bad blocks have been created on a volume within the reported LBA range.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: Rewrite the affected volume LBAs if possible.

0510 **Volume *volume_ID* mounted and mapped to host-*host_ID***

Explanation: Stale volume mounted.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

3500 **Volume *volume_ID* data redundancy error corrected**

Explanation: Redundancy scan found and corrected an incoherency in the parity data for the volume.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

5500 **Host-LUN mapping conflict while mounting drive group. Host:LUN *LUN* maps to Group:Volume *group_ID:volume_ID*.**

Explanation: LUN mapping conflict resolved during mount.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5501 **AutoHost overlap during mount of group *group_ID*. Volume *volume_ID* included for AutoHost *host_ID*.**

Explanation: Auto host overlap detected during mount.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

9503 **Host-LUN mapping conflict during mount of group *group_ID*. Host *host_ID* has no available LUNs for mapping volume *volume_ID*. Host LUN *LUN* mapping deleted.**

Explanation: Unresolvable LUN conflict.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Reconfigure LUN mapping.

9504 **Volume *volume_ID* dismounted with data in write cache**

Explanation: A transition to non-viable state occurred or volume was disorderly dismounted and the volume had at least one sector of unflushed dirty cache.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

9510 **Drive group *group_ID* maximum bad blocks exceeded - Volume *volume_ID* deleted**

Explanation: The Bad Block count for the drive group has exceeded the maximum value.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. The volume is deleted.

Operator response: Acknowledge to clear the alert immediately.

9511 **Volume *volume_ID* data redundancy error encountered - Bad blocks created in LBA range *LBA1* to *LBA2***

Explanation: Redundancy scan found and corrected incoherency, but created bad blocks.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Rewrite affected volume LBAs if possible.

9512 **Volume *volume_ID* migrate incomplete and source group is missing. Volume has been deleted.**

Explanation: Volume migrate was suspended or interrupted, and source group is not available at system reboot time.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately.

Host and connectivity alerts

The alerts in this section are generated to inform the operator of changes in host or connection status.

4601 **Controller host port connectivity error**

Explanation: Controller detected an unexpected loss of connectivity on an enabled host port.

- For a FibreChannel host port, this alert is generated when a link down condition is detected on the host port.
- For a SAS host port, this alert is generated when a 106x internal fault condition requires a 106x reset.
- This alert is not generated for an Apache host port.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the host port connectivity is restored.

Operator response: Replace the controller or host switch.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5600 **Illegal host *host_ID* access attempted**

Explanation: An invalid SCSI initiator port (host) has attempted to access the system.

- For a FibreChannel host port, this alert is generated when a PLOGI frame is received from a host that does not have any LUNs mapped to it.
- For all other types of host ports, this alert is generated when a SCSI command is received from a SCSI initiator port (host) that does not have any LUNs mapped to it.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears when the host becomes valid by being added to the system. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately. Add host and map LUN to allow access.

9600 Controller unable to bind - Usable drives different than survivor controller

Explanation: Unable to rebind with survivor due to missing drives that survivor can see or more drives than the survivor sees. Possible causes include drive or expander failures.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when the controller reboots and all drives are discovered properly.

Operator response: Repair drive connectivity.

9601 Controller reports RAID system unable to begin operations - Usable drives different in each controller

Explanation: Two controllers booting up see different drives, and neither controller can see all of the same drives as the other controller. Possible causes include drive or expander failures.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when controller reboots and all drives are discovered properly.

Operator response: Repair drive connectivity.

Controller configuration alerts

The alerts in this section are generated to inform the operator of problems related to controller configuration.

0700 Controller *controller_ID* configuration script *script_name* execution complete

Explanation: System configuration script has completed with no errors.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0701 Controller port *port_ID* IP address changed to *IP_address*

Explanation: Requested IP address applied.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0702 Controller timestamp updated

Explanation: Other controller and backplane timestamps are in sync, but the timestamp for this controller does not match.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0703 Controller identity updated

Explanation: Other controller and backplane WWNs match each other, but the WWN of this controller does not match them.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically.

Operator response: None.

0704 Survivor controller rebind complete - Controller redundancy restored

Explanation: Rebind sequence complete.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

0705 Controller configuration script *script_name* execution started.

Explanation: Configuration script started.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears automatically after 120 seconds.

Operator response: Acknowledge to clear the alert immediately.

5700 Controller configuration script *script_name* execution failed

Explanation: Configuration script execution failed.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail.

Operator response: Acknowledge to clear the alert immediately. Examine log files to identify errors in the configuration script.

5701 Foreign drive *drive_ID* detected and must be assimilated to become usable

Explanation: Discovered drive contains metadata from an incompatible RAID controller product.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when the drive is assimilated or removed.

Operator response: Assimilate or remove the incompatible drive.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5703 Drive *drive_ID* metadata version is incompatible with current controller firmware version

Explanation: Discovered drive contains incompatible metadata version.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is not notified of this alert by e-mail. Alert clears when one of the following events occurs:

- The drive is removed.
- The drive is assimilated.
- The controller reboots with compatible controller firmware.

Operator response: Assimilate or remove the drive, or update controller firmware.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

5710 Redundant drive group *group_ID* missing spare

Explanation: This redundant group has no viable spare.

System action: By default, the SAS RAID Module system information indicator is not turned on and the operator is not notified of this alert by e-mail. Alert clears when the drive group becomes degraded or has a viable spare.

Operator response: Configure a global spare drive for the group.

This alert can be masked so that it does not trigger the SAS RAID Module system information indicator.

9700 Controller configuration error - *error*

Explanation: The configuration file cannot be processed due to a syntax error, duplicate attribute, or unexpected end of file. Possible causes:

- A parameter file was manually edited.
- An incorrect parameter file was loaded.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when controller reboots.

Operator response: Perform the following steps:

1. Debug the configuration file.
2. Reboot the controller.
3. If the problem persists, perform a concurrent controller firmware update.

9703 Controller configuration error - *error*, **errno *error_number***

Explanation: Configuration file cannot be processed due to system I/O errors. Possible causes:

- A parameter file was manually edited.
- An incorrect parameter file was loaded.

System action: By default, the SAS RAID Module system information indicator is turned on and the operator is notified of this alert by e-mail. Alert clears when controller reboots.

Operator response: Perform the following steps:

1. Correct the problem.
2. Reboot the controller.
3. If the problem persists, perform a concurrent controller firmware update.

Understanding the logs

The alert history log file along with the ones listed in this topic can be used to view the information you need to diagnose and troubleshoot system events.

The IBM BladeCenter S SAS RAID Controller Module stores the alerts definition file as a text based .ini file which also stores user-modified email settings.

The following additional files can be used in conjunction with the alert history log file to provide information needed to diagnose RAID Controller configuration and run time errors:

Table 11. Configuration and Log Files

Header	Header
Online Log	History of controller state changes
System Configuration Log	Stores current RAID controller configuration when requested via API
CLI History & Config Script Logs	Stores history of CLI and script-drive configuration commands executed
Traces Log	Saves firmware debug trace information
Controller State Dump Log	Saves RSP register and data structure image

Capturing logs with the First Time Data Capture Utility

Use the First Time Data Capture Utility (FTDC Utility) to capture the software diagnostic files produced by your RAID Controller.

The FTDC Utility is a command line program that collects, in a single execution, a variety of support files from both RAID Controllers in the IBM BladeCenter S chassis. Support files are made up of the error logs, configuration files, and trace files, all of which contain vital information for maintaining the health of your system and for troubleshooting issues if they occur.

The collected files are aggregated into a single tar file. The tar file is named using the date, time and the IBM BladeCenter S chassis serial number. An example for a file collected on June 2, 2008 (20080602) at 3:17:42 PM (151742 in 24-hour time) from the RAID Controllers in IBM BladeCenter S chassis 23A6789 is as follows: 20080602.151742.23A6789.tar

Program versions for Windows and Linux

There are two versions of the program; one for the Windows environment and one for the Linux environment. The two program versions collect the same support files, and create tar files that are identical with the exception of timestamp information.

You can run the FTDC Utility program in any directory on a Windows or Linux workstation with a network connection to the IBM BladeCenter S chassis and the RAID Controllers within that chassis.

The FTDC Utility consists of three files that must all be installed in the same directory: The Windows version of the utility provides the three files in a self-extracting ZIP file named FTDCn.nn.EXE. The Linux version of the provides the

three files in a TAR file named FTDCn.nn.TAR. Locate the appropriate file on the internet or on the CD provided with your RAID Controller.

Download or copy the file into a directory you will use to run the program. If you are installing the FTDC Utility on a Windows PC, run the FTDCn.nn.EXE program to extract the files. If you are installing the FTDC Utility on a Linux workstation, run the TAR utility to extract the files.

In Windows, the First Time Data Capture Utility program file is named ftdc.exe. The corresponding file in Linux is named ftdc. The file transfer program FTX is named ftx.exe in Windows and ftx in Linux. Its associated file definitions are named fTXFileDefs (this name applies to both environments) and must be in the same directory as the FTDC Utility executable program.

FTDC Utility records its actions in a log file. For each execution of the program, It also records the starting time and the program version. As the FTDC Utility collects each group of files it records in the log, the files that were collected for that group. If there are no files for a file group, the FTDC Utility records that fact in the log as well. The log file contains a minimal amount of information for each execution of the utility. Information from consecutive executions of the FTDC Utility are appended to the file. If the file becomes too large, you can delete the file.

Note: Do not delete the log file while the FTDC Utility is running.

Command line parameters

This section describes the First Time Data Capture Utility command line parameters. If you input the **-help** parameter, or no parameters, the FTDC Utility displays the following usage message and takes no further action:

```
Usage:
ftdc -version
ftdc -help
ftdc -ip <adrs> [-allowoffline]
[-ldir <local dir>] [-log <file name>] [-pwd <password>]
```

The command line parameters presented in this message are:

-version

Displays the version number of the program. No other parameters are allowed on the command line when requesting the program version.

-help Displays the usage message. No other parameters are allowed on the command line when requesting program help.

-ip This parameter must be followed by the IP address of either controller in the IBM BladeCenter S chassis. The First Time Data Capture Utility automatically obtains the IP address of the other controller.

-allowoffline

If the user enters this parameter, the FTDC Utility examines the state of the two controllers. If either of the controllers is hung in an intermediate state for an extended period of time, the FTDC Utility forces the controller to restart, and then collects the resulting support information. The first time you run the FTDC Utility, run it without entering this parameter. In some situations, the utility directs you to halt host system I/O traffic, then re-invoke the FTDC Utility and enter this parameter. Keep in mind that the First Time Data Capture Utility may disrupt host I/O operation. Do not enter this parameter unless directed to do so by the program.

- ldir** This optional parameter supplies the name of a subdirectory where the program stores the tar file. If you do not supply the parameter, the program places the tar file in a subdirectory named `ftdc_files`.
- Note:** The directory name supplied with this parameter must be valid for the operating system in use (Windows or Linux).
- log** This optional parameter provides the name of a log file that contains FTDC Utility execution information. If you do not supply the parameter, the program logs information in a file named `ftdc.log`.
- pwd** Supply this parameter if the password for the controller has been changed. If you do not supply the parameter, the FTDC Utility uses the default parameter for the controller.

If you provide incorrect parameters or fail to provide a required parameter, the FTDC Utility displays the following usage message and makes no further attempt to communicate with the subsystem: Missing or unrecognized parameter name

```
Usage:
ftdc -version
ftdc -help
ftdc -ip <adrs> [-allowoffline]
-lldir <local dir>] [-log <file name>] [-pwd <password>]
```

Recorded information

The First Time Data Capture Utility records its actions in a log file. For each execution of the program, It also records the starting time and the program version. As the FTDC Utility collects each group of files it notes in the log the files that were collected for that group. If there are no files for a file group, the utility notes that fact in the log. The log file contains a minimal amount of information for each execution of the utility and information from consecutive executions of the program are appended to the file. If the file becomes too large, you can delete the file when the FTDC Utility is not running.

Usage examples: The following are command line parameters for collecting the files into the tar file and parameters for examining the resulting tar file:

Note: during operation, the FTX program writes messages to the console. In some cases, the messages seem to indicate a failure (for example, `ERR_INVALID_IP`); however, these messages are part of a normal operation and can be ignored. Examine the First Time Data Capture Utility log to determine if the utility and FTX programs are running as expected.

Examples:

This example collects support information using the default log subdirectory, default log file name, and default controller password: `ftdc -ip 172.31.19.181`

This command collects information in the `myfiles` directory. The FTDC Utility uses the default controller password. `ftdc -ip 172.31.19.181 -ldir myfiles`

This command collects information in the `ftdc_files` directory and records the program actions in a log named `mylog`. The FTDC Utility uses the default controller password. `ftdc -ip 172.31.19.181 -log mylog`

This command collects information in the `ftdc_files` directory and records the program actions in a log named `mylog`. FTDC Utility uses the default controller

password. The FTDC Utility forces either or both controllers to restart if necessary to collect the diagnostic information `ftdc -ip 172.31.19.181 -allowoffline -log mylog`.

Development and Support Option

If you encounter a situation that makes it necessary to force the controller firmware to restart and create the controller dump (CDUMP), you can enter the parameter **-forceoffline** at the command line.

Note: Do not enter the **-allowoffline** parameter when using the **-forceoffline** parameter. Example:

```
ftdc -ip 172.31.19.241 -forceoffline
```

CAUTION:

This option causes both controllers to reboot unconditionally and disrupts any host I/O traffic. Users should only enter this option when directed to do so by support personnel.

Non-concurrent repair procedures

Non-concurrent repair procedures must be performed only after all the application I/O processes are stopped. This section contains the non-concurrent repair procedures for the IBM BladeCenter S SAS RAID Controller Module.

Replacing a single controller using the CLI

Perform the following steps to non-concurrently replace a single RAID Controller using the RAID Controller command line interface (CLI).

Procedure

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Stop all host I/O application processes.
3. Remove any externally attached devices that are connected to any of the four SAS ports on the RAID Controller that is being replaced.
4. Log into the CLI of the RAID Controller.
5. At the <CLI> prompt, enter `list controller` and press Enter to verify the controllers are operating in a dual primary-secondary state.
<CLI> list controller

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	PRIMARY	1	0
1	Ctlr1	SECONDARY	1	0

6. At the <CLI> prompt, enter `shutdown -ctlr <CONTROLLER 0 OR 1> -state servicemode -readytoremove` and press Enter to prepare the controller for

service. The SlotID associated with alert 1101 indicates which controller should be prepared for service. The controller that is prepared for service will reboot in the SERVICE state.

```
<CLI> shutdown -ctlr 0 -state servicemode -readytoremove
Shutdown Command accepted.
```

7. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list and verify alert 2101 is in the list, or verify the amber LED on the controller is in the on SOLID state.

```
<CLI> alert -get
```

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2101	6	20090930162105	0	Info	5005076b0741417f	0	Unmasked
Msg: Controller ready for service – RAID system is down YK12J089A4BG							

8. Remove the RAID Controller.
 - a. Open the release handle on the RAID Controller (rotate the handle up) to disengage the RAID Controller from the bay.
 - b. Slide the RAID Controller out of the bay.
9. Insert the replacement RAID Controller.
 - a. Slide the RAID Controller into the same bay you removed the old RAID Controller.
 - b. Close the release handle (rotate the handle down).
10. Connect any externally attached devices that were previously connected to any of the four SAS ports on the RAID Controller.
11. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

Replacing a single controller using the SCM

Perform the following steps to non-concurrently replace a single RAID Controller using the IBM Storage Configuration Manager.

Procedure

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Stop all host I/O application processes.
3. Remove any externally attached devices that are connected to any of the four SAS ports on the RAID Controller that is being replaced.
4. Log into the IBM Storage Configuration Manager.
5. From the navigation panel, select **BC-S SAS RAID Module > Health > Physical View**.

6. Click **Controllers**.
7. Click the controller that you are replacing.
8. From the **Select a Controller Action** list, select **Service > Shutdown and Recover**.
9. From the **Select an Action** list, select **Shutdown to service mode and Prepare for removal**.
10. Select the controller you are replacing.
11. Read the information that displays and click **OK**.
12. From the navigation panel, select **BC-S SAS RAID Module > Health > Physical View**.
13. Click **Controllers**.
14. Select the **Alerts** tab.
15. Click **View alert** and verify alert 2101 is in the list, or verify that the amber LED on the controller is in the SOLID state.
16. Remove the RAID Controller.
 - a. Open the release handle on the RAID Controller (rotate the handle up) to disengage the RAID Controller from the bay.
 - b. Slide the RAID Controller out of the bay.
17. Insert the replacement RAID Controller.
 - a. Slide the RAID Controller into the same bay you removed the old RAID Controller.
 - b. Close the release handle (rotate the handle down).
18. Select the **Properties** tab and verify the controller status is Normal (Online).
19. Ensure that no additional warnings or critical alerts are generated for the replacement controller.
20. Connect any externally attached devices that were previously connected to any of the four SAS ports on the RAID Controller.
21. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

Results

If the problem is not resolved, collect the logs and contact IBM.

Replacing both controllers

To non-concurrently replace both RAID Controllers, perform the following steps.

Procedure

1. Stop all host I/O applications and power off the host servers.
2. Use the Advanced Management Module to power off both SAS RAID Modules.
 - a. Log into the Advanced Management Module.
 - b. Select **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select both I/O module bays (3 and 4).
 - d. Select **Power Off Module(s)**.
 - e. Click **OK**. The SAS RAID Modules are powered off.
 - f. Verify that the word **Off** is displayed in the **Pwr** column, indicating that the failed SAS RAID Modules are now powered off.
3. Remove the failed SAS RAID Modules.
 - a. Open the release handle on each SAS RAID Module (rotate the handle up) to disengage the SAS RAID Module from the bay.
 - b. Slide each SAS RAID Module out of the bay.
4. Install the replacement SAS RAID Modules.
 - a. Slide a SAS RAID Module into each bay (3 and 4).
 - b. Close each release handle (rotate the handle down).
5. Wait at least five minutes for the replacement SAS RAID Modules to come online.
6. Verify that the replacement SAS RAID Modules are now online.
 - a. Log into the Advanced Management Module.
 - b. Select **I/O Module Tasks > Admin/Power/Restart**.
 - c. Verify that the word **On** is displayed in the **Pwr** column.
7. Verify that the SAS RAID Modules are operating in a dual configuration mode.
 - a. Log into IBM Storage Configuration Manager.
 - b. Select **BCS SAS RAID Module > Health > All Resources**.
 - c. Verify that the status is **Normal (Online)**.
8. Check the SAS Switch firmware level of each SAS RAID Module.
 - a. Log into IBM Storage Configuration Manager.
 - b. Select **BCS SAS RAID Module > Service > Update Firmware**.
 - c. Next to **Current Device**, select the bay of the replacement SAS RAID Module .
 - d. Under **Current Firmware Bundle Level**, ensure that the type is **SAS Switch** and make a note of the level.
 - e. Next to **Current Device**, select the bay of the operational (survivor) SAS RAID Module.
 - f. Under **Current Firmware Bundle Level**, ensure that the type is **SAS Switch** and make a note of the level.
9. If the firmware levels are not equivalent, manually update the firmware level of the backlevel controller (see "Updating controller firmware" on page 164).
10. Verify that the SAS RAID Modules are operating in a dual configuration mode.

- a. Log into IBM Storage Configuration Manager.
 - b. Select **BCS SAS RAID Module > Health > All Resources**.
 - c. Verify that the status is **Normal (Online)**.
11. If the problem is not resolved, collect the logs and contact IBM.

Replacing 6-Disk storage module with 12-Disk Storage Module from Command Line Interface (CLI)

About this task

6-Disk Storage Module (DSM) is the enclosure holding up to six disk drives while 12-Disk Storage Module holding up to 12 disk drives. 12-DSM is supported in the BladeCenter S chassis only with a minimum SAS RAID Controller(RSSM) Firmware code level 1.3.0.008. Both controllers are required to update the FW newer than version 1.3.0.008 before 12-DSM installation. Perform the following steps to non-concurrently replace the 6-DSM with 12-DSM installation.

Procedure

1. Log in to the RAID Controller Command Line Interface(CLI).
2. Confirm both controllers are in a minimum FW code level of 1.3.0.008. Update the SAS RAID controller firmware to code level higher than or equal to version 1.3.0.008. The firmware update procedure please refer to *IBM SAS RAID Controller Module Installation and User's Guide* in Chapter 6, "Updating firmware," on page 31

At the <CLI> prompt, enter swversion and press Enter to list the controllers firmware version. The Package Build No should be no older than 1.3.0.008.

```
<CLI> swversion
Current Machine Local Time: 03/04/2013 04:57:44 PM
```

```
Software version      : 3.0.0.6
UBoot version         : H-1.1.4.6
OS version            : H-2.4.20.12
SES version           : 0107
BMC version           : S0BT10A    0121 02/08/2010
FPGA version          : 01.07
CPLD version          : S0CP00A    C00A 01/01/2000
SAS switch version    : S0SW01D    R107 12/17/2009
BBU FirmwareRev       : 58.0
Package Build No      : 1.3.0.008
```

3. At IBM SAS RAID controller Command Line Interface(CLI) prompt, enter shutdown -system -state servicemode and press Enter to prepare the controller for service. The controller that is prepared for service will reboot in the SERVICE state.

```
<CLI> list controller
Current Machine Local Time: 03/04/2013 04:37:02 PM
```

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	PRIMARY	1	0
1	Ctlr1	SECONDARY	1	0

```
<CLI> shutdown -system -state servicemode
Current Machine Local Time: 03/04/2013 04:37:16 PM
Shutdown Command Successful
```

<CLI>

Broadcast message from root Mon Mar 4 16:37:19 2013...

The system is going down for reboot NOW !!

Log in the CLI prompt again and confirm both controllers are in SERVICE state.

<CLI> list controller

Current Machine Local Time: 03/04/2013 04:39:12 PM

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	SERVICE	1	--
1	Ctlr1	SERVICE	1	--

4. Remove the 6-DSM from the chassis.
 - a. Open the release handles on the DSM (rotate the top handle up and the bottom handle down) to disengage the DSM from the IBM BladeCenter S chassis.
 - b. Slide the DSM out of the IBM BladeCenter S chassis.
5. Insert the replacement 12-DSM in the chassis.
 - a. Slide the DSM into the storage module bay until it stops.
 - b. Close the release handles (rotate the top handle down and the bottom handle up).
6. Enter list enclosure and press Enter to list the firmware version of the DSM. If the firmware level of the replacement DSM is not higher than or equal to 7.15, alert 5014 will generate to indicate that the DSM firmware versions are not equivalent. To resolve this condition and clear the alert, perform a non-concurrent system reboot or non-concurrent firmware update.

<CLI> list enclosure

Current Machine Local Time: 03/04/2013 05:05:24 PM

Encl#	Enclosure	Type	Version	Status
0	Encl0	Controller	0107	Good
1	Encl1	DSM SFF	7.15	Good
2	Encl2	DSM SFF	7.15	Good

7. Enter mountstate -getobject -enclosure and press Enter to list the mount state of the DSMs. Ensure that each DSM is online.

<CLI> mountstate -getobject -enclosure

Current Machine Local Time: 03/04/2013 05:15:22 PM

Enclosure#	State	Type
0	Online	Controller
1	Online	DSM SFF
2	Online	DSM SFF

8. Enter list drive and press Enter to list the drive summary for each disk drive configured in the storage pool. Ensure that the mount state of all disk drives inside the replacement DSM are in the online state.

Updating controller firmware

To manually update the firmware of a SAS RAID Module, perform the following steps.

Procedure

1. Download the SAS Switch firmware.
 - a. Log into IBM Storage Configuration Manager.
 - b. Select **BCS SAS RAID Module > Service > Update Firmware**.
 - c. Next to **Current Device**, select the bay of the affected SAS RAID Module.
 - d. Under **Download Firmware Bundle**, click **Check web for latest available updates**.
 - e. Under **Popular links**, click **Software and device drives**.
 - f. Under **IBM BladeCenter** click **BladeCenter S**
 - g. Click on **Serial attached SCSI (SAS)**.
 - h. Next to **SAS Connectivity Module firmware – IBM BladeCenter**, click the version number.
 - i. Under **File link**, click the .zip link next to **SAS Connectivity Module firmware**.
 - j. Under **Transfer protocol**, select **FTP**.
 - k. Click **I agree** to accept the terms and conditions.
 - l. Save the ZIP file on your local workstation.
 - m. Unzip the file.
2. Put the SAS RAID Modules into service mode.
 - a. At the top of the Update Firmware page, click **Shutdown & Recover**.
 - b. Select **Shut down to service mode**.
 - c. Select **Both Controller 1 and 2**.
 - d. Click **OK**.
 - e. Read the Confirmation Message and click **OK**.
 - f. Verify that the following message is displayed at the top of the Shutdown and Recover page: The controllers were successfully shut down to service mode. Continue to the Update Firmware page to proceed with your firmware update. This message indicates that the SAS RAID Modules are in service mode.
 - g. At the top of the Shutdown and Recover page, click **Update Firmware**.
3. Update the SAS Switch firmware on the affected SAS RAID Module.
 - a. Next to **Current Device**, select the location of the affected SAS RAID Module.
 - b. Click **Browse**.
 - c. Select the FUF file from the ZIP file.
 - d. Click **Open**.
 - e. Click **Install**.
 - f. Read the Confirmation Message and click **OK**.
4. Verify that the following message is displayed at the top of the Update Firmware page: Firmware update has completed successfully. If both SAS Switches are now up to date, RAID controllers need to be rebooted to come back online. Go to Shutdown and Recover page to reboot both controllers. This message indicates that the SAS Switch firmware update completed successfully.

5. Bring the SAS RAID Modules online.
 - a. At the top of the Update Firmware page, click **Shutdown and Recover**.
 - b. Select **Bring online from service mode**.
 - c. Select **Controller 1**.
 - d. Read the Confirmation Message and click **OK**.
 - e. Select **Bring online from service mode**.
 - f. Select **Controller 2**.
 - g. Read the Confirmation Message and click **OK**.

Replacing a Disk Storage Module (non-concurrent procedure)

A Disk Storage Module (DSM) is an enclosure holding up to six disk drives. Perform the following steps to non-concurrently replace a DSM.

About this task

Important: When installing disk drives in the replacement DSM, ensure that you insert each drive in the same slot that it occupied in the previous DSM. If at least one IBM BladeCenter SAS Connectivity Module is installed in the IBM BladeCenter S chassis, the location of each drive is determined by the IBM BladeCenter SAS Connectivity Module zoning configuration that you have selected for the IBM BladeCenter S system. The RAID Controller reports any observed change in drive position. Modifying the position of any drive can cause the system to disarm any replacement detection mechanisms that may have been armed by a previous drive failure or drive removal.

Procedure

1. From IBM Storage Configuration Manager, select **BC-S SAS RAID Module > Health > Active Alerts** to view active alerts associated with RAID devices.
2. Select any alerts associated with the DSM to display the alert details at the bottom of the page.
3. Scroll down to the operator response and click **Replace Disk Storage Module(s)**.
4. Stop all host I/O applications and power off the host servers.
5. Use the Advanced Management Module to power off each RAID Controller.
 - a. Log into the Advanced Management Module.
 - b. Click **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select the check box next to Bay 3 and Bay 4.
 - d. Select **Power Off Module(s)**.
 - e. Click **OK** and wait until each RAID Controller is powered off. The word **Off** is displayed in the **Pwr** column.
6. Before removing any drives, record the position of each drive in the DSM.
7. Remove each drive from the DSM.
 - a. Open the release handle on the disk drive (rotate the handle up) to disengage the hard disk drive from the DSM.
 - b. Slide the hard disk drive out of the DSM.
8. Remove the DSM.
 - a. Open the release handles on the DSM (rotate the top handle up and the bottom handle down) to disengage the DSM from the IBM BladeCenter S chassis.

- b. Slide the DSM out of the IBM BladeCenter S chassis.
9. Install the replacement DSM.
 - a. Slide the DSM into the storage module bay until it stops.
 - b. Close the release handles (rotate the top handle down and the bottom handle up).
10. Install each drive in the replacement DSM. Refer to your record of drive positions to ensure that you install each drive in the same position.
 - a. Slide the drive into the DSM storage module bay until it stops.
 - b. Close the release handles (rotate the top handle down and the bottom handle up).
11. Use the Advanced Management Module to power on each RAID Controller.
 - a. Log into the Advanced Management Module.
 - b. Click **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select the check box next to Bay 3 and Bay 4.
 - d. Select **Power On Module(s)**.
 - e. Click **OK** and wait until each RAID Controller are powered on. The word **On** is displayed in the **Pwr** column.

What to do next

If the problem is not resolved, collect the logs and contact IBM.

Replacing a media tray

Perform the following steps to non-concurrently replace the IBM BladeCenter S chassis media tray with the SAS RAID Module feature installed.

Procedure

1. View the SAS RAID Module Active Alert List and select the alerts associated with the Media Tray resource. The alert details are at the bottom of the page.
2. Scroll down to the operator response and click **Replace Media Tray**.
3. Stop all host I/O applications and power off the host servers.
4. Use the Advanced Management Module to power off both SAS RAID Modules.
 - a. Log into the Advanced Management Module.
 - b. Click **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select the check box next to Bay 3 and Bay 4.
 - d. Select **Power Off Module(s)**.
 - e. Click **OK**.
 - f. Wait until both SAS RAID Modules are powered off. The word **Off** is displayed in the **Pwr** column.
5. Make a note of the current SAS RAID Module **IP Settings**, and any custom passwords.
 - a. Click **I/O Module Tasks > Configuration**.
 - b. Click **Bay 3** under **I/O Module Configuration**.
 - c. Make a note of the **Current IP Configuration** for SAS Switch Subsystem. The values to note are:
 - IP Address
 - Subnet Mask

- Gateway
- d. Make a note of the **Current IP Configuration** for RAID Controller Subsystem. The values to note are:
 - Configuration Method
 - IP Address
 - Subnet Mask
 - Gateway Address
 - VLAN ID
- e. Click **Bay 4** under **I/O Module Configuration**.
- f. Make a note of the **Current IP Configuration** for SAS Switch Subsystem. The values to note are:
 - IP Address
 - Subnet Mask
 - Gateway
- g. Make a note of the **Current IP Configuration** for RAID Controller Subsystem. The values to note are:
 - Configuration Method
 - IP Address
 - Subnet Mask
 - Gateway Address
 - VLAN ID
- 6. Remove each Battery Backup Unit from the Media Tray.
 - a. Open the release handle (rotate the handle down).
 - b. Slide the Battery Backup Unit out of the media tray.
- 7. Remove the Media Tray from the chassis.
 - a. Open the release handles (rotate the top handle up and the bottom handle down) to disengage the media tray from the IBM BladeCenter S chassis.
 - b. Slide the media tray out of the IBM BladeCenter S chassis.

Note: When you remove the media tray, the fan modules begin to run at full speed.
- c. If you are instructed to return the media tray or DVD drive, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.
- 8. Insert the new Media Tray into the chassis.
 - a. Slide the media tray into the IBM BladeCenter S chassis until it stops.
 - b. Close the release handles (rotate the top handle down and the bottom handle up).
- 9. Insert each Battery Backup Unit into the new Media Tray.
 - a. Slide the Battery Backup Unit into the media tray.
 - b. Close the release handle (rotate the handle up).
- 10. Reset the factory default settings for the SAS Switch in bay 3.
 - a. Click **I/O Module Tasks > Configuration**.
 - b. Click **Bay 3** under **I/O Module Configuration**.
 - c. Click **Advanced Configuration** under **Bay 3 (SAS RAID Ctlr Mod)**.
 - d. Click **Restore Factory Defaults** under **Advanced Configuration** for I/O Module 3.

- e. Click **Restore Defaults**.
 - f. Click **OK**.
 - g. Click **OK**.
11. Power on the SAS RAID Module in Bay 4.
 - a. Click **I/O Module Tasks > Admin/Power/Restart**.
 - b. Select the check box next to **Bay 4**.
 - c. Select **Power On Module(s)**.
 - d. Click **OK**.
 12. Verify that both SAS RAID Modules powered on. The word **On** is displayed in the **Pwr** column for both SAS RAID Modules.

What to do next

If this process does not resolve the problem, collect the logs and contact IBM.

Concurrent repair procedures

Concurrent repair procedures can be performed even if application I/O processes are running. This section contains the concurrent repair procedures for the IBM BladeCenter S SAS RAID Controller Module.

Note: Before you perform a concurrent repair procedure, make sure the firmware level of your RAID controllers is 1.2.2.007 or newer.

Replacing a single controller in a dual controller configuration using the CLI

Perform the following steps to concurrently replace a single RAID Controller in a dual controller configuration using the RAID Controller command line interface (CLI).

Procedure

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the **SOLID** or **BLINKING** state.
2. Remove any externally attached devices that are connected to any of the four SAS ports on the RAID Controller that is being replaced.
3. Log into the CLI of the RAID Controller.
4. At the <CLI> prompt, enter `list controller` and press Enter to verify the controllers are operating in a dual primary-secondary state.
<CLI> list controller

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	PRIMARY	1	0
1	Ctlr1	SECONDARY	1	0

5. At the <CLI> prompt, enter `shutdown -ctlr <CONTROLLER 0 OR 1> -state servicemode -readytoremove` and press Enter to prepare the controller for

service. The SlotID associated with alert 1101 indicates which controller should be prepared for service. The controller that is prepared for service will reboot in the SERVICE state.

```
<CLI> shutdown -ctlr 0 -state servicemode -readytoremove
Shutdown Command accepted.
```

6. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list and verify alert 2100 is in the list, or verify the amber LED on the controller is in the on SOLID state.

```
<CLI> alert -get
```

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2100	6	20090930162105	0	Info	5005076b0741417f	0	Unmasked
Msg: Controller ready for service YK12J089A4BG							

7. Remove the RAID Controller.
 - a. Open the release handle on the RAID Controller (rotate the handle up) to disengage the RAID Controller from the bay.
 - b. Slide the RAID Controller out of the bay.
8. Insert the replacement RAID Controller.
 - a. Slide the RAID Controller into the same bay you removed the old RAID Controller.
 - b. Close the release handle (rotate the handle down).
9. The replacement controller's firmware levels will be automatically updated to the same firmware levels running on the survivor controller. Depending on the state of the system, this may take several minutes to complete
10. Connect any externally attached devices that were previously connected to any of the four SAS ports on the RAID Controller.
11. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

Results

If the problem is not resolved, collect the logs and contact IBM.

Replacing a single controller in a dual controller configuration using the SCM

Perform the following steps to concurrently replace a single RAID Controller in a dual controller configuration using the IBM Storage Configuration Manager.

Procedure

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Remove any externally attached devices that are connected to any of the four SAS ports on the RAID Controller that is being replaced.
3. Log into the IBM Storage Configuration Manager.
4. From the navigation panel, select **BC-S SAS RAID Module > Health > Physical View**.
5. Click **Controllers**.
6. Click the controller that you are replacing.
7. From the **Select a Controller Action** list, select **Service > Shutdown and Recover**.
8. From the **Select an Action** list, select **Shutdown to service mode and Prepare for removal**.
9. Select the controller you are replacing.
10. Read the information that displays and click **OK**.
11. From the navigation panel, select **BC-S SAS RAID Module > Health > Physical View**.
12. Click **Controllers**.
13. Select the **Alerts** tab.
14. Click **View alert** and verify alert 2100 is in the list, or verify that the amber LED on the controller is in the SOLID state.
15. Remove the RAID Controller.
 - a. Open the release handle on the RAID Controller (rotate the handle up) to disengage the RAID Controller from the bay.
 - b. Slide the RAID Controller out of the bay.
16. Insert the replacement RAID Controller.
 - a. Slide the RAID Controller into the same bay you removed the old RAID Controller.
 - b. Close the release handle (rotate the handle down).
17. The replacement controller's firmware levels will be automatically updated to the same firmware levels running on the survivor controller. Depending on the state of the system, this may take several minutes to complete.
18. Select the **Properties** tab and verify the controller status is Normal (Online).
19. Ensure that no additional warnings or critical alerts are generated for the replacement controller.
20. Connect any externally attached devices that were previously connected to any of the four SAS ports on the RAID Controller.

21. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

Results

If the problem is not resolved, collect the logs and contact IBM.

Replacing a failed drive

About this task

To replace a failed hard disk drive, perform the following steps.

Attention: Back up the data before replacing a failed hard drive.

Procedure

1. Using IBM Storage Configuration Manager, view the SAS RAID Controller Active Alert List and select the alerts associated with the failed drive. The alert details are displayed at the bottom of the page.
2. Scroll down to the operator response and click **Replace Hard Disk Drive**.
3. Identify the failed drive.
 - a. Select **BCS SAS RAID Module > Health > Physical View**.
 - b. Select the drive that has the information icon underneath it.
 - c. Click the **Alerts** tab to view the drive alert.
 - d. Click **Select a Disk Action > Service > Locate Hardware**. The amber LED on the failed drive begins blinking.
 - e. Make a note of the position of the failed drive.
 - f. Click **Stop** on the **Locate Disk Drive** message box.
4. Remove the failed drive.
 - a. Open the release handle on the hard disk drive (rotate the handle up) to disengage the hard disk drive from the drive enclosure.
 - b. Slide the hard disk drive out of the drive enclosure.
5. Wait at least two minutes before inserting the replacement drive.
6. Insert the new drive into the same position.
 - a. Slide the hard disk drive into the drive enclosure.
 - b. Close the release handle (rotate the handle down).
7. Wait two minutes before verifying that the replaced drive is operational.
8. To verify that the alerts related to the failed drive are no longer in the Active Alert List, select **BCS SAS RAID Module > Health > Active Alerts**.
9. If the problem is not resolved, collect the logs and contact IBM.

Replacing a Disk Storage Module

This section describes the concurrent repair procedure to replace a Disk Storage Module (DSM) in an IBM BladeCenter S chassis.

About this task

A DSM is an enclosure holding up to six disk drives. Concurrent DSM replacement is only supported with RAID 1 and RAID 10 configurations where storage pool enclosure redundancy has been configured. You can also concurrently replace a DSM if there are no storage pools using the disk drives in the DSM. You can verify storage pool enclosure redundancy by reviewing the detail pool data using the RAID Controller command line interface (CLI) or the IBM Storage Configuration Manager.

Note: If your DSM does not meet the requisites for concurrent replacement, follow the steps in “Replacing a Disk Storage Module (non-concurrent procedure)” on page 165.

Perform the following steps to concurrently replace a DSM using the RAID Controller CLI. Information enclosed in “<>” is specific to the local system configuration.

Procedure

1. Log in to the RAID Controller CLI.
2. At the <CLI> prompt, enter `list pool` and press Enter to list the summary for each storage pool. Ensure the storage pool is not degraded and the status is viable.

```
<CLI> list pool
Current Machine Local Time: 09/15/2009 02:06:46 PM
```

Pool#	ID	Name	RaidType	OwnerCtlr	TotalCap	AvailCap	Status	State	Degraded
0	1	RAID10_Pool	10	Slot 1	2095GB	1975GB	Viable	ONV	No

```
State: OFN/SN=Offline Non-viable/Service Non-viable
ONF/OFF/SF=Online Failed/Offline Failed/ Service Failed
ONV/OFV/SV= Online Viable/Offline Viable/Service Viable
```

ONN=Online Non-viable/Pending Non-Viable; one or more drives are missing in this pool.

The pool state changes to ONV if missing drive(s) comes back to the pool.
The pool state changes to OFN if the user acknowledges the alert.

3. Enter `detail pool -name <STORAGE_POOL_NAME>` and press Enter to list the detailed information for the storage pool. For the <STORAGE_POOL_NAME>, use the storage pool name shown in the `list pool` output from the previous step. The number of disk drives configured for the storage pool must be equivalent between the primary and secondary section, and evenly distributed between each DSM. In the following example, six disk drives are configured in a RAID10 storage pool configuration. Three disk drives in the primary section are in DSM 2, and three drives in the secondary section are in DSM 1.

```
<CLI> detail pool -name RAID10_Pool
Current Machine Local Time: 09/15/2009 02:07:13 PM
```

ID	Name	RaidType	OwnerCtlr	TotalCap	AvailCap	Status	State	Degraded
1	RAID10_Pool	10	Slot 1	2095GB	1975GB	Viable	ONV	No

State: OFN/SN=Offline Non-viable/Service Non-viable
ONF/OFF/SF=Online Failed/Offline Failed/ Service Failed
ONV/OFV/SV= Online Viable/Offline Viable/Service Viable

The pool state changes to OFN if the user acknowledges the alert.

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ct10	Ct11	RPM	FW level
0	2:1	9QK0SWEJ	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
1	2:2	9QK0QCJB	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
2	2:3	9QK0QC50	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ct10	Ct11	RPM	FW level
0	1:1	9QK0SWLM	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
1	1:2	9QK0V0ZB	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
2	1:3	9QK0HQ9V	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D

Volumes	Cap	GrpName	RaidType	Status
RAID10_Pool:RAID10_VOL1	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL2	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL3	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL4	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL5	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL6	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL7	15GB	RAID10_Pool	10	VBL INI
RAID10_Pool:RAID10_VOL8	15GB	RAID10_Pool	10	VBL INI

- Current Machine Local Time: 09/15/2009 02:07:53 PM

Drive E:T is Enclosure:Tray; tray numbers start at 1, and tray 1 is the uppermost tray.

Chapter 11. Troubleshooting and support 173

FOR=foreign LCS/SLS=current/stale local spare
 CBL/SCL=current/stale auto-copy-back local spare
 GLS/SGS=current/stale global spare
 CBG/SCG=current/stale auto-copy-back global spare

State: OK=healthy M=missing P=PFA predicted failure
 U=unreliable (M/P/U can be combined)
 INI=initialized UNS=unsupported (non-IBM) drive PM=path missing
 IMD=incompatible metadata with this software version; either assimilate drive or
 update controller firmware.
 UNF=firmware version unsupported for drive

5. Enter mountstate -getobject -enclosure and press Enter to list the mount state of the DSM that is being replaced. Ensure that each DSM is online.

```
<CLI> mountstate -getobject -enclosure
Current Machine Local Time: 09/15/2009 02:08:29 PM
```

Enclosure#	State	Type
0	Online	Controller
1	Online	DSM
2	Online	DSM

6. Enter list enclosure and press Enter to display the firmware version of the DSMs. Record the firmware version of each DSM.

```
<CLI> list enclosure
Current Machine Local Time: 09/15/2009 02:09:06 PM
```

Encl#	Enclosure	Type	Version	Status
0	Encl0	Controller	0107	Good
1	Encl1	DSM	1.08	Good
2	Encl2	DSM	1.08	Good

7. Enter mountstate -setobject -dismount -enclosure 1 -okdegraded and press Enter to dismount the DSM that you will replace. The RAID controller prepares the DSM for service by dismounting the DSM and the disk drives inside the DSM.

```
<CLI> mountstate -setobject -dismount -enclosure 1 -okdegraded
Current Machine Local Time: 09/15/2009 02:16:00 PM
Set Enclosure MountState successful
```

8. Enter alert - get and press Enter to query the active alert list. Ensure alert 2000 was generated for the DSM that was dismounted, and ensure alert 2300 was generated for each disk drive in the DSM that was dismounted.

```
<CLI> alert -get
Current Machine Local Time: 09/15/2009 02:16:27 PM
Existing Alerts :
```

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2000	21	20090915141600	0	Info	5005076b0741417f	0	Unmasked
Msg: Dismounted drive enclosure 1 ready to remove							
2300	38	20090915141523	1	Info	5005076b0741417f	0	Unmasked
Msg: Drive 01:01 ready for removal							
2300	40	20090915141523	1	Info	5005076b0741417f	0	Unmasked
Msg: Drive 01:02 ready for removal							
2300	39	20090915141523	1	Info	5005076b0741417f	0	Unmasked

Msg: Drive 01:03 ready for removal								

2300	17	20090915141522	0		Info	5005076b0741417f	0	Unmasked

Msg: Drive 01:04 ready for removal								

2300	18	20090915141522	0		Info	5005076b0741417f	0	Unmasked

Msg: Drive 01:05 ready for removal								
2300	16	20090915141522	0		Info	5005076b0741417f	0	Unmasked

Msg: Drive 01:06 ready for removal								

9. Verify the Amber Fault LED is on and in the SOLID state for the DSM that is being replaced and for each disk drive inside the DSM. For information on LED states, see "Understanding LEDs" on page 101.
10. Enter list drive and press Enter to list the drive summary for each disk drive configured in the storage pool. In the DSM that you are replacing, ensure that the mount state of all the disk drives are in the service state.

<CLI> list drive

Current Machine Local Time: 09/15/2009 02:17:29 PM

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ctl0	Ctl1	RPM	FW level
0	1:1	9QK0SWLM	698GB	--	UNA	OK	Service	1	1	7200	BC1D
1	1:2	9QK0VOZB	698GB	--	UNA	OK	Service	1	1	7200	BC1D
2	1:3	9QK0HQ9V	698GB	--	UNA	OK	Service	1	1	7200	BC1D
3	1:4	9QK0QCGS	698GB	--	UNA	OK	Service	1	1	7200	BC1D
4	1:5	9QK0HQ74	698GB	--	UNA	OK	Service	1	1	7200	BC1D
5	1:6	9QK0QCEQ	698GB	--	UNA	OK	Service	1	1	7200	BC1D
6	2:1	9QK0SWEJ	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
7	2:2	9QK0QCJB	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
8	2:3	9QK0QC50	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
9	2:4	9QJ1NG5W	931GB	--	UNA	OK	Online	1	1	7200	BC1D
10	2:5	9QK0SWLY	698GB	--	UNA	OK	Online	1	1	7200	BC1D
11	2:6	9QK0QC85	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D

Drive E:T is Enclosure:Tray; tray numbers start at 1, and tray 1 is the uppermost tray.

Usage: UNA=unassigned GRP/SGR=current/stale group member
FOR=foreign GLS/SGS=current/stale global spare
CBG/SCG=current/stale auto-copy-back global spare

State: OK=healthy M=missing P=PFA predicted failure
U=unreliable (M/P/U can be combined)
INI=initialized UNS=unsupported (non-IBM) drive PM=path missing
IMD=incompatible metadata with this software version; either assimilate drive
or update controller firmware.
UNF=firmware version unsupported for drive

11. Enter list pool and press Enter to list the pool summary for each storage pool. Ensure that the state of the storage pool is online and viable.

<CLI> list pool

Current Machine Local Time: 09/15/2009 02:17:49 PM

Pool#	ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
0	1	RAID10_Pool	10	Slot 1	2095GB	1975GB	Degraded -InTransition	ONV	Yes

State: OFN/SN=Offline Non-viable/Service Non-viable
ONF/OFF/SF=Online Failed/Offline Failed/ Service Failed

ONV/OFV/SV= Online Viable/Offline Viable/Service Viable

ONN=Online Non-viable/Pending Non-Viable; one or more drives are missing in this pool.

The pool state changes to ONV if missing drive(s) comes back to the pool.

The pool state changes to OFN if the user acknowledges the alert.

12. Remove the DSM from the chassis.

- Open the release handles on the DSM (rotate the top handle up and the bottom handle down) to disengage the DSM from the IBM BladeCenter S chassis.
- Slide the DSM out of the IBM BladeCenter S chassis.

13. Record the slot position of each disk drive, then remove each disk drive from the DSM.

- Open the release handle on the disk drive (rotate the handle up) to disengage the hard disk drive from the DSM.
- Slide the hard disk drive out of the DSM.

14. Enter alert -get and press Enter to query the active alert list. Ensure alert 0003 was generated for the DSM that was removed from the chassis.

<CLI> alert -get

Current Machine Local Time: 09/15/2009 02:20:38 PM

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
3	22	20090915141947	0	Info	5005076b0741417f	1	Masked
Msg: Drive enclosure 1 removed							

15. Insert each disk drive in the same slot position of the replacement DSM. You do not need to place each disk drive back in the same slot position of the replacement DSM, however, it is a good practice to do so.

- Slide the drive into the DSM storage module bay until it stops.
- Close the release handles (rotate the top handle down and the bottom handle up).

16. Insert the replacement DSM in the chassis.

- Slide the DSM into the storage module bay until it stops.
- Close the release handles (rotate the top handle down and the bottom handle up).

17. Enter alert -get and press Enter to query the active alert list. Ensure alert 0002 was generated for inserting the replacement DSM in the chassis.

<CLI> alert -get

Current Machine Local Time: 09/15/2009 02:21:53 PM

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2	42	20090915142137	0	Info	5005076b0741417f	1	Masked
Msg: Compatible drive enclosure 1 found							

18. Enter list enclosure and press Enter to list the firmware version of the DSM. If the firmware level of the replacement DSM is not the same as the previous DSM, alert 5014 will generate to indicate that the DSM firmware versions are not equivalent. To resolve this condition and clear the alert, perform a non-concurrent system reboot or non-concurrent firmware update.

<CLI> list enclosure
Current Machine Local Time: 09/15/2009 02:22:06 PM

Encl#	Enclosure	Type	Version	Status
0	Encl0	Controller	0107	Good
1	Encl1	DSM	1.06	Good
2	Encl2	DSM	1.08	Good

19. Enter mountstate -getobject -enclosure and press Enter to list the mount state of the DSMs. Ensure that each DSM is online.

<CLI> mountstate -getobject -enclosure
Current Machine Local Time: 09/15/2009 02:23:46 PM

Enclosure#	State	Type
0	Online	Controller
1	Online	DSM
2	Online	DSM

20. Enter list drive and press Enter to list the drive summary for each disk drive configured in the storage pool. Ensure that the mount state of all disk drives inside the replacement DSM are in the online state.

<CLI> list drive
Current Machine Local Time: 09/15/2009 02:25:04 PM

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ct10	Ct11	RPM	FW level
0	1:1	9QK0SWLM	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
1	1:2	9QK0V0ZB	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
2	1:3	9QK0HQ9V	698GB	--	GLS	OK	Online	1	1	7200	BC1D
3	1:4	9QK0QCGS	698GB	--	UNA	OK	Online	1	1	7200	BC1D
4	1:5	9QK0HQ74	698GB	--	UNA	OK	Online	1	1	7200	BC1D
5	1:6	9QK0QCEQ	698GB	--	UNA	OK	Online	1	1	7200	BC1D
6	2:1	9QK0SWEJ	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
7	2:2	9QK0QCJB	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
8	2:3	9QK0QC50	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D
9	2:4	9QJ1NG5W	931GB	--	UNA	OK	Online	1	1	7200	BC1D
10	2:5	9QK0SWLY	698GB	--	UNA	OK	Online	1	1	7200	BC1D
11	2:6	9QK0QC85	698GB	RAID10_Pool	GRP	OK	Online	1	1	7200	BC1D

Drive E:T is Enclosure:Tray; tray numbers start at 1, and tray 1 is the uppermost tray.

Usage: UNA=unassigned GRP/SGR=current/stale group member
FOR=foreign GLS/SGS=current/stale global spare
CBG/SCG=current/stale auto-copy-back global spare

State: OK=healthy M=missing P=PFA predicted failure
U=unreliable (M/P/U can be combined)
INI=initialized UNS=unsupported (non-IBM) drive PM=path missing
IMD=incompatible metadata with this software version; either assimilate drive
or update controller firmware.
UNF=firmware version unsupported for drive

What to do next

If the problem is not resolved, collect the logs and contact IBM.

Removing and reinserting an active controller

You can resolve some software problems associated with an IBM BladeCenter S SAS RAID Controller Module by removing and reinserting the same RAID Controller without significant interruption to the server.

Important:

- Do not remove a RAID Controller if it is the only functioning RAID Controller in the chassis. Removing the only functional RAID Controller may cause data loss.
- Do not use these steps to install a new RAID Controller on your server. These steps are only intended to remove and reinsert the same RAID Controller.

Removing and reinserting an active controller using IBM Storage Configuration Manager

1. Log into IBM Storage Configuration Manager.
2. Verify the status of the IBM BladeCenter S SAS RAID Controller Modules.
 - a. Select **BC-S SAS RAID Module**.
 - b. Select **Health > All Resources**.
3. If a device is attached to an external port on the RAID Controller, ensure that all applications are properly taken offline.
4. Remove the RAID Controller.
 - a. Disconnect all cables from the module.
 - b. Open the release handle by rotating the handle down to disengage the module from the IBM BladeCenter S chassis.
 - c. Slide the module out of the bay.
5. Reinsert the same RAID Controller.
 - a. Open the release handle by rotating the handle down.
 - b. Slide the RAID Controller into the module bay until it stops.
 - c. Close the release handle by rotating the handle up.
 - d. Connect all cables to the module.

The IBM BladeCenter S will detect that you have reinserted the RAID Controller and automatically powers it on.

Removing and reinserting an active controller using the RAID Controller command line interface

1. In your browser, in the URL address field, enter `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the Advanced Management Module interface. Click **GO** or press Enter. The Enter Network Password window opens.

If you have the Advanced Management Module connected to your network, log in using the network IP assigned to it. If you are using the default IP address, your management system (the computer you are using to manage your IBM BladeCenter S components) must be physically connected through an Ethernet cable to the Advanced Management Module .

Note: The default IP address for the Advanced Management Module is 192.168.70.125.

2. In the User Name field, type the initial default user ID, **USERID**. The user ID and password are case sensitive.
3. In the Password field, type the initial default password, **PASSWORD** (the sixth character is a zero) and click **OK**. The Welcome window opens.
4. In the Inactive session timeout value field, select the timeout value for this Web session and click **Continue**. The Advanced Management Module window opens.

5. Click **I/O Module Tasks > Configuration**. The I/O Module Configuration window opens.
6. Click the link for either the connectivity module in I/O module bay 3 or in I/O module bay 4.
7. From the **Current IP Configuration for RAID Controller Subsystem** section, click the **Advanced Configuration** link. The Advanced Configuration window opens.
8. To start a Telnet session, click **Start Telnet Session**. The Login screen opens.
9. At the **Login** prompt, type the initial default user ID, USERID and press Enter. The user ID and password are case sensitive. The Password prompt displays.
10. At the **Password** prompt, type the initial default password, PASSWORD (the sixth character is a zero).
11. From the command line, use the **list controller** command to verify the status of the RAID Controllers.
12. If a device is attached to an external port on the RAID Controller, ensure that all applications are properly taken offline.
13. Remove the RAID Controller.
 - a. Disconnect all cables from the module.
 - b. Open the release handle by rotating the handle down to disengage the module from the IBM BladeCenter S chassis.
 - c. Slide the module out of the bay.
14. Reinsert the same RAID Controller.
 - a. Open the release handle by rotating the handle down.
 - b. Slide the RAID Controller into the module bay until it stops.
 - c. Close the release handle by rotating the handle up.
 - d. Connect all cables to the module.

The IBM BladeCenter S will detect that you have reinserted the RAID Controller and automatically powers it on.

Replacing a media tray

Perform the following steps to concurrently replace the IBM BladeCenter S chassis media tray using the RAID Controller command line interface.

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Log into the CLI of the RAID Controller.
3. At the <CLI> prompt, enter `mountstate -getobject -mediatray` and press Enter to query the mount state. Verify the media tray is in the ONLINE state.
 <CLI> `mountstate -getobject -mediatray`

Tray#	State
0	Online

4. At the <CLI> prompt, enter mountstate -setobject -dismount -mediatray 0 and press Enter to prepare the media tray for service.

```
<CLI> mountstate -setobject -dismount -mediatray 0
Current Machine Local Time: 02/18/2010 09:47:01 PM
Set MediaTray MountState successful
```

5. At the <CLI> prompt, enter mountstate -getobject -mediatray and press Enter to query the mount state. Verify the media tray is in the SERVICE state.

```
<CLI> mountstate -getobject -mediatray
```

Tray#	State
0	Service

6. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list. Verify alerts 2200 and 2005 are in the active alert list.

```
<CLI> alert -get
```

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2200	242	20100218214701	0	Info	5005076b07441aff	0	Unmasked
Msg: Battery (Serial #Y1Y01078M24T) ready for service							
2005	243	20100218214701	0	Info	5005076b07441aff	0	Unmasked
Msg: Dismounted media tray ready to remove							
2200	243	20100218214701	1	Info	5005076b07441aff	0	Unmasked
Msg: Battery (Serial #Y1Y0107BL09M) ready for service							

7. Remove the media tray from the chassis.
 - a. Open the release handles (rotate the top handle up and the bottom handle down) to disengage the media tray from the IBM BladeCenter S chassis.
 - b. Slide the media tray out of the IBM BladeCenter S chassis.

Note: When you remove the media tray, the fan modules begin to run at full speed.

- c. If you are instructed to return the media tray or DVD drive, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.
8. Remove each Battery Backup Unit from the media tray.
 - a. Open the release handle (rotate the handle down).
 - b. Slide the Battery Backup Unit out of the media tray.
9. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list. Verify alert 0006 is in the active alert list. This alert is automatically removed from the active alert list after two minutes.

```
<CLI> alert -get
```

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
6	180	20100219131844	0	Info	5005076b07419fff	1	Unmasked

```
-----  
Msg: Media tray was removed or swapped  
-----
```

10. Insert the new media tray into the chassis.
 - a. Slide the media tray into the IBM BladeCenter S chassis until it stops.
 - b. Close the release handles (rotate the top handle down and the bottom handle up).
11. Insert each Battery Backup Unit into the new media tray.
 - a. Slide the Battery Backup Unit into the media tray.
 - b. Close the release handle (rotate the handle up).
12. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list. Verify alert 0005 is in the active alert list. This alert is automatically removed from the active alert list after two minutes.
<CLI> alert -get

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
5	186	20100219132402	0	Info	5005076b07419fff	1	Unmasked
Msg: Media tray inserted							

13. At the <CLI> prompt, enter mountstate -getobject -mediatray and press Enter to query the mount state. Verify the media tray is in the ONLINE state.
<CLI> mountstate -getobject -mediatray

Tray#	State
0	Online

14. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

If the problem is not resolved, collect the logs and contact IBM.

Replacing a Battery Backup Unit

The system contains two Battery Backup Units, one for each RAID Controller. Normal write cache operation in the IBM BladeCenter S SAS RAID Controller Module requires that at least one Battery Backup Unit (BBU) have a charge sufficient to maintain the write cache for 72 hours. The BBU can be replaced without interrupting system operation as long as one of the following conditions is true:

- Only one BBU is replaced and the other BBU is functional with at least 72 hours of charge.
- The BBU to be replaced is already nonfunctional or not charged to the 72 hour level.

If either of the above conditions exists, you can pull the failed BBU and insert a replacement without further controller action.

If the BBU replacement operation would cause a functional charged BBU to be removed and the other BBU to be in the missing, failed, or not charged state, you must disable the write cache before replacing the BBU and then re-enable it afterward.

Replacing a Battery Backup Unit using the RAID Controller command line interface

Perform the following steps to concurrently replace the Battery Backup Unit (BBU) using the RAID Controller command line interface.

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Log into the CLI of the RAID Controller.
3. At the <CLI> prompt, enter mountstate -getobject -bbu and press Enter to query the mount state. Verify the media tray is in the ONLINE state.
<CLI> mountstate -getobject -bbu

CtlrId#	Battery State
Ctlr 0	Online
Ctlr 1	Online

4. At the <CLI> prompt, enter mountstate -setobject -dismount -bbu <0 or 1> and press Enter to prepare the BBU for service.
<CLI> mountstate -setobject -dismount -bbu 0
Set Battery MountState successful
5. At the <CLI> prompt, enter mountstate -getobject -bbu and press Enter to query the mount state. Verify the BBU is in the SERVICE state.
<CLI> mountstate -getobject -bbu

CtlrId#	Battery State
Ctlr 0	Service
Ctlr 1	Online

6. At the <CLI> prompt, enter alert -get and press Enter to query the active alert list. Verify alerts 2200 is in the active alert list, or verify the amber LED on the BBU is in the SOLID state.
<CLI> alert -get

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
2200	193	20100219134122	0	Info	5005076b07419fff	0	Unmasked
Msg: Battery (Serial #Y1Y01078M227) ready for service							

7. Remove the Battery Backup Unit from the media tray.
 - a. Open the release handle (rotate the handle down).
 - b. Slide the Battery Backup Unit out of the media tray.

8. Insert the new Battery Backup Unit into the media tray.
 - a. Slide the Battery Backup Unit into the media tray.
 - b. Close the release handle (rotate the handle up).
9. At the <CLI> prompt, enter `mountstate -getobject -bbu` and press Enter to query the mount state. Verify the BBU is in the ONLINE state.
 <CLI> `mountstate -getobject -bbu`

CtrlId#	Battery State
Ctrlr 0	Online
Ctrlr 1	Online

10. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

If the problem is not resolved, collect the logs and contact IBM.

Replacing a Battery Backup Unit using the IBM Storage Configuration Manager

Perform the following steps to concurrently replace the Battery Backup Unit (BBU) using the IBM Storage Configuration Manager.

1. Log into the chassis using the Advanced Management Module and illuminate the blue chassis identification LED to ensure the repair action is conducted on the correct chassis.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **On** or **Blink** next to **Location**. Depending on the selection, the blue chassis identification LED will be in the SOLID or BLINKING state.
2. Remove any externally attached devices connected to any of the four SAS ports on the controller that is being replaced.
3. Log into the IBM Storage Configuration Manager.
4. From the navigation panel, select **BC-S SAS RAID Module > Health > Physical View**.
5. Click **BBUs**.
6. Click the BBU that is being replaced.
7. From the **Select a BBU Action** list, select **Prepare for Replacement**.
8. Read the information that displays and click **OK**.
9. Click on the BBU that was prepared for replacement.
10. Select the **Alerts** tab and verify alert 2200 is in the list, or verify that the BBU amber LED on the controller is in the SOLID state.
11. Remove the Battery Backup Unit from the media tray.
 - a. Open the release handle (rotate the handle down).
 - b. Slide the Battery Backup Unit out of the media tray.
12. Insert the new Battery Backup Unit into the media tray.
 - a. Slide the Battery Backup Unit into the media tray.

- b. Close the release handle (rotate the handle up).
- 13. Log into the Advanced Management Module and turn off the blue chassis identification LED.
 - a. Log into the Advanced Management Module.
 - b. Click **Monitors > LEDs > Media Tray and Rear Panel LEDs**.
 - c. Click **Off** next to **Location**. The blue chassis identification LED will turn off.

If the repair procedure did not resolve the problem, collect the logs and contact IBM.

Troubleshooting known issues

This topic details some of the conditions that produce known issues for the IBM BladeCenter S SAS RAID Controller Module.

Brown out conditions and the IBM BladeCenter S SAS RAID Controller Module

Issue:

A "brownout" is a condition caused by a voltage level unexpectedly going below the normal minimum level specified for the system. Systems supplied with three-phase electric power also suffer brownouts if one or more phases are absent, at reduced voltage, or incorrectly phased. Brownout conditions affect the RAID Controllers and disk subsystem in a detrimental manner resulting in an Emergency Power Off Warning (EPOW) signal and a high probability of data loss.

If a brownout occurs, the power supply in the IBM BladeCenter S chassis triggers an EPOW signal to storage system which causes it to suspend all host IO operations and disk service communication despite the fact that this was not a sustained loss of power. This prompts the Battery Backup Units go into service, which moves the data to cache memory and places it in a persistent state. Once an EPOW signal occurs, the set of actions it initiates must complete before you can resume normal operations. This can take several minutes, and require multiple system restarts.

The individual Blade servers react to the EPOW warning differently than the storage system. In most cases, if power does not cease completely, a number of the Blade servers might remain operational. However, because disk service communication stops, the system can become unstable.

Recommendation

In configurations where outage due to brown outs are unacceptable, ensure your system is protected with an Uninterrupted Power Supply (UPS) or other similar solution.

Data package collection in the intermediate state

Issue:

If you are using the IBM Storage Configuration Manager to collect a data package and one or more of your RAID Controllers is in an intermediate state you will not be able to collect this package, and the following message appears:

The Collect Support Data operation is complete, with errors.
The RAID Subsystem component support data package could not be created.
To collect support data for the RAID subsystem, use the command line interface to invoke the First Time Data Capture utility with the -allowoffline option.
Refer to the Installation and User Guide troubleshooting section,
"Collecting logs with the First Time Data Capture Utility" for instructions.
A support bundle for the remaining components was successfully created.
Click here to download the support file to your local machine.

Recommendation:

Start the First Time Data Capture Utility program using no parameters other than either the IP address of either RAID Controller.

Note: In Windows, the First Time Data Capture Utility program file is named `ftdc.exe`. The corresponding file in Linux is named `ftdc`.
The First Time Data Capture Utility can determine if one or both controllers are in an intermediate state after a sufficient timeout period, but because one controller might still be providing host access, the First Time Data Capture Utility collects no log data, generates a message to the user that the `-allowoffline` command line option must be specified, and then exits. After the utility exits, reissue the command to start the First Time Data Capture Utility again, but this time with the IP address and the `-allowoffline` parameter. The program will then collect the existing log files from both controllers. If the program finds that both controllers are in an intermediate state for longer than the allowed timeout period, it initiates a restart of the controllers. If this happens you will be instructed to make sure that host IO is suspended before requesting log file capture. After the controllers restart, the program collects the logs from both controllers.

VLAN 4095 with the Intelligent Copper Pass thru Module

Issue:

In some test cases, using an Intelligent Copper Pass thru Module (ICPM) to supply network connectivity with the VLAN 4095 ID has resulted in an inability to communicate with the RAID Controllers.

Recommendation:

Cabling ports 7 and 14 makes them live. The ICPM senses a link for ports 7 and 14, and allows you to Telnet to both RAID Controllers from the Advanced Management Module using VLAN 4095.

POST and TCP/XML communication error upon startup or reboot

Issue:

The Advanced Management Module indicates a POST and TCP/XML communication error message for the RAID Controller during system start or reboot and the module fails to complete POST.

Recommendation:

Before contacting IBM Support, attempt the following recovery procedures:

1. Log into the Advanced Management Module.
2. Click **I/O Module Task > Admin/Power/Restart**
3. Select the I/O Bay where the error is indicated.
4. Select **Restart Module(s)** and **Run Standard Diagnostics**.
5. Verify the error no longer exist.

If these steps did not correct the error, collect the logs and contact IBM Support for further assistance.

RAID Controller critical and warning errors interfere with firmware update process

Issue:

If the RAID Controller reports any critical or warning errors, the firmware update process might not complete successfully.

Recommendation:

Resolve any critical or warning errors prior to starting the firmware update process.

Before starting the firmware update process, log in to the IBM Storage Configuration Manager application and query the **Active Alert** list. If any critical or warning errors exist on the system, resolve them before starting the firmware update process. To view the **Active Alert** list perform the following steps:

1. Log in to the IBM Storage Configuration Manager application.
2. Click **BC_S SAS RAID > Module Health > Active Alerts**.
3. Verify no **critical** or **warning** alerts exist.

If there are critical or warning alerts, resolve the issues that caused them before starting the firmware update process.

How to reset the SAS RAID controllers to the factory defaults

This section contains information about how to reset the SAS RAID Module to the factory defaults.

Before you reset the SAS RAID Module to the factory defaults, you must end all application I/O processes and shut down any active Blade servers in accordance with the recommended non-concurrent practices. Then, use the reset to factory defaults function within Advanced Management Module to reset SAS RAID modules. To reset the SAS RAID modules to the factory default settings, you must power off both SAS RAID Modules via AMM.

To reset both SAS RAID modules, complete the following steps:

1. Stop all host I/O applications and power off the Blade servers.
2. Use the Advanced Management Module to reset to the factory defaults:
 - a. Log into the Advanced Management Module.
 - b. Select **I/O Module Tasks > Admin/Power/Restart**.
 - c. Select the check boxes next to bay 3 and bay 4.
 - d. From the **Available actions** menu, select **Power Off Module(s)**.
 - e. Click **Perform** action.
 - f. Wait until both SAS RAID Modules are powered off. The **Off** message will be displayed in the **Pwr** column.
3. Reset the SAS RAID module in Bay 3 to the factory defaults:
 - a. Select **I/O Module Tasks > Configuration**.
 - b. In the **I/O Module Configuration** section, select **Bay 3**.
 - c. In the Bay 3 section that displays, select **Advanced Configuration**.
 - d. In the **Advanced Configuration for I/O Module 3** section, select **Restore Factory Defaults**.
 - e. Select **Restore Defaults**.
 - f. Select **OK**.
 - g. The SAS RAID Module in bay 3 will power on. Wait until the SAS RAID Module in bay 3 successfully powers on.
The **On** message will display in the **Pwr** column, and the message **POST results available: Module completed POST successfully** will display in the **POST Status** column.
 - h. Power off the SAS RAID Module in bay 3 until the **Off** message is displayed in the **Pwr** column
4. Reset the SAS RAID module in Bay 4 to the factory defaults:
 - a. Select **I/O Module Tasks > Configuration**.
 - b. In the **I/O Module Configuration** section, select **Bay 4**.
 - c. In the Bay 4 section that displays, select **Advanced Configuration**.
 - d. In the **Advanced Configuration for I/O Module 4** section, select **Restore Factory Defaults**.
 - e. Select **Restore Defaults**.
 - f. Select **OK**.
 - g. The SAS RAID Module in bay 4 will power on. Wait until the SAS RAID Module in bay 4 successfully powers on.

The **On** message will display in the **Pwr** column, and the message **POST results available: Module completed POST successfully** will display in the **POST Status** column.

- h. Power off the SAS RAID Module in bay 4 until the **Off** message is displayed in the **Pwr** column
5. Power on both SAS RAID modules in bay 3 and bay 4:
 - a. Select **I/O Module Tasks > Admin/Power/Restart**.
 - b. Select the check boxes next to bay 3 and bay 4.
 - c. From the **Available actions** menu, select **Power On Module(s)**.
 - d. Click **Perform action**.
 - e. Both SAS RAID modules in Bay 3 and Bay 4 will power on. Wait until the both SAS RAID Modules in bay 3 and bay 4 successfully power on.

The **On** message will be displayed in the **Pwr** column, and the message **POST results available: Module completed POST successfully** will display in the **POST Status** column.

Note: Performing the steps to reset the factory defaults does not affect any logical configuration data on the SAS RAID Modules.

Resolving DSM firmware mismatch issue when DSM_SFF is installed

About this task

If the DSM_SFF is installed with RSSM controllers running old version firmware (version 1.2.x.xxx and below), the DSM firmware mismatch issue would occur. When users observe Alert 5014 and 9004, a firmware upgrade to latest firmware version (version 1.3.x.xxx or above) should be performed.

```
<CLI> alert -get
Current Machine Local Time: 04/03/2013 03:06:19 PM
```

Existing Alerts :

AlertCode	Id	Time	SlotID	Severity	WWN	Ackable	MaskState
5014	3	20130403065910	0	Warning	5005076b07402cff	0	Unmasked
Msg: Drive enclosure 2 firmware mismatch exists. Reboot system or execute controller firmware update.							
5014	5	20130403065910	0	Warning	5005076b07402cff	0	Unmasked
Msg: Drive enclosure 1 firmware mismatch exists. Reboot system or execute controller firmware update.							
9004	9	20130403070021	0	Critical	5005076b07402cff	1	Unmasked
Msg: Drive enclosure 2 firmware update failed							
9004	10	20130403070021	0	Critical	5005076b07402cff	1	Unmasked
Msg: Drive enclosure 2 firmware update failed							

Figure 25. Users will observe Alert 5014 and 9004 when this issue occurs

```
<CLI> firmwareupgrade -getstatus
Current Machine Local Time: 04/03/2013 03:08:31 PM
Ctrl 0 Firmware Upgradation Status is FW_UPGRADE_FAILED_DSMUPGRADE
Ctrl 1 Firmware Upgradation Status is FW_UPGRADE_IDLE

Drive Upgrade Cumulative Status is IDLE
```

Figure 26. Alert 9004 is caused by controller failed to flash the DSM firmware due to the firmware downgrade preventing mechanism of DSM_SFF module

Procedure

1. Put the controller into service mode by issuing **shutdown -system -state servicemode** command in the <CLI> prompt. After the controller rebooted, ensure both controllers enter service mode by issuing **list controller** command in the <CLI> prompt.

```
<CLI> list controller
Current Machine Local Time: 04/03/2013 01:42:00 PM
```

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	SERVICE	1	--
1	Ctlr1	SERVICE	1	--

Figure 27. <CLI> list controller

2. Perform RSSM firmware upgrade to the latest version of firmware (version 1.3.x.xxx or above). Please refer to *IBM BladeCenter S SAS RAID Controller Module Installation and User's Guide* Chapter 6 and 11 for detail instructions.
3. After the RSSM firmware upgrade completed, please check whether both Alert 5014 and 9004 disappear and all the firmware upgrade status are IDLE. If so, then the issue is resolved.

```
<CLI> firmwareupgrade -getstatus
Current Machine Local Time: 04/03/2013 01:35:02 PM
Ctlr 0 Firmware Upgradation Status is FW_UPGRADE_IDLE
Ctlr 1 Firmware Upgradation Status is FW_UPGRADE_IDLE

Drive Upgrade Cumulative Status is IDLE
```

Figure 28. All the firmware upgrade status are IDLE

Appendix. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check <http://www.ibm.com/systems/info/x86servers/serverproven/compat/us> to make sure that the hardware and software is supported by your IBM product.
- Go to <http://www.ibm.com/supportportal> to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
 - Hardware and Software Maintenance agreement contract numbers, if applicable
 - Machine type number (IBM 4-digit machine identifier)
 - Model number
 - Serial number
 - Current system UEFI and firmware levels
 - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/supportportal>.

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at <http://www.ibm.com/supportportal>. IBM System x information is at <http://www.ibm.com/systems/x>. IBM BladeCenter information is at <http://www.ibm.com/systems/bladecenter>. IBM IntelliStation information is at <http://www.ibm.com/systems/intellistation>.

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at <http://www.ibm.com/de/support/ecurep/terms.html>.

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw

Creating a personalized support web page

You can create a personalized support web page by identifying IBM products that are of interest to you.

To create a personalized support web page, go to <http://www.ibm.com/support/mynotifications>. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/supline/products>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services> or see <http://www.ibm.com/planetwide> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services.

To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld> and click **Business Partner Locator**. For IBM support telephone numbers, see <http://www.ibm.com/planetwide>. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/us/en/copytrade.shtml>.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1,048,576 bytes, and GB stands for 1,073,741,824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1,000,000 bytes, and GB stands for 1,000,000,000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as total bytes written (TBW). A

device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. IBM is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 12. Limits for particulates and gases

Contaminant	Limits
Particulate	<ul style="list-style-type: none">• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2¹.• Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282.• The deliquescent relative humidity of the particulate contamination must be more than 60%².• The room must be free of conductive contamination such as zinc whiskers.
Gaseous	<ul style="list-style-type: none">• Copper: Class G1 as per ANSI/ISA 71.04-1985³• Silver: Corrosion rate of less than 300 Å in 30 days

Table 12. Limits for particulates and gases (continued)

Contaminant	Limits
	<p>¹ ASHRAE 52.2-2008 - <i>Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size</i>. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.</p> <p>² The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.</p> <p>³ ANSI/ISA-71.04-1985. <i>Environmental conditions for process measurement and control systems: Airborne contaminants</i>. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.</p>

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

*Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.*

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) statement

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA)
Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase)

Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Index

Numerics

12-Disk Storage Module 162
6-Disk Storage Module 162

A

accessible documentation 198
active alerts 109
add capacity command 90
add mirror command 82
alert command 62
alerts 109
assimilate drive command 82
assistance, getting 191
Australia Class A statement 199

B

battery backup unit 13
 installing 14
 removing 15
 replacing 181
battery command 63
BBU 13

C

cache settings command 64
Canada Class A electronic emission statement 199
capturing with FTDC utility 155
chassis
 power-off sequence 29
China Class A electronic emission statement 202
chpassword command 65
Class A electronic emission notice 199
CLI
 display commands 54
 system control and configuration commands 62
 volume management commands 82
 volume services commands 89
CLI commands
 add capacity 90
 add mirror 82
 alert 62
 assimilate drive 82
 battery 63
 cache settings 64
 chpassword 65
 clilog 65
 commparams 65
 configure access 66
 configure alert 67
 configure pool 68
 configure timeout 68
 controller config 69
 copyback 83

CLI commands (*continued*)
 create pool 84
 create volume 85
 datascrub 90
 delete all 91
 delete pool 86
 delete volume 86
 detail controller 54
 detail drive 55
 detail pool 56
 detail volume 57
 detail volume verbose 59
 email alert 70
 enclosure reporting 71
 event log 72
 expand -volume 91
 global spare 87
 host 88
 hostlun 88
 initialize 92
 list controller 59
 list drive 60
 list features 75
 list killedpaths 92
 list pool 61
 list volume 62
 locate 72
 mountstate 75
 post result 77
 service mode 77, 101
 service mode command 101
 shellscript 79
 show raid levels 79
 shutdown 79
 swversion 80
 synchronize volume 93
 time 81
 validate key 81
 view long running tasks 93
CLI, RAID controller 53
clilog command 65
clustering 38
Command Line Interface 162
commparams command 65
components
 battery backup unit 13
 concurrent procedures 168
 configure access command 66
 configure alert command 67
 configure pool command 68
 configure timeout command 68
connectivity module
 illustration 10
 option package 11
 summary of features and specifications 9
 Telnet interface
 overview 17
contamination, particulate and gaseous 197
controller config command 69

controllers
 list controller command 59
controls and indicators
 battery backup unit 13
create pool command 84
create volume command 85
creating a personalized support web page 193
custom support web page 193

D

datascrub command 90
DDM 1
delete all command 91
delete pool command 86
delete volume command 86
detail controller command 54
detail drive command 55
detail pool command 56
detail volume command 57
detail volume verbose command 59
Disk Drive Module 1
Disk Storage Module 1
 replacing 165, 172
documentation
 format 198
 using 192
drive
 replacing 171
DSA, sending data to IBM 192
DSM 1
 replacing 165, 172

E

electronic emission Class A notice 199
email alert command 70
enclosure reporting command 71
European Union EMC Directive conformance statement 200
event log command 72
expand -volume command 91

F

FCC Class A notice 199
firmware updates 31
First Time Data Capture Utility 155

G

gaseous contamination 197
Germany Class A statement 200
global spare command 87

H

hardware
 prerequisites 13
hardware service and support telephone numbers 193
help
 from the World Wide Web 192
 from World Wide Web 192
 sending diagnostic data to IBM 192
 sources of 191
host command 88
hostlun command 88

I

IBM BladeCenter
 shut down 29
IBM BladeCenter S
 illustration 10
IBM BladeCenter S SAS RAID Controller Module 1
IBM SAS RAID Controller Module
 installation 19
 shut down 29
IBM Storage Configuration Manager 1
 installation 22
IBM Taiwan product service 193
ID
 requirements 23
IGMP snooping 38
important notices 196
information center 192
information panel indicators {LEDs} 101
initialize command 92
install
 IBM Storage Configuration Manager 22
 RAID controller 19
 SAS controller 19
installing
 battery backup unit 14
 tape device 99

J

Japan Class A electronic emission statement 201
Japan Electronics and Information Technology Industries Association statement 202
JEITA statement 202

K

Korea Class A electronic emission statement 202

L

LEDs 101
 battery backup unit 13
list volume command 59
list drive command 60
list features command 75
list killedpaths command 92

list pool command 61
list volume command 62
locate command 72
log files 155
Log files 155
logical identifiers 11

M

media tray
 battery backup unit 13
 replacing 179
Microsoft Cluster Service
 configuring blades 38
mountstate command 75

N

New Zealand Class A statement 199
notes, important 196
notices 195
 electronic emission 199
 FCC, Class A 199

O

option package 11

P

particulate contamination 197
password
 requirements 23
 reset 23
People's Republic of China Class A electronic emission statement 202
physical location codes 11
post result command 77
predefined zones
 modifying 97
product service, IBM Taiwan 193

R

RAID controller
 reset to factory defaults 187
RAID Controller 1
 alerts 109
 detail controller command 54
 installation 19
 removing and reinserting 178
 replacing 158, 159, 161, 168, 170
 troubleshooting 101
 updating firmware 164
RAID Controller CLI 53
RAID levels 34
related documentation 12
removing
 battery backup unit 15
RSSM zones
 configuring 97
 predefined 97
Russia Class A electronic emission statement 202

S

safety information 5
SAS Expansion Card
 installation 19
SCM 1
 installation 22
sending diagnostic data to IBM 192
service and support
 before you call 191
 hardware 193
 software 193
service mode command 77
shellscript command 79
show raid levels command 79
shut down
 IBM BladeCenter 29
 IBM SAS RAID Controller Module 29
shutdown command 79
software service and support telephone numbers 193
static-sensitive devices
 handling 8
storage configuration 35
storage pool 33
storage pools
 add capacity command 90
 create pool command 84
 delete all command 91
 delete pool command 86
 detail pool command 56
 list pool command 61
support web page, custom 193
swversion command 80
synchronize volume command 93
system resources
 locating 11

T

Taiwan Class A electronic emission statement 203
tape device
 installing 99
telecommunication regulatory statement 198
telephone numbers 193
Telnet
 connectivity module interface overview 17
time command 81
trademarks 196
troubleshooting
 known issues 184
troubleshooting 101
TS2230 99
TS2240 99
TS2340 99
TS2900 99
TS3100 99

U

United States FCC Class A notice 199

V

- validate key command 81
- view long running tasks command 93
- VMware 36
- volumes 33, 36
 - create volume command 85
 - delete all command 91
 - delete volume command 86
 - detail volume command 57
 - detail volume verbose command 59
 - expand -volume1 command 91
 - global spare command 87
 - list volume command 62
 - synchronize volume command 93

Z

- zones
 - configuring 97
 - predefined 97



Part Number: 00MV718

Printed in USA

(1P) P/N: 00MV718

