SGI® Modular InfiniteStorage™ (MIS)
Platform Installation Guide

Record of Revision

Version	Description
001	March 2012 Original Printing
002	March 2013 Modified for external release.
003	May 2013 Added Cable Management Arm length adjustment instructions, System Layout diagrams, added significant images and made major edits.
004	July 2013 Updated safety information, fan replacement, and power supply information (email reporting). Updated Environmental Requirements to include shipping information.
005	August 2013 Added DC power supply option. 1st Run instructions added, along with boot drive replacement procedures.
006	September 2013 Added BBU and RAID card monitoring. Minor edits.

:

Contents

Figures

Tables

Introduction

This guide describes setup and installation of the SGI® Modular InfiniteStorage™ (MIS) platform. With two main configurations possible for the enclosure (server & storage, or JBOD—Just a Bunch Of Disks) this guide covers inspecting the shipment, preparing for installation, how to install, and gives examples of some possible external cabling options.

Audience

This guide is written for owners/users of the MIS platform who need to install the unit themselves, rather than relying on SGI installation services. It is written with the assumption that the reader has a good working knowledge of computers, servers, networking, hardware, software and RAID arrays.

Important Information

The following section details several safety precautions that should be observed at all times. First, the MIS requires the proper environment in which to operate. Second, a fully loaded MIS platform can weigh up to 220lb. Third, electricity is a major concern, especially Electrostatic Discharge (ESD), detailed later in this section. Please read these sections carefully prior to set up.

	CAUTION
	Observe all ESD precautions. Failure to do so can result in damage to the equipment.

CAUTION

Do not apply floor plating over open floor tiles. Unsupported floor plating can collapse under heavy equipment and result in damage to the computer equipment.
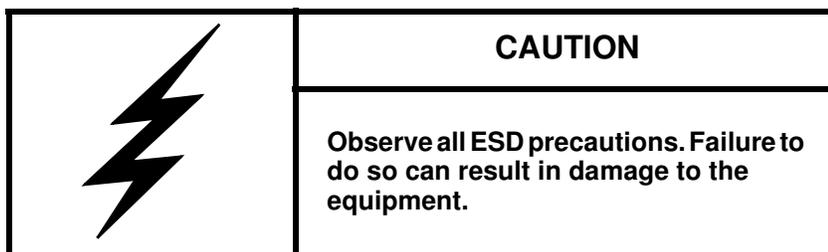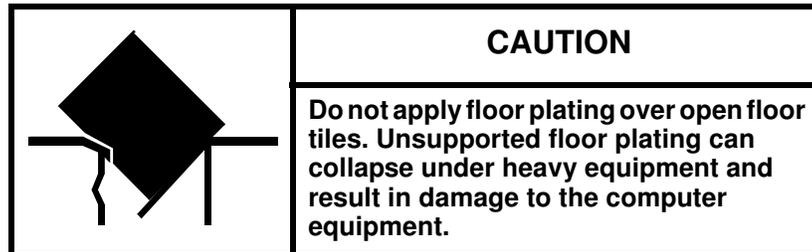
Environmental Requirements

The following are the environmental requirements for the MIS platforms.

Operating temperature: **41° to 95° F [5° to 35° C] (up to 5,000 ft. [1,500 m])**
 – Derate max temperature (95° F [35° C]) by 1.8° Fahrenheit [1° Celsius] per 1,000 ft. [305 m] of altitude above 5,000 ft. [1525 m])
 – Temperature rate of change must not exceed 18° F [10° C] per hour

Operating humidity: **8% to 80% non-condensing**
 – Humidity rate of change must not exceed 10% relative humidity per hour

Operating altitude: **up to 10,000 ft. [up to 3,050 m]**

Shipping temperature: **-40° to 140° F [-40° to 60° C]**
 – Temperature rate of change must not exceed 36° F [20° C] per hour

Shipping humidity: **10% to 95% non-condensing**

Shipping altitude: **up to 40,000 ft. (up to 12,200 m)**

Storage temperature: **41° F [5° C] to 113° F [45° C]**
 – Temperature rate of change must not exceed 36° F [20° C] per hour

Storage humidity: **8% to 80% non-condensing**

Storage altitude: **up to 40,000 ft. [up to 12,200 m]**

Safety Precautions

Do NOT wear loose clothing, such as neckties or unbuttoned shirt sleeves, while working on the unit. These can be pulled into a cooling fan or tangled in cabling.

Remove ALL jewelry and any metal objects from your body, which are excellent electrical conductors. These can harm you and/or cause short circuits if they come into contact with printed circuit boards or powered areas.

Be aware of the locations of the power on/off switch on the chassis as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.

Do NOT work alone when working with high voltage components. When working around exposed electrical circuits, another person should be nearby, who is familiar with the power-off controls, to switch off the power if necessary.

Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards with which they come into contact.

Do NOT use mats designed to decrease static electrical discharge. Instead, use rubber mats that have been specifically designed as **electrical insulators**.

The power supply power cords MUST include a grounding plug and MUST be plugged into GROUNDED electrical outlets.

Do NOT attempt to transport/move a fully loaded MIS system! An MIS system can weigh up to 220lbs. when fully loaded. If the system must be moved, first remove the drives from the chassis. When lifting the system, two people (one at each end) should lift slowly with feet spread apart to distribute the weight. Always follow safe lifting practices when moving heavy objects. More information on moving large objects, requiring a two-person team, is available in the Centers for Disease Control's, "Ergonomic Guidelines for Manual Material Handling" (http://www.cdc.gov/niosh/docs/2007-131/pdfs/2007-131.pdf)

Power should always be disconnected from the system when removing or installing system components that are not hot-swappable. When disconnecting power, you should first do a clean shut down of the operating system, then power down the system, and then unplug all power cords (the unit has more than one power supply cord).

The maximum overcurrent protection shall be 50A per power supply. The overcurrent protection shall be provided by the facility power distribution. All national and local electrical code would apply. Check with your local licensed electrician for details.

The branch current protection shall be provided by customer. All national and local electrical code would apply. Check with your local licensed electrician for details.

ESD Precautions

Caution: Electrostatic Discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards.

The following measures are generally sufficient to neutralize this difference before contact is made to protect your equipment from ESD:

- Use a grounded wrist strap designed to prevent static discharge.

- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.

- Touch a grounded metal object before removing the board from the antistatic bag.

- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.

- Handle a board by its edges only; do not touch its components, peripheral chips, memory modules or contacts.

- When handling chips or modules, avoid touching their pins.

- Put the server board and peripherals back into their antistatic bags when not in use.

- For grounding purposes, make sure your computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the server board.

Safety & Emissions

The following is a list of agency approvals for MIS on safety and emissions.

Electromagnetic Compatibility

Table 0-1 lists the region and compliance reference for EMC (Electromagnetic Compatibility) compliance.

Table 0-1   MIS Server Platform Region and EMC Compliance References

Region	Compliance Reference
Australia/ New Zealand	AS/NZS CISPR 22 (Emissions)
USA/Canada	Industry Canada ICES-003 Issue 4 FCC CFR47, Part 15 Subpart B
CENELEC Europe	EN55022 Emissions EN55024 Immunity
International	CISPR 22/ CISPR 24
Japan	VCCI V-3 Certification
Korea	KCC KN22, KN24 Verification
Taiwan	BSMI CNS 13438 Verification
Russia	EAC

Safety Certification

National Recognized Testing Laboratory (NRTL) provides the safety certification for ITE products. NRTL's offer various product markings depending on the type of products being tested and satisfactory tests results. Underwriters Laboratories (UL) and Canadian Standards Association (CSA) are typical (NRTL's) that provides safety certification services for Information.

Technology Equipment (ITE). Table 0-2 lists the region and compliance reference for safety compliance.

Table 0-2   MIS Server Platform Region and Functional Safety Listing Mark

Region	Compliance Reference
USA/Canada	CSA 60950-1 / UL60950-1 CAN/CSA STD C22.2 No. 60950-1
IEC (Europe)	IEC60950-1 – CB Certification, CE Mark
Russia	EAC

The following documents are relevant to the MIS platform:

- *MegaRAID SAS Software User Guide*, publication number 51530-0x.

- *MegaRAID 6Gb/s SAS RAID Controllers User Guide*, publication number 41450-0x.

- *Intel Server Boards and Server Platforms Server Management Guide*, publication number 37830-002

- *Intel® Remote Management Module 4 and Integrated BMC Web Console User Guide* (pdf) Revision 2.6 (also refer to the **Help** files located within the BMC itself, see Figure 2-17 on page 61)

- Intel's *System Event Log Troubleshooting Guide for EPSD Platforms Based on Intel Xeon Processors E5 4600/2600/2400/1600/1400 Product Families* (pdf)

- Intel's *System Event Log Troubleshooting Guide for EDSP Platforms Based on Intel Xeon Processor E5 4600/2600/2400/1600/1400 Product Families* (http://download.intel.com/support/motherboards/server/sb/g90620001_s1400_s4600_systemeventlog_troubleshooti.pdf) for translation of the hex codes used in Alert Emails (see Figure 2-24 on page 70)

- Intel's *Intel Server Board S2600JF, Technical Product Specification*:

- IPMItool comes with Linux. Information on IPMItool can be found at http://ipmitool.sourceforge.net/manpage.html

- IPMIutil is for Windows and is available for download through http://ipmiutil.sourceforge.net/. Information on this tools can be found at http://ipmiutil.sourceforge.net/docs/UserGuide. (SGI does not provide support for Windows, or any Windows utilities.)

- More Information on IPMI can be found through
  http://www.intel.com/content/www/us/en/servers/ipmi/what-is-ipmi.html and
  http://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface

- SGI InfiniteStorage series documentation (http://techpubs.sgi.com)

- Man pages (http://www.linuxmanpages.com/)

Various formats of SGI documentation, release notes, and man pages are available. The SGI
Technical Publications Library (http://docs.sgi.com/) contains the most recent and most
comprehensive set of online books, release notes, man pages, and other information. Refer to the
SGI Supportfolio™ web page for documents which access requires a support contract (as do the
MegaRAID books cited above). See "Product Support" on page xxi. You can also view man pages
by typing `man <title>` on a command line in Linux.

Conventions

The following conventions are used throughout this document:

Convention	Meaning
Command	This fixed-space font denotes literal items such as commands, files, routines, path names, signals, messages, and programming language structures.
variable	The italic typeface denotes variable entries and words or concepts being defined. Italic typeface is also used for book titles.
[ ] <..>	Brackets enclose optional portions of a command or directive line.
GUI element	This font denotes the names of graphical user interface (GUI) elements such as windows, screens, dialog boxes, menus, toolbars, icons, buttons, boxes, fields, and lists.

Product Support

SGI provides a comprehensive product support and maintenance program for its products, as
follows:

- If you are in North America, contact the Technical Assistance Center at +1 800 800
  4SGI (4744) or contact your authorized service provider.

- If you are outside North America, contact the SGI subsidiary or authorized distributor in your country. International customers can visit http://www.sgi.com/support/ Click on the "Support Centers" link under the "Online Support" heading for information on how to contact your nearest SGI customer support center.

For Microsoft® products, only Windows® 2008 R2 SP1 is WHQL certified.

Software Downloads

SGI provides the software that has been approved for use on the MIS platforms, including" SGI approved" versions of 3rd party software. These SGI approved versions have been tested for quality assurance and hardware/software/firmware compatibility with the MIS. To obtain software, either contact SGI Customer Support for the most recent approved versions, or download from the Supportfolio web site: http://support.sgi.com (requires Supportfolio account and password for access).

Customers who wish to run Windows buy only the hardware from SGI. The customer is then responsible for operating system installation and configuration, and all support arrangements with Microsoft. Drivers, utilities (including IPMIutil), device manager, etc., and other required software for Windows are not provided by SGI. These must be obtained from the OEM or downloaded from 3rdparty sites

CRU/FRU

Some of the components on the MIS platform are customer-replaceable units (CRUs), meaning that these modules were designed to be repaired/replaced by you, the customer. These include fan assemblies, power supplies, storage drives, and boot drives, all of which are hot-swappable. However, many of the other components on the MIS platform should be serviced by SGI field technicians ONLY, so as not to violate the warranty agreement. The components are field-technician replaceable units, or FRUs. It is important to note that our CRUs can be easily installed and replaced by customers, which enables a speedy recovery of proper system operation.

For additional information about CRUs, please see:

- Customer Replaceable Units (CRUs) Installation Policy (http://www.sgi.com/services/support/cru/policy.html)
- Customer Replaceable Units (CRU) and Customer Obligations (http://www.sgi.com/services/support/cru/obligations.html)

Purchasable Support & Maintenance Programs

SGI provides several comprehensive product support and maintenance programs for its products. SGI also offers services to implement and integrate Linux-based applications in your environment.

*   Refer to http://www.sgi.com/services/

*   If you are in North America, contact the Technical Assistance Center at +1-800-800-4SGI (4744), or contact your authorized service provider.

*   If you are outside North America, contact the SGI subsidiary or authorized distributor in your country. See http://www.sgi.com/global/index.html for more information.

Reader Comments

If you have comments about the technical accuracy, content, or organization of this document, please contact SGI. Be sure to include the title and document number of the manual with your comments. (Online, the document number is located in the front matter of the manual. In printed manuals, the document number is located at the bottom of each page.)

You can contact SGI in any of the following ways:

*   Send email to the following address: techpubs@sgi.com

*   Contact your customer service representative, and ask that an incident be filed in the SGI incident tracking system.

*   Send mail to the following address:

SGI
Technical Publications
46600 Landing Parkway
Fremont, CA 94538

SGI values your comments, and will respond to them promptly.

Installation Guide

This is an installation guide for the SGI® Modular InfiniteStorage™ (MIS) Servers and JBODs. This guide is for those customers who require, as a matter of security or otherwise, that *they* perform installation and first-use of the MIS product, rather than SGI installing and performing initial set-up. Please refer to the *SGI® Modular InfiniteStorage™ (MIS) User Guide, version 1.5* for instructions for use past initial installation.

Shipment Overview

To reduce the chassis weight for shipping and installation, the system ships with the drives in drive carriers, removed from the chassis. You will need to install the drives into the locations specified on the attached labels after the chassis is installed in the rack.

The rail kit that ships with the system must be used to support the product. This rail kit enables the system to slide forwards and backwards in the rack for service access.

The procedures required to install a system will depend on which configuration is ordered:

If an SGI D-rack configuration is ordered (Figure 1-1), one or more chassis ship in the rack and the drives ship in separate boxes. The rail kits are already installed in the rack and on each chassis and the chassis are installed in the rack. You must install the drives into the chassis in the locations specified on the attached labels. Refer to "Acclimatization" on page 4 for more details.

If a configuration without a rack is ordered, the chassis and drives ship in separate boxes. You must install the rail kit in the customer's rack and on each chassis and then two people are required to install each chassis in the rack. You must then install the drives into the locations specified on the attached labels. Refer to "Installing MIS Platforms" on page 5 for more details.

Inspecting a Shipment

It is important that you inspect all equipment received from a shipping carrier before signing for the shipment. Be sure to do the following when you arrive at a site to install equipment and when you receive equipment directly from a shipping carrier:

1. Inspect the shipment.

   • Does the number of pieces received match the bill of lading?

   • Have boxes been opened or is there damage to the packaging?

2. Open the shipment.

   • After removing the packaging, is there any visible damage?

3. Record any issues/problems (if applicable).

   • Use the bill of lading to record any issues discovered during the inspection.

   • Take photos of all visible damage.

   • Sign for the shipment after making notes on the bill of lading.

4. Report the issues to SGI.

Contact the Customer Support Center (CSC) at 1-800-800-4744 (in the United States; refer to http://www.sgi.com/support/supportcenters.html for other local numbers) to begin the replacement process.

Take photos of any damage and in your message, please send a brief description of the problem to ships@sgi.com. A coordinator will contact you about the problem.

Figure 1-1   SGI Destination Rack (D-Rack)

Acclimatization

If the equipment has been in transit for more than 24 hours to reach the install site, then a wait is required, especially for HDDs. To acclimatize the shipment, wait **4 to 8 hours** for the equipment to acclimate to the data center environment before proceeding with the installation.

Caution: Failure to let equipment acclimate can cause condensation damage to the equipment.

Preparing to Install

Uncrate the rack and inspect the shipment for any damage. (Refer to "Inspecting a Shipment" on page 2.)

Be aware that the increased weight and size of the tall racks can cause the racks to tip over if the racks are improperly handled. To minimize your own personal risk of injury, use extra care and allow extra time when moving racks.

Be sure to evaluate the path you will be moving a rack along before moving the rack. Plan the move by anticipating any issues and removing any obstacles. Use extra caution during the actual move and roll the rack on to the data center floor.

Required Tools

The following tools are required:

- #1 and #2 Phillips screwdrivers,

- Long #2 Phillips screwdriver,

- Flat-head screwdriver,

- Thin-tipped flat-head screwdriver

- 10mm hexagonal socket wrench,

- A wheeled cart with breaks, sturdy enough to hold the chassis, and on which to work.

Note: Screwdrivers with magnetic tips are recommended.

Installing MIS Platforms

After a shipment has been inspected (page 2) and acclimated (page 4) to the location, there are two scenarios for installing MIS platforms (server and/or JBOD). One way is to install the platforms into a rack that is already on location (D-Rack or other supported rack systems). The next scenario is installing MIS platforms that have been shipped in an SGI D-Rack. In this scenario, the chassis are already installed into the rack, and the drives were shipped separately.

To install an MIS platform into a rack that is already on location:

1. First locate all boxes in the shipment. There should be a single box that holds each chassis and multiple boxes with drives for each chassis (each box holds up to 20 drives).

2. Next, the rolling rails that support the MIS chassis in the rack must be installed, and the chassis placed into the rack, following the rack placement guide provided in the cabling guide (page 26). These procedures requires two people.

3. Once the chassis is installed into the rack, the drives can be installed into their carriers, and the drives with carriers can be installed into the system (page 23).

4. Following this, the chassis can be returned to the rack in the stowed position (page 20). That complete, the system can be cabled and powered on.

5. If there are no faults, the system can then be zoned to its desired configuration.

To install a system that is shipped in a D-Rack:

1. First locate all boxes in the shipment. There should be a single box that holds the D-Rack and multiple boxes with drives for each chassis (each box holds up to 20 drives).

2. Go straight to the instructions for "Sliding the Chassis Forward/Backwards" on page 20, and continue following the instructions from there.

Installing the Front Bezel Grille

The MIS Chassis ships without the front grille attached. There are two or three cables (one or two for control panel functionality, and one for the S9D network interface) at the the front left corner of the chassis (Figure 1-3). These cables must be attached to their corresponding sockets on the front bezel grille, before attaching the grille to the chassis. To do so, follow these instructions.

1. Orient the front bezel grille so that the left inner edge containing the sockets (Figure 1-2) lines up with the front left edge of the chassis where the cables protrude.

2. Use the two latches on the bezel grille to help attach it to the chassis on the left side, and work from the right side (swinging it open like a door, rather than top or bottom, for ease of cabling).
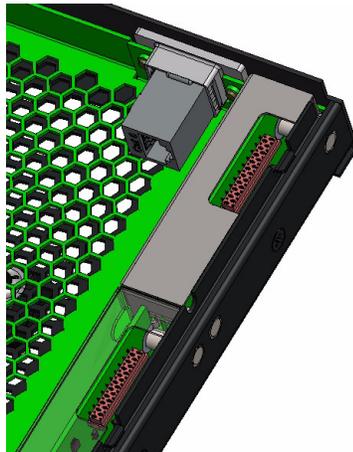
Figure 1-2　　　Front Bezel Grille Control Panel Sockets and S9D Network Interface

Figure 1-3　　　Chassis Front Cables

3. Plug the ribbon cable(s) into their corresponding control panel socket (Figure 1-4).

Figure 1-4   Control Panel Ribbon Cables Attached to Front Bezel

4. Plug the network cable into the underside of the S9D network interface (Figure 1-5s).

Figure 1-5   S9D Network Interface Cable

5. Once all the wires have been successfully connected, swing the grille shut such that it can be snapped into place on the front of the chassis using the attached tabs (Figure 1-6). Push firmly but gently to attach the front grille.
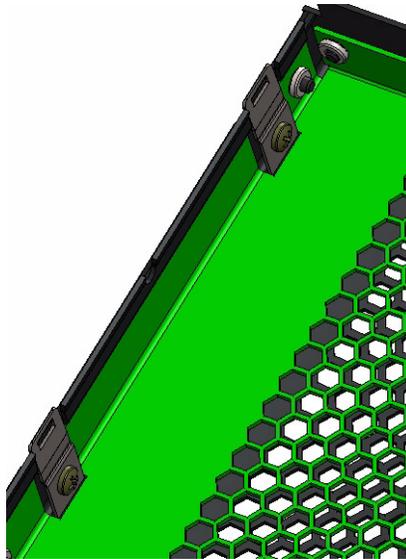
Figure 1-6   Front Bezel Grille Attach Tabs

D-Rack Stiffener*

Note: The following procedure is for installing into a D-Rack *already on location*, where the customer is required to install the outer rails into the SGI D-Rack. **These instructions are for SGI D-Racks on location ONLY.** SGI D-Racks shipped with chassis will come pre-installed with rolling rails and D-Rack Stiffener.

If you are installing rails into a SGI D-Rack on location, it will require installation of the D-Rack Stiffener. This item is two brackets: the attachment plate with a wedge-shaped cut-out (Figure 1-7), and the adjustment plate with interlocking tabs (Figure 1-8).
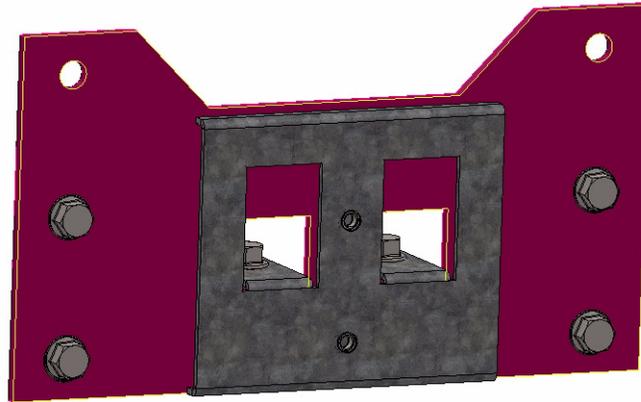
Figure 1-7   D-Rack Stiffener Attachment Plate
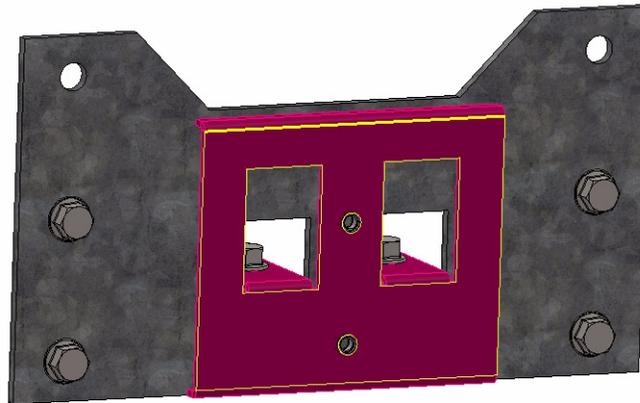
Figure 1-8   D-Rack Stiffener Adjustment Plate

These two pieces come together to form a single unit, held together by two vertical 6x16 metric hex flange bolts (Figure 1-9, in cyan) to make the D-Rack Stiffener, and attached to the D-Rack using four bolts (Figure 1-9, in magenta).
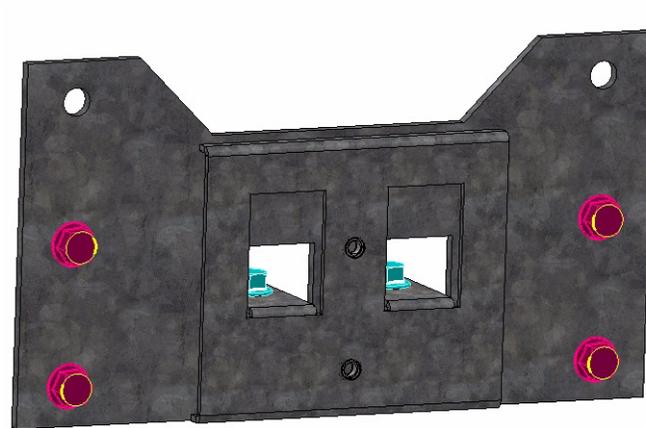
Figure 1-9   D-Rack Stiffener Bolts

Figure 1-10   D-Rack Stiffener

1. Due to their construction, it is easiest to join the brackets together first, and then attach the D-Rack Stiffener to the D-Rack.

2. Attach the inner bracket to the outer bracket using the vertical bolt and socket wrench (Figure 1-9). Do **not** tighten these bolts all the way. They will be used later for altering rail aligning using the alignment tool.

Note: The screws that attach the D-Rack Stiffener to the rack can be tightened all the way.

3. Attach the the D-Rack Stiffener to the D-Rack using the four support screws. There are six holes available for the screws, but two will be blocked. Use the remaining four holes (Figure 1-9).

Note: When installing, leave the vertical bolts of the D-Rack Stiffener loose. The vertical bolts in the D-Rack Stiffener will allow the rails to be adjusted later using the alignment tool.

Installing the Rolling Rails

These instructions are for installing the rolling rails on chassis shipped separately (i.e., not in a rack) The rolling rails are used to support the chassis in the rack and provide ease of movement out the front and back of the rack, for easier and safer serviceability (Figure 1-11).
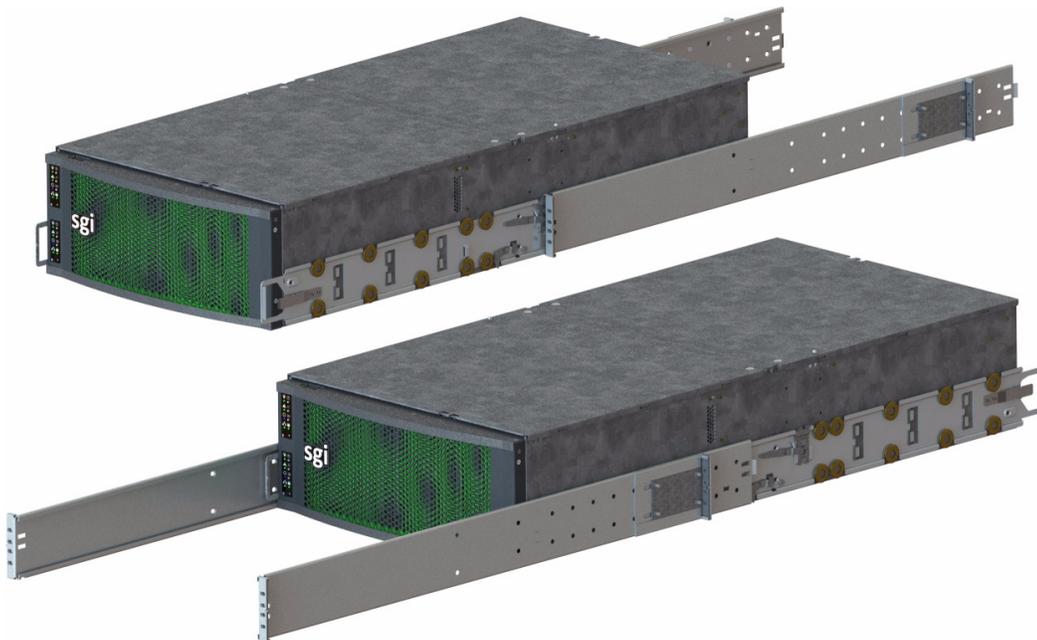
Figure 1-11 Rolling Rails

Shipping Tabs

The MIS rolling rails are shipped with safety shipping tabs to keep the rails from rolling out during shipping. These tabs will need to be removed prior to removing the inner rolling rail from the outer rail.

Figure 1-12   Safety Tab on Rolling Rails

1. Remove the screw holding the safety tab in place using a phillips screwdriver.

2. Remove the shipping tab from the rails.

The rails can now be separated. Keep the tabs and screws in a safe place for possible future use (such as shipping the unit to another location).

Installing the Outer Rails

1. Hold up the outer rails up to the rack to determine if their depth is correct.

2. If the rail cannot be secured to the rack at the front and rear, perform the following steps.

    a. Remove the four screws that hold the rear mounting plate to the rail.

    b. Move the rear mounting plate until the depth of the rail is correct for the depth of the rack.

c. Secure the screws on the adjustment plate firmly in place.

Note: For these next steps, it is helpful to use two people.

d. Use the long phillips screwdriver to fasten the rear screws of the rail to the rack (2 & 5 in Figure 1-13). Keep these screws loose for later adjustment.
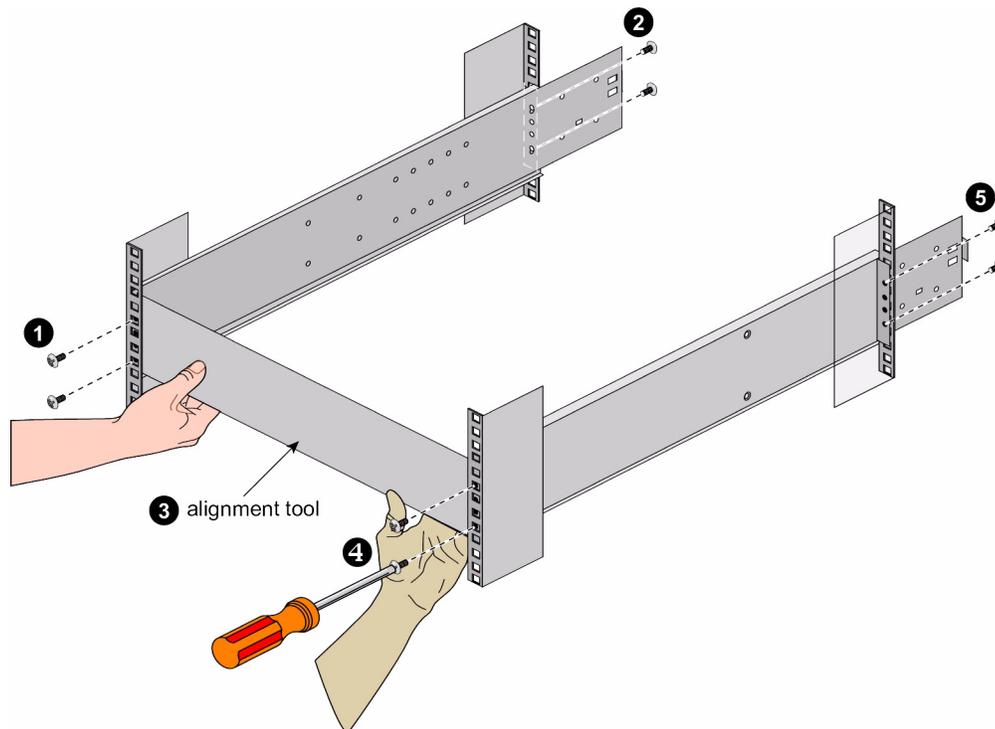
Figure 1-13   Fasten the Rails to the Rack

3. Attach the rail to the rack at the front using the screws provided, keeping them loose for later adjustment (1 & 4 in Figure 1-13).

Aligning the Outer Rails

⚠ **Warning: These steps *must* be taken or the wheels of the inner rail can get bound to the outer rail, causing the chassis to get stuck.**

1. Tighten the screws on the left rail *completely:* middle bolts first (for D-racks), then the front screws, and lastly, the rear.

2. Using the included alignment tool (Figure 1-14), insert it into the rails so that it rests on the inner track of the outer rails, just as a chassis would.
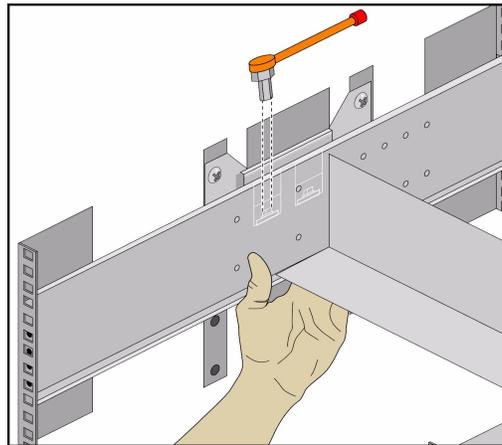
Figure 1-14   Alignment with the D-Rack Stiffener Vertical Bolt

3. Adjust the right rail until it is flush with the alignment tool and the left rail. Ensure that the tool can be slid smoothly from the front to rear of the rack. (This step is also best accomplished with two people, as shown in Figure 1-15.)

Figure 1-15   Adjustment Using the Alignment Tool

4. Tighten the screws on the right rail in order of front then back, leaving the middle bolts last (for D-racks), so as to keep as straight an alignment as possible.

5. Double-check the alignment by moving the alignment tool through the rack. There should be no play between the alignment tool and the rails. (Figure 1-16)

Figure 1-16   Slide the Alignment Tool from Front to Back

6. When satisfied, remove the alignment tool from the rack.

Installing the Air Ducts

The air ducts are installed in the rack and are installed direcly above the rails. The remain in the rack to provide the proper air flow when the chassis is in the stowed position.

1. Place the left air duct above the left rail.

2. Using its mounting screws, attach the air duct to the rack.

Note: Some air ducts use a Velcro strip in place of a second screw. If this is the case, place the hook side of the Velcro on the air duct tab, and the fuzzy size of the Velcro on the outside of the outer rail.

---

3. Repeat this for the right side.
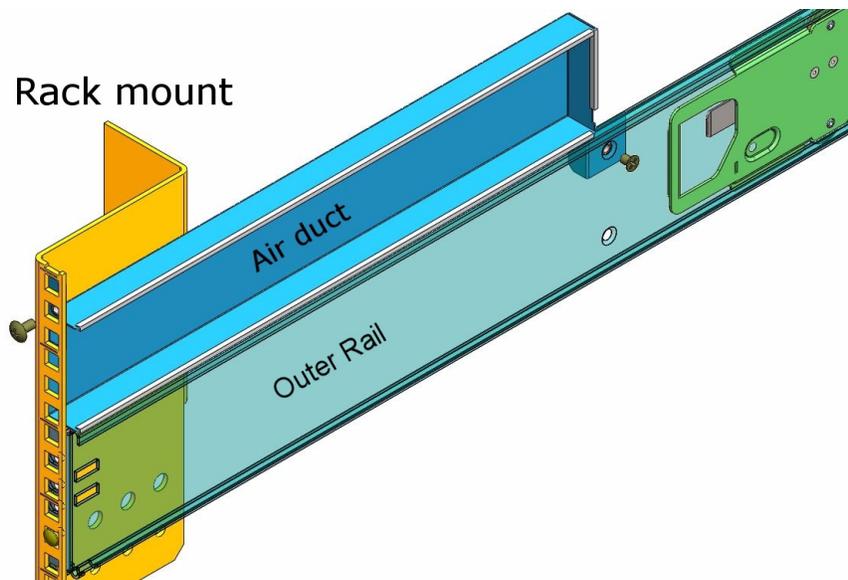
Figure 1-17   Air Duct above Outer Rail

Installing the Inner Rolling Rails

1. Align the rolling rails to the chassis so that the word "**Front**" is at the front of the chassis

---

Note: The word "**Front**" will be upside-down on one side of the chassis (Figure 1-18).
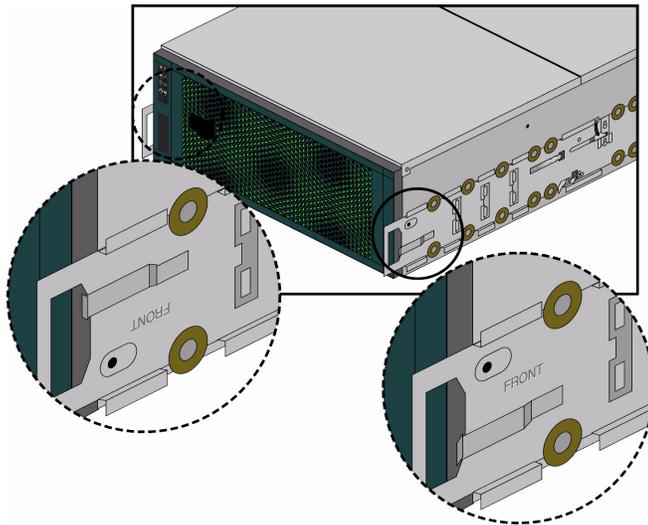
Figure 1-18   Align Rails to **Front**

2. Locate the six support tabs along the side of the chassis (Figure 1-19).
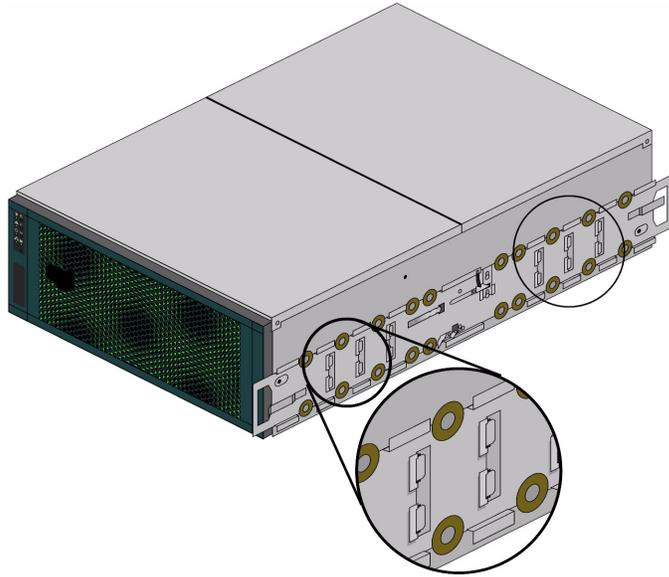
Figure 1-19   Support Tabs

3.   Slide the rolling rail beneath the support tabs on the side of the chassis until it locks firmly
     into place.
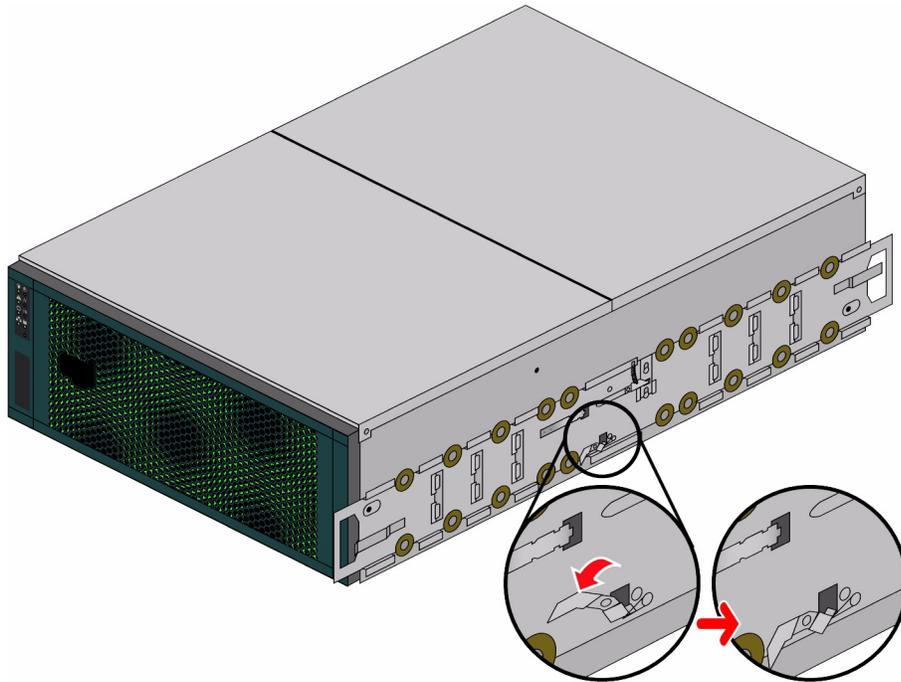
Figure 1-20   Place Safety Latches in Unlatched Position

4. Using the included screws, attach the rolling rail to the chassis. Make sure the screw heads are counter-sunk, so as not to catch on anything when rolling in the rack.

5. You may have to move aside a safety latch in order to install some rolling rail screws. Be sure to set the safety latches back to their home positions after rolling rail installation (Figure 1-21).

Figure 1-21   Return Latch to Home Position

6. Do this for both sides.

Install the Chassis into the Rack

1. Using two people, line up the inner rails on the chassis with the outer rails in the rack. Slide the chassis into the rack.

2. Motion into the rack will stop, by design, when the first set of safety latches on the inner rails catch in position on the outer rails. Move the safety latches to the unlatched position and continue to place the chassis into the rack.

3. Test the motion of the chassis in the rack by moving it forward and backwards in the rack. This should only require one person to roll the rack forwards and backwards. The chassis should catch and latch at 20" from either side of the rack.

Sliding the Chassis Forward/Backwards

To slide the chassis out in either direction, follow these steps:

1. Push the two release latches in, at the left and right sides and in the center of the rail mounts, towards the center of the chassis.

2. Pull the chassis out using the handles. The chassis will latch at the 20" limit.

3. To slide the chassis back in, depress the two release latches near the rail and slide it back in.

Caution: Make sure that only *one* person moves the chassis in the rack at any given time. It is possible to get your fingers caught in the latches on either end if, while you're trying to push the chassis back into a locked position, someone else accidently *pulls* from the other side. This can trap your finger between the metal edges of the rail mount and the rack (potentially resulting in injury). For more precautions, please see "Safety Precautions" on page xvii.

Removing the Front or Rear Chassis Cover

As shown in Figure 1-23, the top of the chassis is bifurcated; that is, there are front and rear chassis covers. Except for power supply maintenance, all service actions require that you remove the front or rear chassis cover, detailed below.

1. Remove the single security screw from the cover (Figure 1-22).

Remove screw
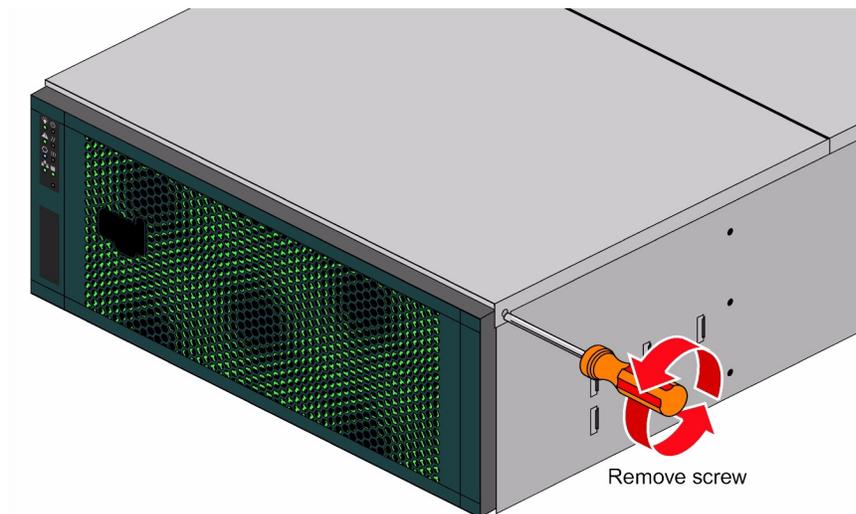
Figure 1-22   Top Cover Security Screw Removal

2. Push the detent, and slide the cover out and up from the chassis.
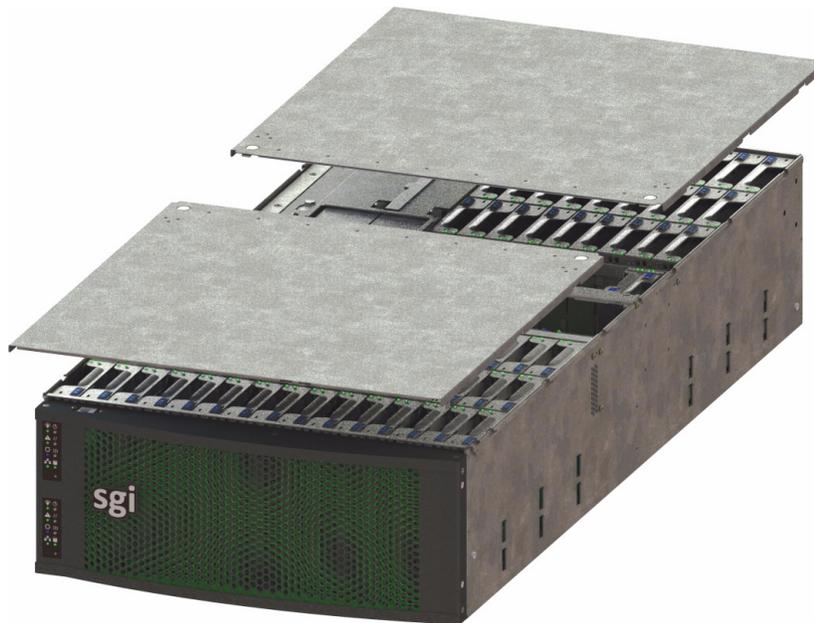
Figure 1-23   Front & Rear Chassis Covers

Selecting Which Side to Access

If you are servicing any of the **fans** or **StorBricks 0-4**, or using the **MIS-S9D Proprietary Network Interface**, access them through the **FRONT** of the rack, and extending the chassis out forward.

If you are servicing the **boot modules**, **StorBricks 5-8**, **server modules**, **JBOD I/O modules**, **internal** or **external cabling**, access them through the **REAR** of the rack, and extending the chassis out backwards.

Table 1-1   Access Points

Target	Access Instructions
Boot Module	REAR access, extend chassis BACKWARDS
Drives in StorBrick 0-4	Extend chassis FORWARD
Drives in StorBricks 5-8	REAR access, extend chassis BACKWARDS

Target	Access Instructions
Exterior Air Ducts	FRONT access, extend the chassis BACKWARDS
External Cabling	REAR access, no need to extend the chassis from the rack
Fans	Extend chassis FORWARD
Internal Cabling	REAR access, extend chassis BACKWARDS
JBOD I/O Modules	REAR access, no need to extend the chassis from the rack
MIS-S9D Proprietary Network Interface Port	FRONT panel, on top of the grille.
Power Supplies	REAR access, no need to extend the chassis from the rack
Server Modules	REAR access, no need to extend the chassis from the rack

Warning: **Only extend ONE (1) MIS chassis out of a rack in either direction at any given time (e.g., one chassis extended backwards and one chassis extended forwards – OK; two or more chassis extended out forwards or backwards – BAD). Too much weight in either direction can potentially tip the rack over, causing injury or death.**

Installing the Drives

Drives are labeled with chassis, StorBrick, and drive information. To install the drives, first slide the chassis forward out of the rack to access StorBricks 0 through 4. Drives are shipped in their drive carriers, and are ready for immediate installation into the StorBricks. To install a hard drive into the StorBrick, perform the following steps.

Warning: **Boot Drives CM0-0 & CM0-1 are the ONLY installed boot drives in single server. Be sure to install them into the correct drive slots. Installing the boot drives in the wrong slot requires a complete reinstall of the operating system once returned to the correct slots. Boot Drives CM0-0, CM0-1, CM1-0, & CM1-1 are all installed in dual sever.**

Boot drives are installed with the raised sheet metal facing outward, away from its partner drive (Figure 1-24).
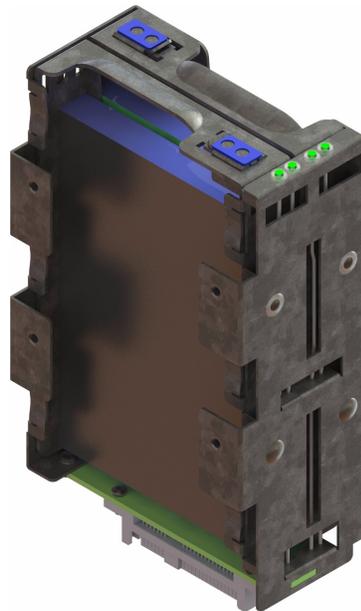
Figure 1-24   Boot Drive Module

Important: Due to thermal requirements, **drive slots 0, 1, and 2 must always be populated in every StorBrick**, with **drives all the same model and size form factor**. This sets up proper air flow through the system.

To install the capacity drives into the StorBricks, perform the following steps.

1. Locate the drives for StorBricks 0-4 and order them on a cart according to the labels on the drive carriers.

2. Pull the chassis from the front of the rack (see "Sliding the Chassis Forward/Backwards" on page 20).
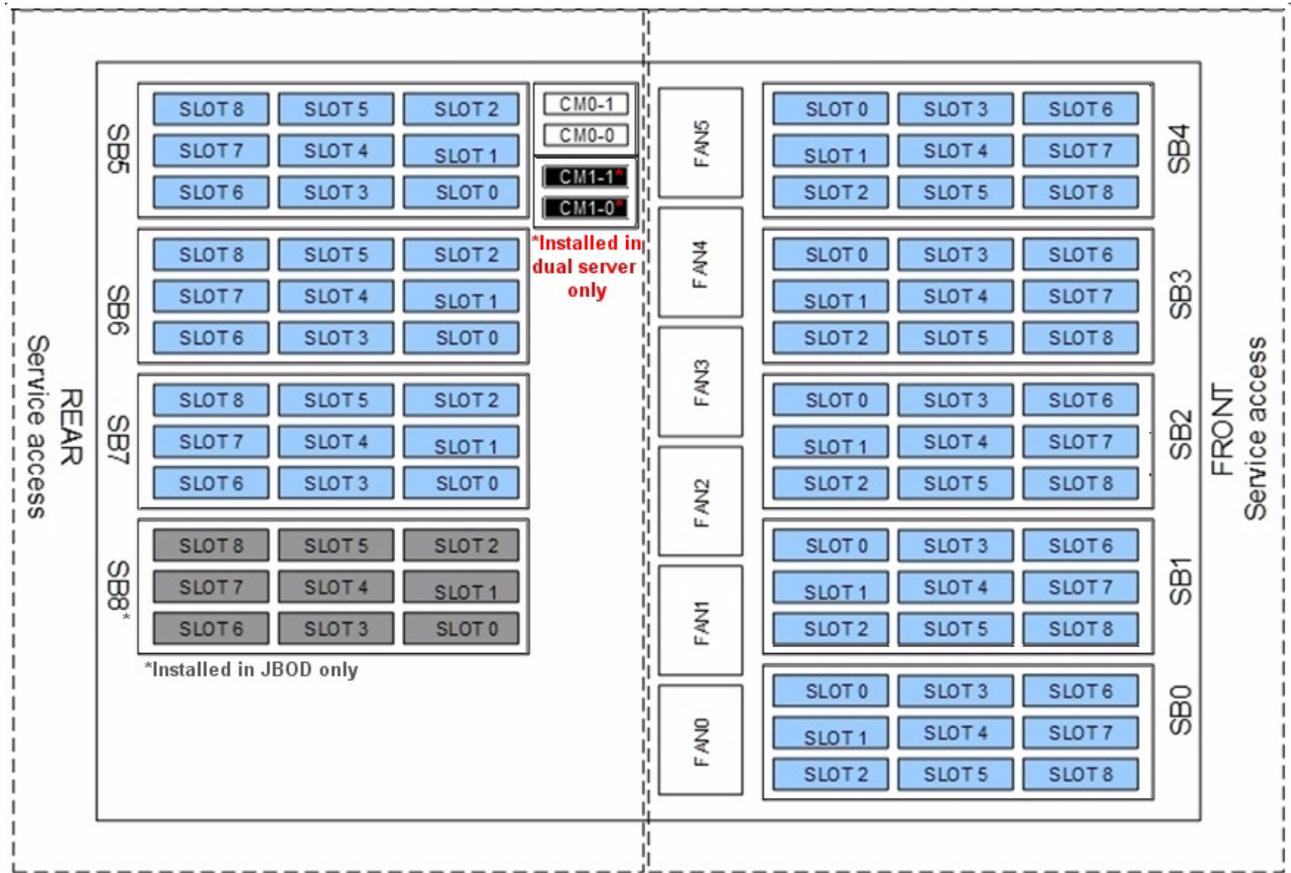
Figure 1-25   System Layout Diagram – Drive & Fan Placement
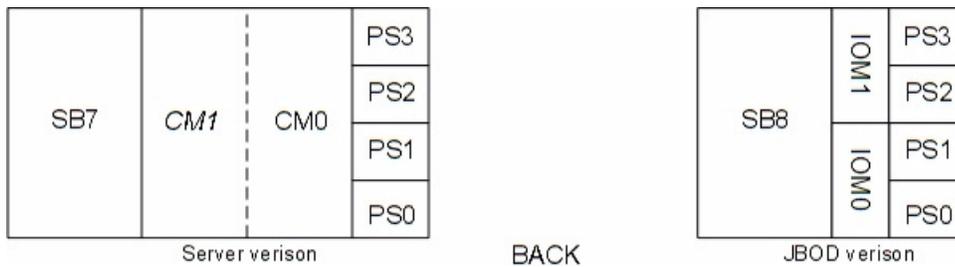
Figure 1-26   System Layout Diagram – Chassis Rear View

3. Remove the front chassis cover by first removing its safety screw, then by pressing the top cover button and lifting the cover from the chassis (see "Removing the Front or Rear Chassis Cover" on page 21).

4. Place the corresponding drive into its drive slot (a system layout diagram, Figure 1-25, is also provided on the inside of one of the top chassis covers). Press the drive firmly into the StorBrick. You will know the drive is in place when the latch on the top of the drive carrier snaps into place.

5. When all drives are in their correct slots, place the top cover on the chassis and secure it with its safety screw.

6. Move the chassis to the stowed position in the rack.

7. From the rear of the rack, move the chassis out backwards and repeat the above steps for the rear of the chassis (StorBricks 5-7 for a server, and 5-8 for a JBOD).

Cable Guide & Chassis Rack Location

For systems that have multiple chassis, determine the proper location for each chassis in the rack: an MIS server platform can support up to four MIS JBOD enclosures.
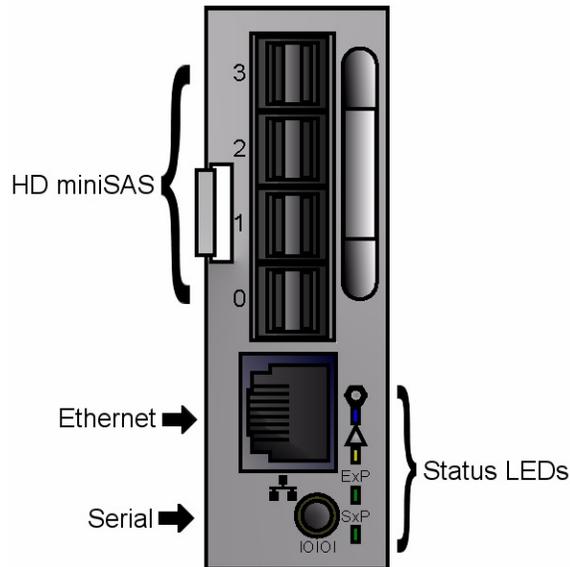
Figure 1-27   JBOD I/O Module Port Diagram

JBODs connect to the MIS Server using an external HBA. JBODs require the presence of an external HBA to connect to the MIS Server. Each HBA can support up to two JBODs, each server can support up to two JBOD HBAs, for a maximum of four JBODs per server.

The top JBOD LED is a blue identification (ID) LED. The second is a green/amber fault LED. Below that is **ExP** (SAS activity of the expander on the StorBricks) activity LED and the **SxP** (SAS activity of the targed SMP for the expander on the StorBricks) activity LEDs. (Figure 1-28)
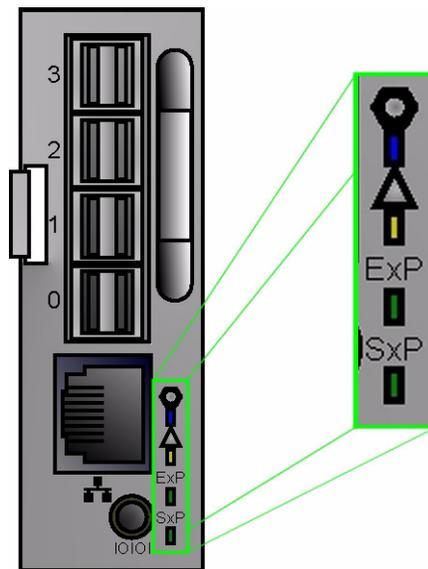
Figure 1-28   JBOD I/O LEDs

The server is always located in the **middle** of the JBOD enclosures, as seen in the layouts in Figure 1-29 through Figure 1-43 (cable colors are for clarity and may not correspond with actual cable colors).

The following are a few suggestions for cable configurations given a single or dual chassis configuration, and a variety of JBODs. **This is by no means a complete list, nor is it the only way to configure connections.**
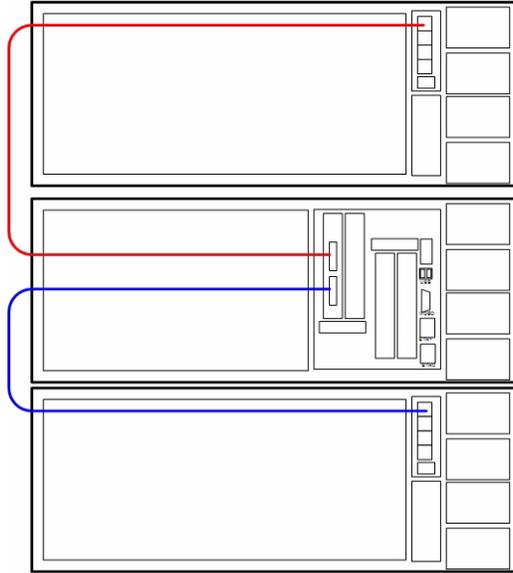
Figure 1-29   Cable Guide – Single Server with two JBODs
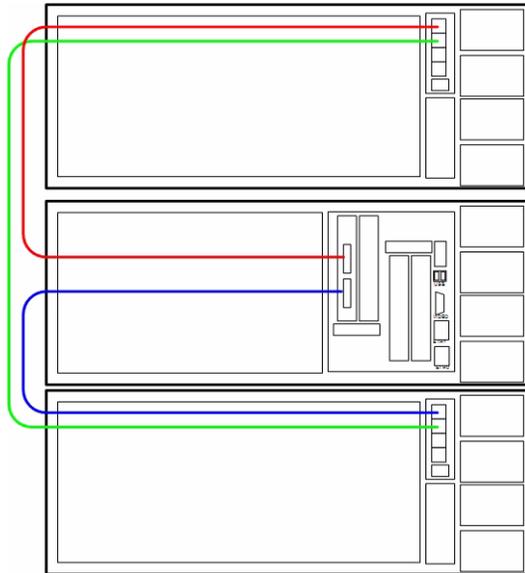
Figure 1-30   Cable Guide – Single Server with two JBODs Shared
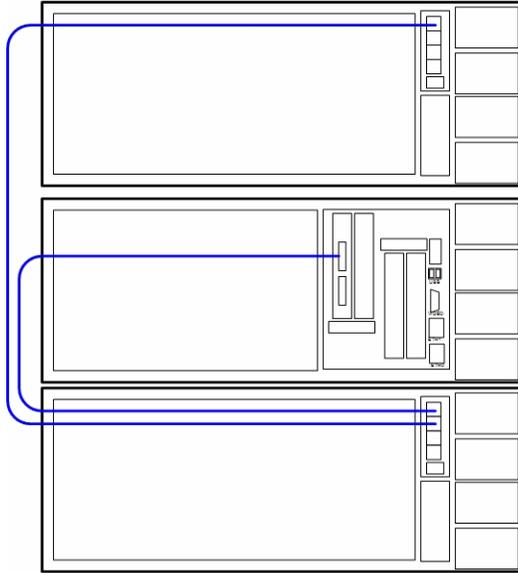
Figure 1-31   Cable Guide – Single Server with two JBODs daisy-chained
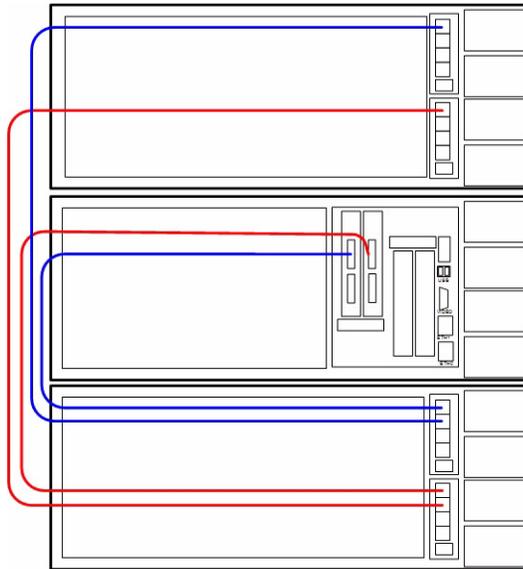
Figure 1-32   Cable Guide – Single Server with two HBAs, 2 JBODs with Dual I/O
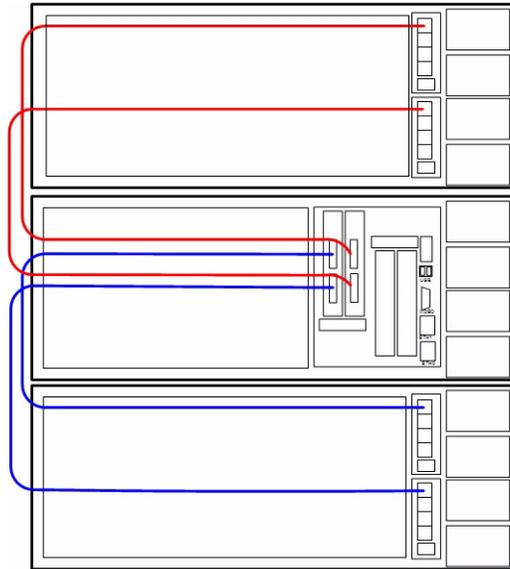
Figure 1-33   Cable Guide – Single Server with 2 HBAs, 2 JBODs with Dual I/O, split
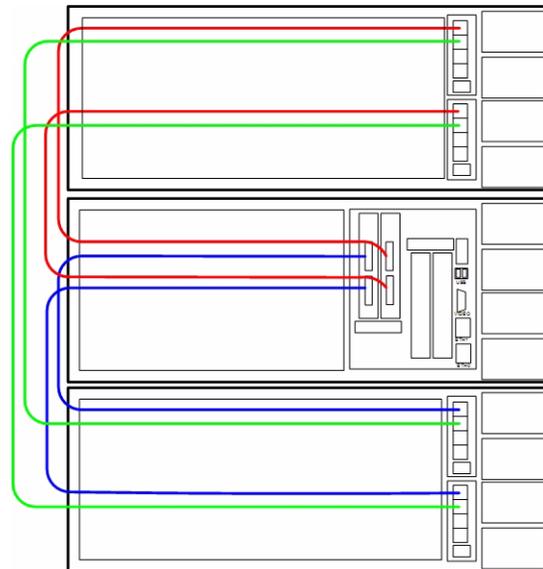
Figure 1-34   Cable Guide – Single Server with 2 HBAs, 2 JBODs with Dual I/O, shared
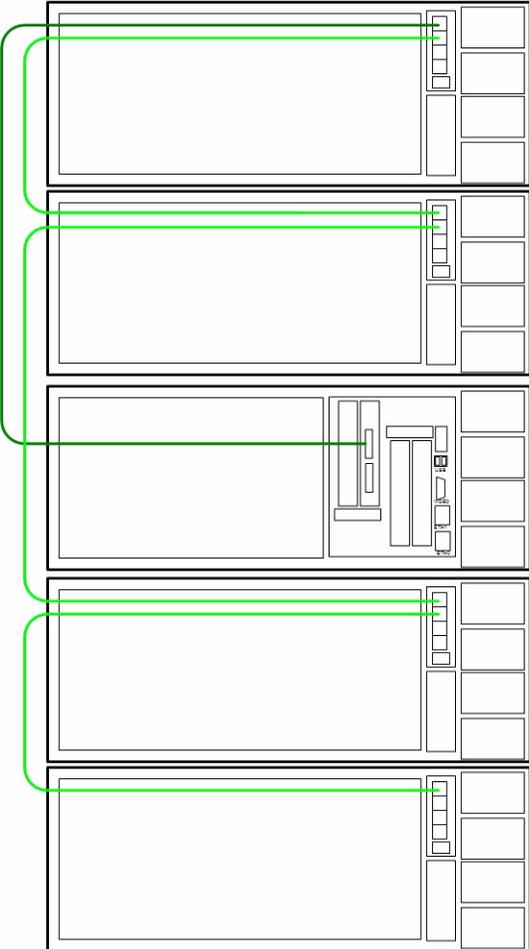
Figure 1-35   Cable Guide – Single Server with four JBODs daisy-chained
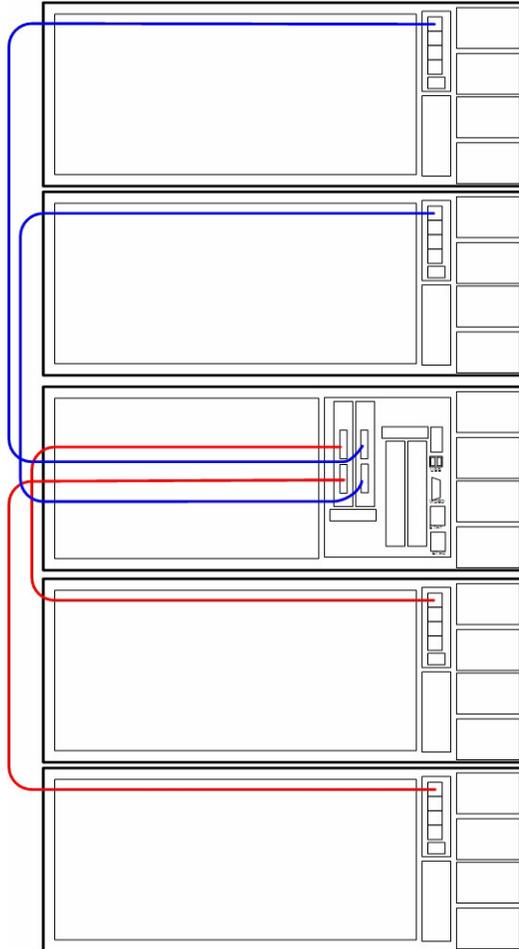
Figure 1-36 Cable Guide – Single Server, Dual HBA, four JBODs
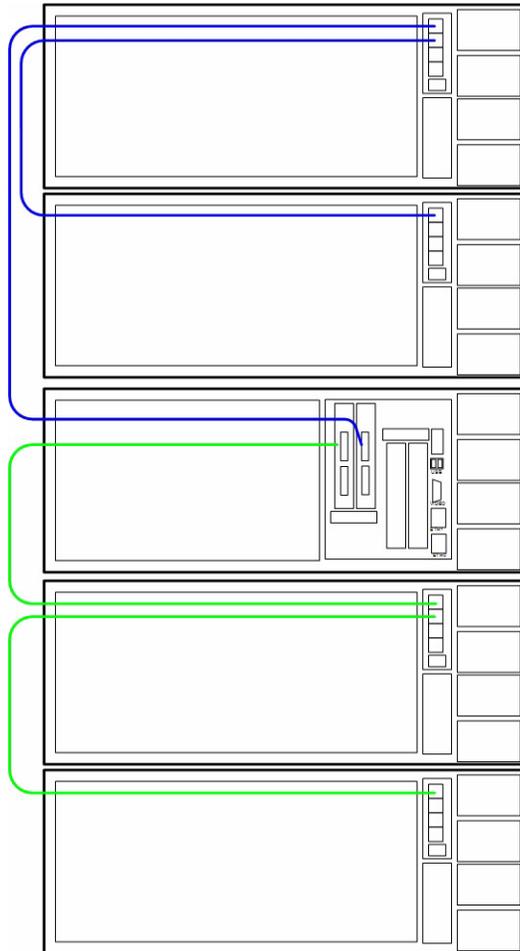
Figure 1-37   Cable Guide – Single Server, Dual HBAs, four JBODs daisy-chained
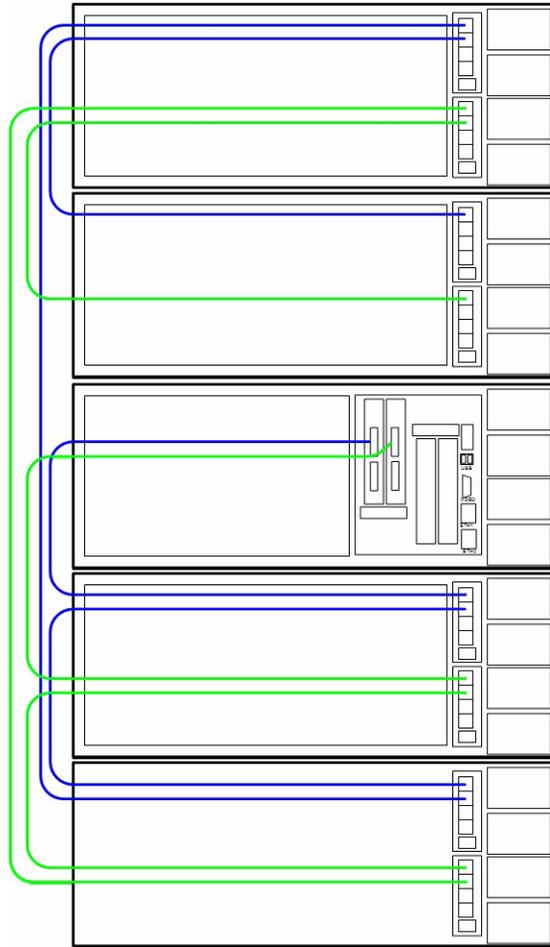
Figure 1-38   Cable Guide – Single Server, Dual HBAs, four JBODs with Dual I/O, split daisy-chain
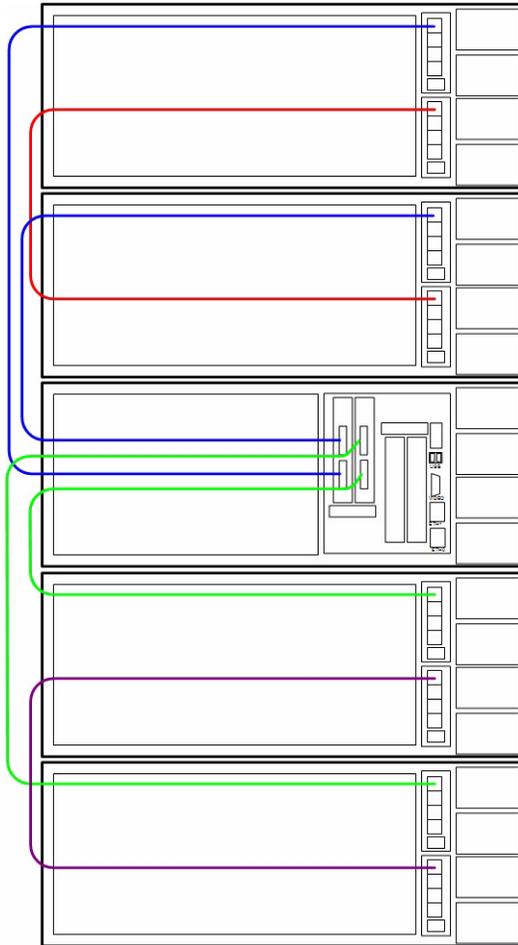
Figure 1-39   Cable Guide – Single Server with Dual HBAs, 4 JBODs with Dual I/O split-share
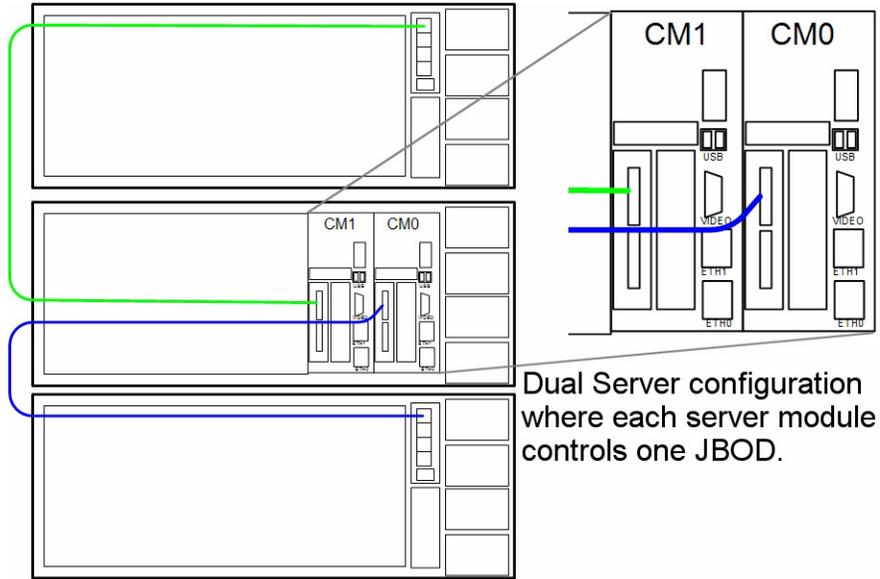
Figure 1-40   Cable Guide – Dual Server with two JBODs
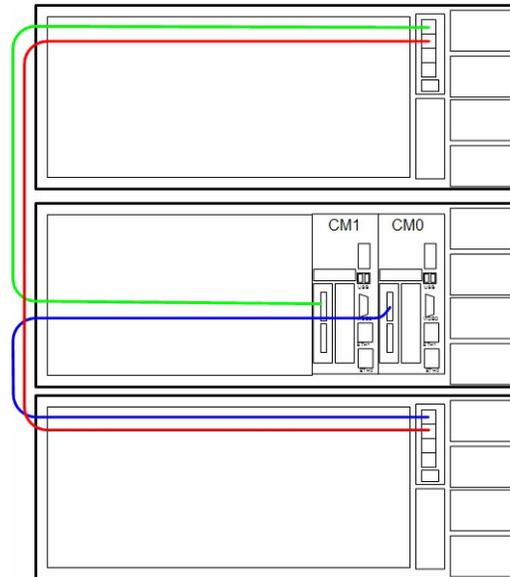
Figure 1-41   Cable Guide – Dual Server with two JBOD shared
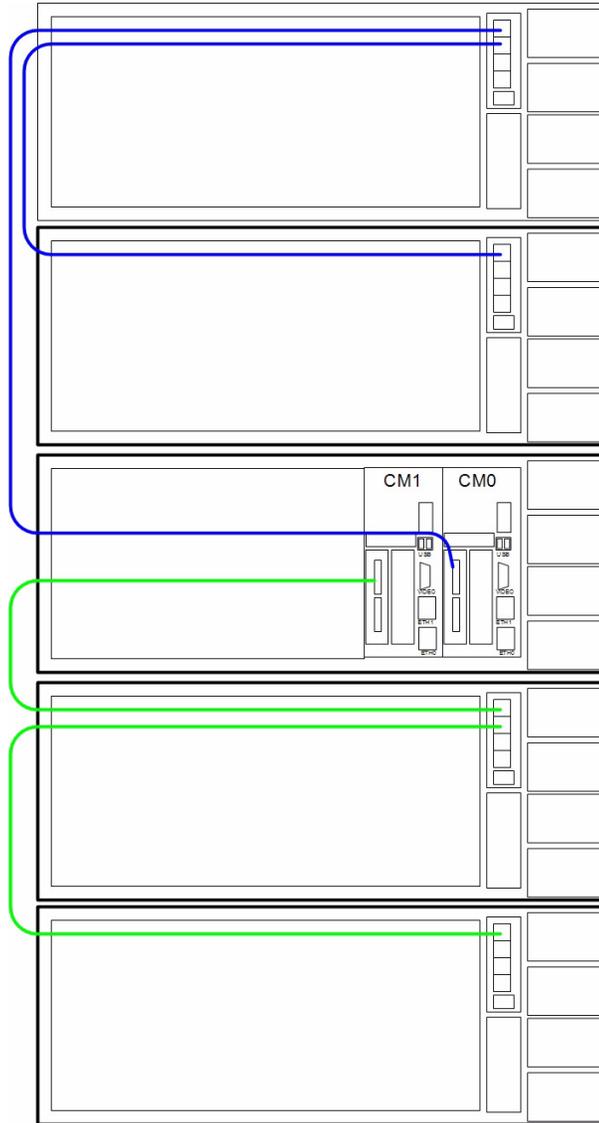
Figure 1-42   Cable Guide — Dual Server with four JBODs
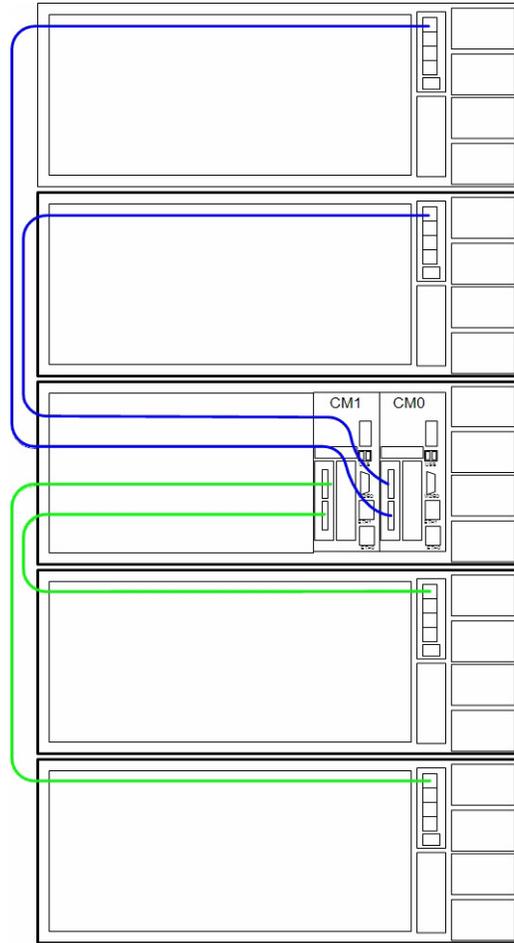
Figure 1-43   Cabling Guide – Dual Server with four JBOD split
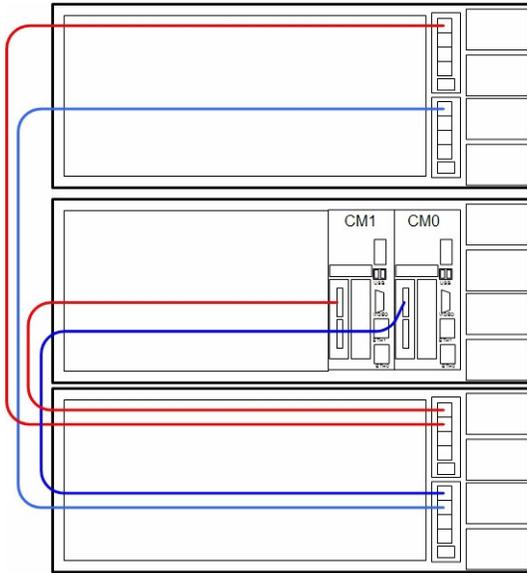
Figure 1-44   Cable Guide – Dual Server with 2 JBODs with Dual I/O
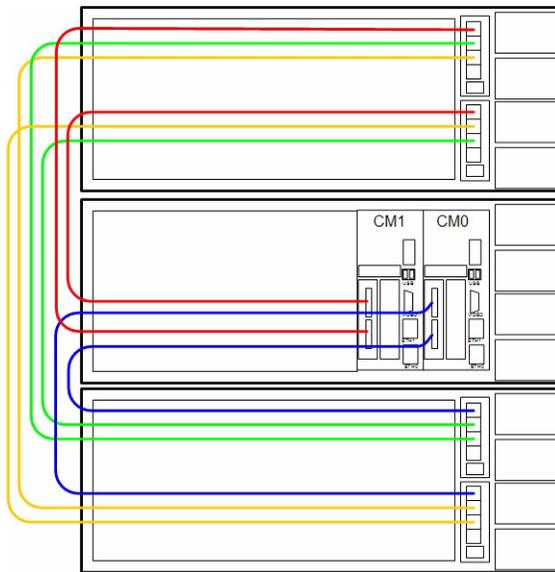
Figure 1-45   Cable Guide – Dual Server with 2 shared JBODs with Dual I/O
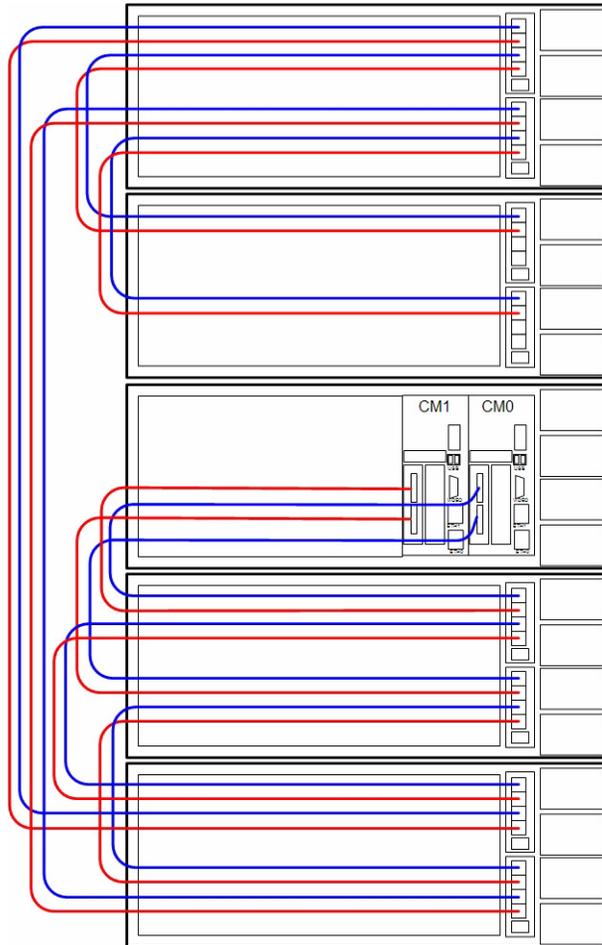
Figure 1-46   Cable Guide – Dual Server with 4 JBODs daisy-chained

Cable Management Arm

The cable management arm is an optional addition to the MIS chassis that helps keep cables organized in the rack. It attaches to a plate on the rear of the MIS chassis and to the rack in which the chassis is mounted. The cable management arm comes in a length designed for 26" deep racks, such as the D-Rack. It can be shortened to accommodate other rack sizes (Figure 1-47).
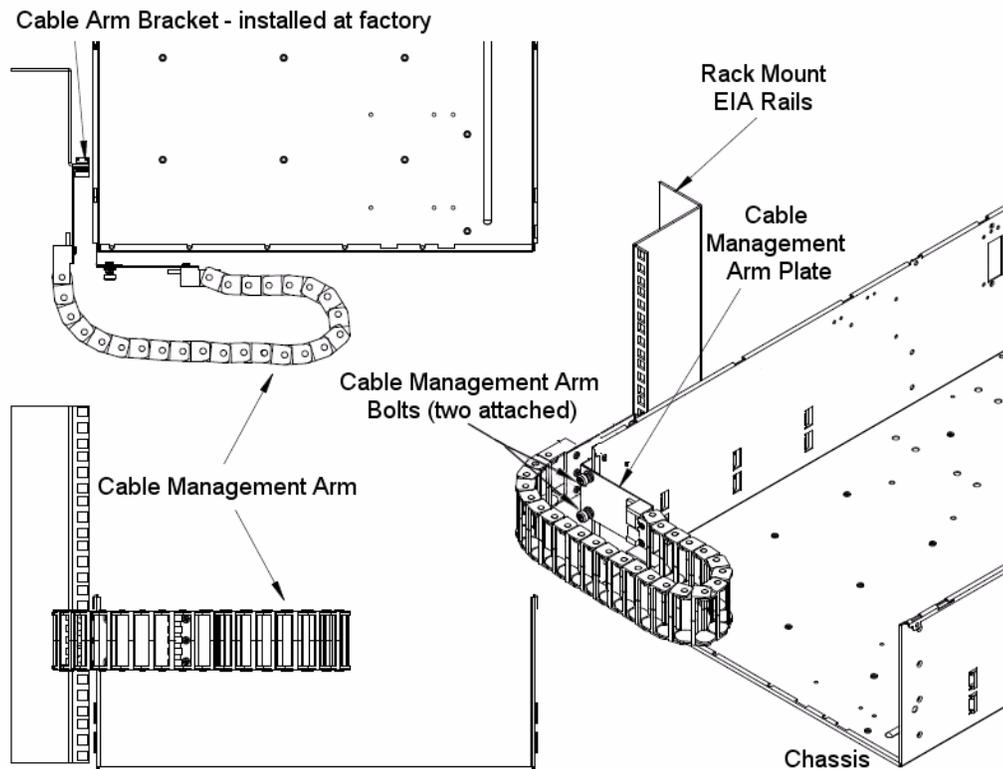
Figure 1-47   Cable Management Arm

Shortening the Cable Management Arm

Removing segments from the cable management arm is done using a thin flat-head screwdriver.

- For a 26" deep rack, do not remove any sections.

- For a 30" deep rack, remove 3 sections of the arm.

- For a 34" deep rack, remove 6 sections of the arm.

There are two ways that segments can be removed: either while the cable management arm is not attached to the chassis or rack, and devoid of cables, or while attached to the rack and chassis, full of cables.

Shortening the Cable Arm While Empty

For the first method, segments are removed from the *end* of the arm. Use the flat-head screwdriver and slip it between the plastic pieces that form the joint of the arm (Figure 1-48).

Figure 1-48   Remove Segments from the End of an Empty Arm

Pry the joint open using the thin blade of the screwdriver by wedging it between the plastic parts that make up the joint and twisting the screwdriver until the outer plastic piece pops off of the inner plastic tab (Figure 1-49).

Figure 1-49   Pry the Joint Apart

Figure 1-50   Pull the Segments from the Arm

The segments are now removed from the end of the arm (Figure 1-50), and the arm can now be attached to the chassis and rack (Figure 1-51).

Figure 1-51   Shortened Arm Ready for Installation

Shortening the Cable Arm While Full

The second way to shorten the cable management arm is while it is already installed on the rack, with cables in it. In this case, the segments are removed from the *middle* of the cable management arm (Figure 1-52).

Figure 1-52   Remove Segments from the Middle of a Full Arm

Pry the joint of a segment open by using the thin blade of a flat-head screwdriver by wedging it between the plastic parts that make up the joint and twist the screwdriver until the outer plastic piece pops off of the inner plastic tab (Figure 1-53).

Figure 1-53   Pry Open the Segment Joint

Repeat for the joint on the other side, then pull the arm apart by sliding it down the cables (Figure 1-54).

Figure 1-54   Pull Apart the Cable Management Arm

Pry apart the segment joint on the other end of the section you wish to remove (Figure 1-55), until the number of unwanted segments have been separated from the rest of the cable arm.

Figure 1-55   Pry Apart the Joint at the Other End

Once complete, separate the section of unwanted segments from the cables by twisting the section off (Figure 1-56).

Figure 1-56   Twisting the Section of Segments from the Cables

Bring the two spliced ends of the cable management arm together, and snap the joint together (Figure 1-57).

Figure 1-57   Join the Spliced Ends of the Cable Management Arm

The cable arm should now be the appropriate length for the depth of the rack.

Installing the Cable Management Arm

To install the cable management arm, first extend the chassis out the rear of the rack ("Sliding the Chassis Forward/Backwards" on page 20). Next, lie the cable management arm on a table with the

open side up. Lay the cables to be attached to the chassis on top, and starting at one end, press the cables into the arm until they snap inside. Continue to press the cables down the length of the arm until they are all inside. Once complete, slide the arm down the cables until there is enough length to allow the arm to be bolted into place on the Cable Arm Bracket (Figure 1-47 on page 41) .

Using the attached bolts, fasten the Cable Management Arm Plate to the Cable Arm Bracket. Then, wrap the arm around itself (as in Figure 1-47). Next, slide the chassis out the front of the rack to be able to access the rack mount EIA side rails. Attach the end arm plate to the EIA rail using the provided screws and nuts. Return the chassis to the stored position in the rack.

The cables can now be connected to their corresponding inputs (power, networking). Once cabling is complete, use the provided velcro strips to wrap the cords and hold them tight (Figure 1-58).

Figure 1-58   Included: Velcro Cable Ties

Turning the Power On

Note: If your MIS came from the factory with the operating system pre-installed, you can power on the system and continue to the 1st-run instructions below. Otherwise, you should install the operating system at this time.

To power-on an MIS server platform, hold down the power button firmly until the fans spin up and the hardware lights come on. This will initialize the the machine's BIOS and start internal diagnostics, including hardware status, RAID Volume information, missing hardware alerts (e.g., missing batteries), and missing configuration alerts. This process will be repeated for each

expander in the machine, and finally (if conditions allow), the machine's operating system will load and the welcome/login screen appear.

If the machine is powering on and there is a fault (e.g., the machine was in the middle of a rebuild when the power was cut, a degraded RAID set is in the system, battery is exhausted, etc.), these warnings will appear during start-up.

If the platform is an MIS dual server and both servers are powered down, performing the above steps powers on the server with which you are working, the drives, and the fans. The second server will remain powered off until it is powered on, then all power will be turned on.

For a JBOD unit, the power button on the front panel will turn on the power to that I/O module, the fans and the drives. If a second module is installed and powered off, it will remain off until it, too, is powered on.

1st-Run Instructions

Before using your new MIS system, there are some first-run steps that will need to be taken to configure the platform for use. These are necessary steps that are performed once during set-up, and then require little to no follow-up once complete. For example, one or both LAN channels must be configured as either DHCP or static addresses, and at least one user account must be enabled to use the LAN channel(s), before the Server Management BMC LAN or the Intel RMM4 can be utilized. The 1st-run steps include:

- "Entering the BIOS" on page 50,

- "Setting User Accounts" on page 51,

- "Configuring BMC DHCP Host Name" on page 52,

- "Setting the BMC IP Address" on page 52

- "Configure Intel® Rapid Storage Technology enterprise (RSTe)" on page 53,

- "Enabling IPMI on a Linux System" on page 56,

- "Accessing IPMI on a Linux System" on page 56.

Safe Power-Off

There are different ways to shut down an MIS machine. The preferred method is to go into the machine's operating system and select **Shut Down**. This will prompt the user to enter a password before allowing the shut-down process. Other ways to power off the machine include:

- Using the OS GUI power-off procedure at the console screen, if a keyboard/mouse/video monitor is connected.

- When logged in via an ssh session and executing an IPMItool `power off` command.

- When logged in to the BMC and using the remote front panel to power off the sever.

- Using the remote console screen connection to the OS GUI power-off procedure, if a KVM RMM4Lite session is established through the BMC.

- Connecting to the Fan Base Service Page using the MIS-S9D proprietary network interface and using the **Shutdown** button.

If the platform is an MIS dual-server and **both** servers are powered up, performing the above steps **only** powers off the server with which you are working. The fans, drives and second server will remain powered on until the second server is powered off, then all power (but standby) will be turned off.

For a JBOD Unit, the power button on the front panel will turn off the power to that I/O module. If a second module is installed and powered on, it, the fans and the drives will remain on until it, too, is powered off.

One additional way to shut down the platform is to hold down the **Power** button on the front of the unit until the machine powers off. However, this forces the machine off and does not allow the machine to go through normal shut-down procedures, requiring a recovery process at start-up.

To shut down using IPMItool, use the following commands:
On a local server: # **ipmitool power off**
For a remote server: # **ipmitool −H** <host> **−U** <user> **−P** <pswd> **power off**
For example: # **ipmitool −H 137.8.64.3 −U admin −P Password01 power off**
where the host IP address is 137.8.64.3, the user is admin with the password: Password01.

If power is lost from outside the machine (power outage), the machine will recognize the loss of power and execute an emergency shutdown procedure. If there is a battery back-up unit installed, it will protect integrity of cache in the event of power or server failure.

Entering the BIOS

Many of the 1st-run steps require entering the BIOS setup during the platform's Power-On Self-Test (POST). Configuration of the Server Management BMC LAN and the Intel® RMM4 is done using BIOS setup. When the BIOS is entered, the Main screen is usually displayed. However, serious errors cause the system to display the Error Manager screen instead of the Main screen.

1. To enter setup, press **F2** when prompted (Figure 1-59) or during the first splash screen (if **Quiet Boot** is **Enabled**, no prompt will be shown).
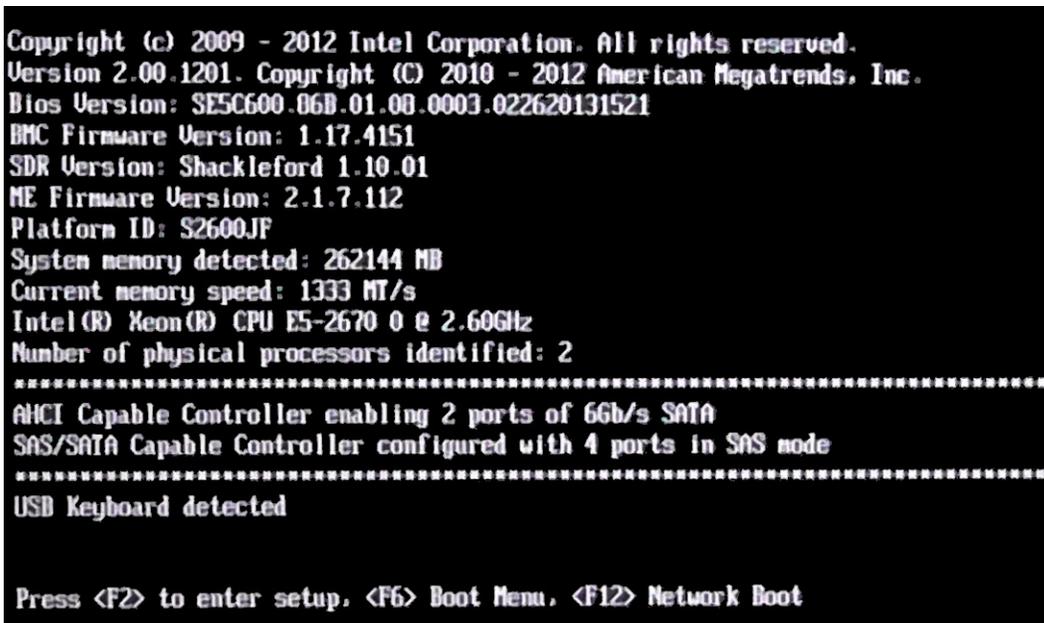
Figure 1-59   POST Prompt to enter Setup

2. In the BIOS setup, navigate to the **Server Management** tab and press **Enter** to select.

3. Scroll down to **BMC LAN Configuration** and press **Enter**.

When first powered on, by default, the **Server Management BMC LAN** and **Intel® RMM4** both have a static IP address of **0.0.0.0** (Figure 1-60).

4. To configure the **Server Management BMC LAN**, scroll to **IP source - IP source**, and select **Dynamic** or **Static**.
    If static is chosen, enter in the **IP address**, **Subnet mask**, and **Gateway IP** to be used.

5. Hit the **F10** key to save your changes.

Important: `Intel (R) RMM4 LAN configuration` is not used, as LAN Channel 3 is not available. Because of the configuration of the server modules, the riser that is normally used for the Intel Dedicated Management NIC is actually used for Riser 2 connectivity in SGI Server Modules. As such, the Intel Dedicated Management NIC cannot be used in SGI server modules, and LAN Channel 1 is shared between the BMC and the operating system.

Setting User Accounts

User accounts **must** be configured to enable login authentication for the Integrated BMC Web Console, otherwise it will not be available for use. To configure email accounts, scroll down to **User Configuration** on the **Server Management** page. Up to five BMC User IDs can be configured: **anonymous** (*cannot* be used to log into the BMC), **root**, and **User 3-5**.


```
          Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
                        Server Management

  BMC LAN Configuration                              Select BMC IP source. When
                                                     static option is selected, IP
  IP source                  IP source               address, subnet mask and
  IP source                  [Static]                gateway are editable. When
  IP address                 10.10.20.170            dynamic option selected, these
  Subnet mask                255.255.255.0           fields are read-only and IP
  Gateway IP                 0.0.0.0                 address is acquired
                                                     automatically (DHCP).
  Intel (R) RMM4 LAN configuration
  Intel (R) RMM4             Present
  IP source                  [Static]
  IP address                 10.10.10.170
  Subnet mask                255.255.255.0
  Gateway IP                 0.0.0.0
                                                     →←: Select Screen
                                                     ↑↓: Select Item
  User configuration                                 Enter: Select
  User ID                    [anonymous]             +/-: Change Opt.
  Privilege                  [Administrator]         F1: General Help
  User status                [Enabled]               F9: Setup Defaults
  User name                  anonymous               F10: Save  ESC: Exit
  User password

          Version 2.00.1201. Copyright (C) 2010 American Megatrends, Inc.
```

Figure 1-60   BIOS – Server Management Page

1. Scroll down to **User ID**. Select the **User** that you want to use and hit **Enter**.

2. Scroll down to **User status** and select **Enabled**.

3. Scroll down to **User password** and change the password. You will have to enter the password twice.

Important: User name and password are cAsE sEnSiTivE.

---

4. When complete, hit the **F10** key to save your settings.

Configuring BMC DHCP Host Name

In order to be able to configure DHCP Host Name, at least one of either **Server Management BMC LAN** and **Intel® RMM4** must be set to receive their **IP address** as **Dynamic** (see "Setting User Accounts" on page 51). Otherwise this options will not be available.

To change this option, complete the following instructions.

1. Go to the **Server Management** page in the BIOS and navigate to **BMC DHCP Host Name**.

1. Hit **Enter** to select **BMC DHCP Host Name**.

2. Enter in the IP address and hit **Enter**.

3. Hit **F10** to save.

Setting the BMC IP Address

The BMC shares NIC 1 in a server module with the operating system. To access the BMC via IPMItool on a remote system or via the Integrated BMC Web Console, you must configure the BMC with its own IP address. The BMC is configured to obtain an IP address through DHCP by default.

1. The BMC IP Address is set during POST, by pressing **F2** to go into the BIOS.

2. Next, navigate to the **Server Management** tab (Figure 1-61), scroll down to **BMC LAN Configuration** and press **Enter**.

3. Scroll down to **IP Source** and select **Static**.

4. Configure the **IP Address**, **Subnet Mask**, and **Gateway IP** as required.

```
                Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
                             Server Management

    BMC LAN Configuration                                    Select BMC IP source. When
                                                             static option is selected, IP
    IP source                      IP source                 address, subnet mask and
    IP source                      [Static]                  gateway are editable. When
    IP address                     10.10.20.170              dynamic option selected, these
    Subnet mask                    255.255.255.0             fields are read-only and IP
    Gateway IP                     0.0.0.0                   address is acquired
                                                             automatically (DHCP).
    Intel (R) RMM4 LAN configuration
    Intel (R) RMM4                 Present
    IP source                      [Static]
    IP address                     10.10.10.170
    Subnet mask                    255.255.255.0
    Gateway IP                     0.0.0.0
                                                             →←: Select Screen
                                                             ↑↓: Select Item
    User configuration                                       Enter: Select
    User ID                        [anonymous]               +/-: Change Opt.
    Privilege                      [Administrator]           F1: General Help
    User status                    [Enabled]                 F9: Setup Defaults
    User name                      anonymous                 F10: Save  ESC: Exit
    User password


                Version 2.00.1201. Copyright (C) 2010 American Megatrends, Inc.
```

Figure 1-61   BIOS Server Management Tab

5. Press **F10** to save your settings.

Important: Keep a record of the **DHCP Host Name** and assigned **IP address**. These will be needed later when you are trying to connect to the Integrated BMC Web Console.

Configure Intel® Rapid Storage Technology enterprise (RSTe)

By default, any MIS platform that ships from SGI with an operating system installed from the factory will have RSTe enabled to allow mirroring of the boot drives. If a system is shipped *without* an operating system installed, RSTe will need to be enabled from the BIOS.

1. In the BIOS, select the Advanced tab, navigate to Mass Storage Controller Configuration and press **Enter** (Figure 1-60).

2. Navigate to **SAS/SATA Capable Controller** and hit **Enter**.

```
        Aptio Setup Utility - Copyright (C) 2010 - 2012 American Megatrends, Inc.
    Main  Advanced  Security  Server Management  Boot Options  Boot Manager            ▶

  ▶ Processor Configuration                        View/Configure mass storage
  ▶ Power & Performance                            controller information and
  ▶ Memory Configuration                           settings.
  ▶ Mass Storage Controller Configuration
  ▶ PCI Configuration
  ▶ Serial Port Configuration
  ▶ USB Configuration
  ▶ System Acoustic and Performance Configuration




                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F9: Setup Defaults
                                                   F10: Save  ESC: Exit



        Version 2.00.1201. Copyright (C) 2010 - 2012 American Megatrends, Inc.
```

Figure 1-62   BIOS – Advanced tab, Mass Storage Controller Configuration

3. In the pop-up window that appears, select **Intel(R) RSTe** and hit **Enter** (Figure 1-63).


```
                                          SATA mo
  ┌── SAS/SATA Capable Controller ──┐ Te ia
  │ Disabled                        │
  │ INTEL(R) ESRT2 (LSI*)           │
  │ INTEL(R) RSTe                   │        Sel
  └─────────────────────────────────┘        Sel
                                             r:
                                          +/-: Ch
```

Figure 1-63   BIOS – Intel(R) RSTe Selection

4. Hit **F10** to save your changes and **Esc** to exit BIOS. The machine will now reboot.

5. At POST, hit **Ctrl** + **i** to enter the **Intel® Rapid Storage Technology enterprise** user interface (Figure 1-64).

From here you can create the RAID volume to mirror the boot drives and enable hot-swappable capability. For more information refer to *Intel® Rapid Storage Technology enterprise (Intel® RSTe) for Linux OS Software User's Guide* or *Intel® Rapid Storage Technology enterprise (Intel® RSTe) for Microsoft Windows* Operating System Software User's Guide*.

Figure 1-64 Intel Rapid Storage Technology enterprise (RSTe) User Interface

Intelligent Management Platform Interface (IPMI 2.0)

IPMI 2.0 is a standardized computer system interface used by system administrators for out-of-band management of computer systems and monitoring of their operation. The development of this interface specification was led by Intel Corporation. IPMI is a message-based, hardware-level interface specification: an IPMI subsystem operates independently of the operating system (OS) (i.e., out-of-band). This allows administrators to manage a system remotely in the absence of an operating system, before an OS has booted (allowing e.g. BIOS settings to be remotely monitored or changed), when the system is powered down, or after OS or system failure, which is the key characteristic of IPMI compared with in-band system management (such as, by remote login using SSH). Multiple disparate servers can all be managed together using IPMI because of its standardized interface and protocol.

The BMC supports LAN Alerting in the form of SNMP Traps that follows the Platform Event Trap format. SNMP Traps are typically sent as unreliable datagrams. However, IPMI includes PET Acknowledge and retry options that allow an IPMI-aware remote application to provide a positive acknowledge that the trap was received. Alert-Over-LAN notifies remote system management applications about PEF selected events, regardless of the state of the server's operating system. LAN alerts can be sent over any of the LAN channels supported by a system. IPMI is used, particularly, to enable email alerts for power supply failures.

Programs such as IPMItool for Linux and IPMIutil for Windows are industry freeware standards that can both be used to configure and issue IPMI commands. IPMI must be enabled in Linux to access these features. The Microsoft IPMI device driver is automatically installed with Windows Server 2008.

Enabling IPMI on a Linux System

To use IPMI on a Linux system, the ipmi service must be running. Use the # service ipmi status command to determine if the service is running.

If the service is running, the output will be similar to:
```
# service ipmi status
ipmi_msghandler module loaded.
ipmi_si module loaded.
ipmi_devintf module loaded.
/dev/ipmi0 exists.
```

If the service is not running, use the # ipmi service start command to start the service.
```
# service ipmi start
Starting ipmi drivers:                                        [  OK  ]
```

Accessing IPMI on a Linux System

To access IPMI from a remote system, the BMC on the local system must be configured for network access. (Refer to "Setting the BMC IP Address" on page 52 for the procedure to enable network access.) On a local system, simply use the ipmitool command with the command it should run: # **ipmitool <**command**>**.

For example:
```
# ipmitool power status
Chassis Power is on
```

From a remote system, you must also specify a host, user, and password to access the system:
```
# ipmitool −H <host> −U <user> −P <password> power status
```

For example, the host here is at the IP address **137.38.64.3**, the user is **admin**, and the password is **Password1**:
```
# ipmitool −H 137.38.64.3 −U admin −P Password1 power status
Chassis Power is off
```

Enabling System Monitoring

Once configured, when a system component fails, the BMC sends an alert (when configured to do so; see "Alert Email" on page 69 for more information). Capacity drive failures are recognized and reported through MegaRAID Storage Manager (MSM). Boot drive failures are monitored and reported through mdadm. Fan and power supply failures are monitored through the fan baseboard and are reported by the BMC, with a few adjustments. This section explains how to set up monitoring on system modules.

BMC Integrated Web Console

The BMC Integrated Web Console is a web-based program provided by Intel, and is used to give general system information such as system diagnostics, server health, environmental reporting, and event logs. Additionally, the BMC-IWC provides a remote virtual control panel for the MIS Server, allowing for remote locating and reboot.

Configuration Tab

The Configuration tab of the BMC Web Console is used to configure various settings, such as alerts, users accounts for the BMC, and network settings. It contains the following menu options in the left navigation pane: **IPv4 Network**, **IPv6 Network** (not used), **Users**, **Login**, **LDAP**, **VLAN**, **SSL**, **Remote Session**, **Mouse Mode**, **Keyboard Macros**, **Alerts**, **Alert Email**, and **Node Manager**.

Alerts

The **Alerts** page allows you to configure which system events generate alerts and the external network destinations to which they should be sent. When one of the selected system events occurs, an alert is generated and sent to the configured destination(s). Each LAN channel can have up to two destinations.
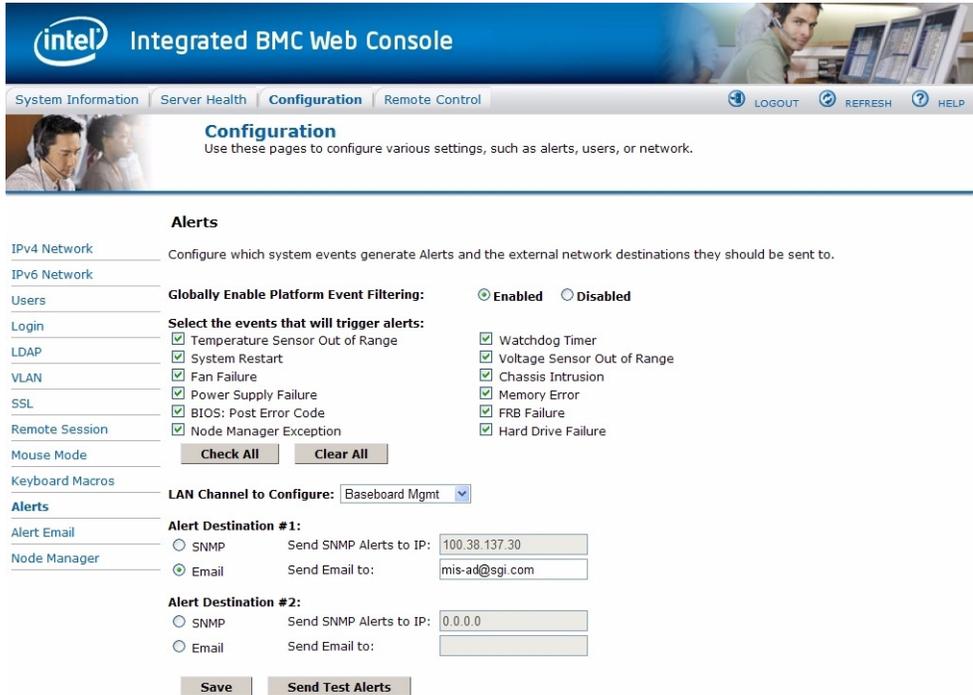
Figure 1-65   BMC Web Console – Alerts Page

To receive alerts for power supplies, see "Power Supply Monitoring" on page 69. The fan base firmware will monitor all Power Supply Units (PSUs) installed in the system and generate SEL entries regardless of whether or not the alerts are enabled. This functionality cannot be turned off.

Globally Enable Platform Event Filtering

Global control for enabling or disabling platform event filtering. This can be used to prevent sending alerts until you have fully specified your desired alerting policies.

Warning: Do NOT disable except under explicit instruction from SGI Technical Support. When filtering is globally disabled through this setting, alerts (such as power supply faults) will *not* be sent.

Select Events

Select one or more system events that will trigger an Alert. These events correspond to the 13 IPMI preconfigured Platform Event Filters (PEFs) set by Intel. This area only allows the selection of those 13 PEF filters configured by Intel: **Temperature Sensor Out of Range**, **System Restart**, **Fan Failure**, **Power Supply Failure**[1], **BIOS: POST Error Code**, **Node Manager Exception**[2], **Watchdog Timer**, **Voltage Sensor Out of Range**, **Chassis Intrusion**, **Memory Error**, **FRB Failure**, **Hard Drive Failure**[3].

> **Warning:** **Clearing all events disables Alerts.**

LAN Channel

Select which LAN channel to configure destinations for. Each LAN channel has its own set of up to two destinations. Alert destinations can be one of two types:

- SMTP Trap

- Email (requires Alert Email to be configured)

The **Check All** button selects all events to generate Alerts. The **Clear All** button unchecks all events so no Alerts will be generated. Click the **Save** button to save any changes made.

Send Test Alert

To test whether an alert will reach its destination, set the **LAN Channel** field to the desired channel and configure at least one destination. Then click **Send Test Alerts** to send a simple test alert to the destination(s) for that channel.

---

[1] Not used by SGI – Power Supply failure is reported through the BMC, but Power Supply Alerts are not configured through this interface. Instead, power supply failure is reported by configuring Platform Event Filters 5, 19, and 20.

[2] Requires configuration of Node Manager.

[3] Boot drives only. Capacity Drives are monitored using MegaRAID Storage Manager software ("Creating the Drive Groups in MegaRAID (CentOS, Linux & Windows)" on page 102).

Alert Email
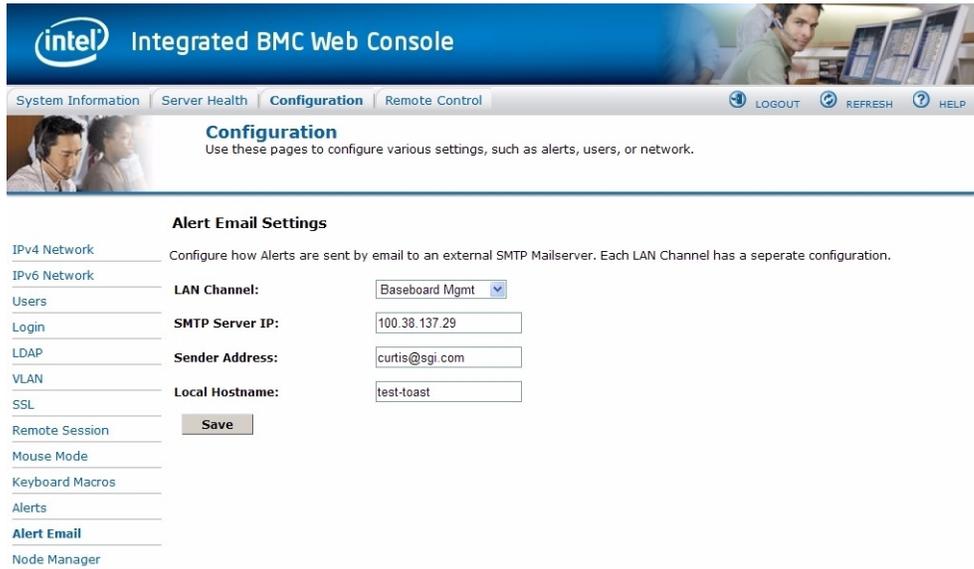
Figure 1-66   BMC Web Console – Alert Email Settings

Alert Email Settings allows you to configure how Alerts are sent by email to an external SMTP Mailserver. Each LAN Channel has a separate configuration, selected through the drop-down menu. The **SMTP Server IP** is the IP address of the remote SMTP Mailserver that Alert email should be sent to. The **Sender Address** is the string to be put in the `From:` field of outgoing Alert emails. **Local Hostname is** a name for the local machine that is generating the alert, and this name is included in the outgoing Alert email. The **Local Hostname** is a string of maximum 18 alpha-numeric characters. Spaces and special characters are not allowed.

Once these settings are saved, you can go to the previous Alerts screen and click the button **Send Test Alert**. If the **SMTP Server IP** address is correct, an email containing hexadecimal code should be sent to the emails configured on the Alerts page. To understand what these hex codes mean, see Intel's *System Event Log Troubleshooting Guide for EDSP Platforms Based on Intel Xeon Processor E5 4600/2600/2400/1600/1400 Product Families* (http://download.intel.com/support/motherboards/server/sb/g90620001_s1400_s4600_systemev entlog_troubleshooti.pdf).

In this example, the mail server's IP address is `100.38.137.29`. When the **Send Test Alert** button is pushed, it creates an alert email from the `Sender Address` (in this example,

Figure 1-67, `curtis@sgi.com`), with the heading "**Alert from <Local Hostname>**" (in this example, the local hostname is `test-toast`).

Figure 1-67   BMC Web Console – Alert Email Result

The resulting hex code in the email can be translated using the code tables given in Intel's *System Event Log Troubleshooting Guide for EDSP Platforms Based on Intel Xeon Processor E5 4600/2600/2400/1600/1400 Product Families*. In our example, the hex code includes the record identification (**RID**), a time stamp for when the event was generated in `MM/DD/YYYY HH:MM:SS` format (**TS**), the number of the sensor that generated the event (**SN**), they sensor type code (**ST**), event directory (**ED**), event type – Asserted or Deasserted (**ET**), event code (**EC**), record identification used for SEL record access (**RID**), record type in Hex code (**RT**), time stamp for when the event was logged (**TS**), generator identification in hex including RqSA and LUN if the event was generated from the IPMB software and software identification if the event was generated from system software (**GID**):

- 0001 – BIOS POST for POST errors, RAS Config/State, Timestamp Synch, OS Boot events

- 0033 – BIOS SMI Handler

- 0020 – BMC Firmware

- 002C – ME Firmware

- 0041 – Server Management Software

- 00C0 – HSC Firmware HSBP A

- 00C2 – HSC Firmware HSBP B

In the example above (Figure 1-67), you'll notice that the **GID** is `0020`, indicating correctly that the alert was sent from the BMC Firmware.

Continuing with the hex code contained within the email, ER is the IPMI version in use: 04 = IPMI version 2.0, 03 = IPMI version 1. Sensor Type (**ST**) and Sensor Number (**S#**) come next, followed by the Event Trigger (**ET**), Event Data (**ED**) and finally Event X (**EX**).

```
-----Original Message-----
From: AlertEmail [mailto:              ]
Sent: Tuesday, July 23, 2013 7:05 PM
To:
Subject: Alert from <dlv1>


Event that generated this alert:
RID:0013 TS:07/24/2013 01:05:14 SN:MIS PSU2 STATUS
ST:Power Supply ED:Input Lost ET:Asserted EC:OK
RID:0013 RT:02 TS:51EF284A GID:002E ER:04 ST:08 S#:72
ET:6F ED:03 FF FF EX:00 FF FF FF FF FF FF FF
```

Figure 1-68   Alert Email – Power Cord Pulled from Power Supply Module

```
-----Original Message-----
From: AlertEmail [mailto:              ]
Sent: Tuesday, July 23, 2013 6:12 PM
To:
Subject: Alert from <dlv1>


Event that generated this alert:
RID:0011 TS:07/24/2013 00:11:45 SN:MIS PSU1 STATUS ST:Power
Supply ED:Presence detected ET:Deasserted EC:OK
RID:0011 RT:02 TS:51EF1BC1 GID:002E ER:04 ST:08 S#:71 ET:EF
ED:00 FF FF EX:00 FF FF FF FF FF FF FF
```

Figure 1-69   Alert Email – Power Module Pulled From Chassis

Drive Monitoring

Capacity drive monitoring can be performed by MegaRAID Storage Manager. Boot drive monitoring, since it is not a part of the StorBricks, is monitored using **M**ultiple **D**evices **Adm**inistration tool: mdadm. By default, if the MIS platform comes with a factory-installed operating system, boot drives are mirrored using RAID 1 and capacity drives are shipped with RAID 6. For those MIS Servers not shipped with an OS, RSTe must be enabled in the BIOS to allow boot drive mirroring and hot-swappable capabilities.

The following sections explain how to use the MegaRAID Storage Manager software to monitor the status of capacity drives and the mdstat command to monitor boot drives (Windows 2008 uses the Windows System Resource Manager to enable email alerts, see *KB Article cc732728* for more information).

The MegaRAID Storage Manager software does a background check every hour to verify if the controller and the system time are in synch. If the time difference between the controller and the system is more than 90 seconds, the MegaRAID Storage Manager software synchronizes the time so that the controller time and the system time are in synch. mdadm polls the md arrays every 60 seconds (default value). This can be adjusted using the -d mode and entering in a value of seconds, though it is recommended that you keep the default value and only adjust this time for troubleshooting.

Boot Drive Monitoring

Issue a #cat /proc/mdstat command to see current status (stat) of the multiple devices (md) attached to the processor (proc).

Boot drive status is indicated by either a U for up or _ for down. In the following example, everything is normal ([UU]), and md127 is the container for md125 and md126.

```
# cat /proc/mdstat
Personalities : [raid1] [raid0] [raid10] [raid6] [raid5] [raid4]
md125 : active raid1 sdb[1] sdc[0]
      111357952 blocks super external:/md127/0 [2/2] [UU]

md126 : active raid1 sdb[1] sdc[0]
      5556224 blocks super external:/md127/1 [2/2] [UU]

md127 : inactive sdc[1](S) sdb[0](S)
      6306 blocks super external:imsm
```

In the next example below, a drive has failed. Notice that sdc[0] is now missing from md125, md126 (their numbers changing from [2/2] to [2/1]), and the container md127. Additionally, a failed drive is indicated in the notation [U_].

```
# cat /proc/mdstat
Personalities : [raid1] [raid0] [raid10] [raid6] [raid5] [raid4]
md125 : active raid1 sdb[1]
      111357952 blocks super external:/md127/0 [2/1] [U_]

md126 : active raid1 sdb[1]
      5556224 blocks super external:/md127/1 [2/1] [U_]

md127 : inactive sdb[0](S)
      3153 blocks super external:imsm
```

To enable monitoring of the boot drives, the following usage of the mode `--monitor` is employed:

```
mdadm --monitor <raiddevice> [options] <devices>
```

This usage causes `mdadm` to periodically poll a number of `md` arrays and to report on any events noticed. If any devices are listed on the command line, `mdadm` will only monitor those devices, otherwise, all arrays will be monitored. Further, adding `--scan` causes the operation to be applied to all arrays listed in `/proc/mdstat`. If `--scan` is given, then an email address **must** be specified on the command line. If `--scan` is given and an email address is *not* available, then `mdadm` will not monitor anything. Without `--scan`, `mdadm` will continue monitoring as long as something was found to monitor.

The result of monitoring the arrays is the generation of events. These events are passed to a given email address using the option `-m=<email address>` or `--mail=<email address>`. If no email is given, then each event is reported to `stdout`.

The `-t` or `--test` option generates a **TestMessage** alert for every array found at startup. This alert gets mailed and passed to the alert program. This can be used for testing that the alert messages get through successfully.

The different events are listed in Table 1-2 below.

Table 1-2   Events

Tag	Description
DeviceDisappeared	An `md` array which previously was configured appears to no longer be configured.
RebuildStarted	An `md` array started reconstruction.
Rebuild##	Where **##** is 20, 40, 60, or 80, this indicates that rebuild has passed that many percentage of the total.
RebuildFinished	An `md` array that was rebuilding is not any more, either because it finished normally or was aborted.
Fail	An active component device of an array has been marked as faulty.

Table 1-2   Events

Tag	Description
NewArray	A new `md` array has been detected in the `/proc/mdstat` file.
DegradedArray	A newly noticed array appears to be degraded. This message is not generated when `mdadm` notices a drive failure that causes degradation, but only when `mdadm` notices that an array is degraded when it *first sees* the array.
TestMessage	An array was found at startup, and the `--test` option was given.

Only **Fail**, **DegradedArray**, and **TestMessage** cause email to be sent. Each event has an associated array device (e.g., `/dev/md1`) and possibly a second device. For **Fail**, the second device is the relevant component device. Use the command `mdadm --help` or `mdadm <option> --help` for more information on `mdadm` or the `mdadm` options, respectively.

Capacity Drive Monitoring

When devices automatically go from an optimal state to a different state, such as a drive failure, the MegaRAID Storage Manager software gets those events from the controller and gives a notification using different alert delivery methods. A pop-up notification is started automatically when you login to the operating system (Figure 1-70).
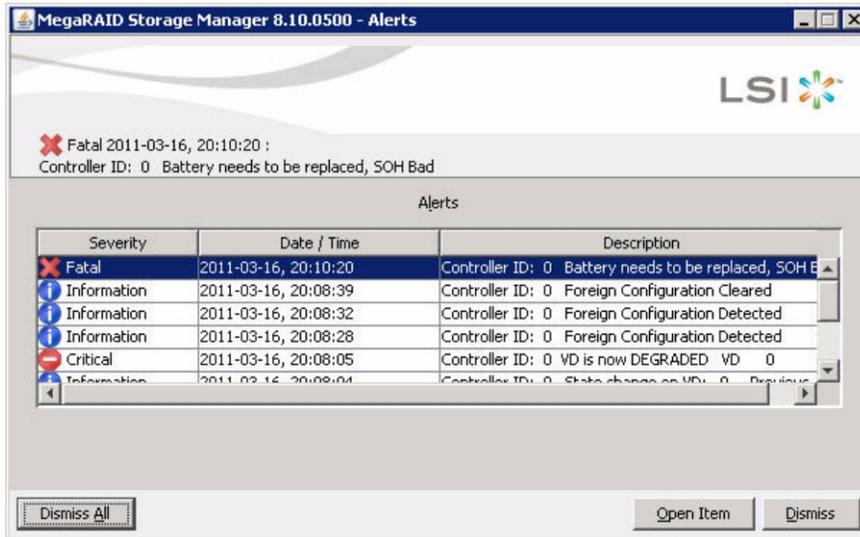
Figure 1-70   MegaRAID Storage Manager – Alerts Pop-up Window

To receive email alerts for capacity drive failures, from the main screen select **Tools** and **Configure Alerts**. In the **Configure Alerts** window, the **Alert Settings** tab allows you edit the alert delivery method for different severity levels by clicking the **Edit** button, or change the method of delivery and/or severity level for each individual event using the **Change Individual Events...** button (Figure 1-71).

Note: The **Save Backup...** button and **Load Backup...** buttons are used to save/load the *entire* alerts configuration to/from an `.xml` backup file, not just the settings for the tab with which you are working.
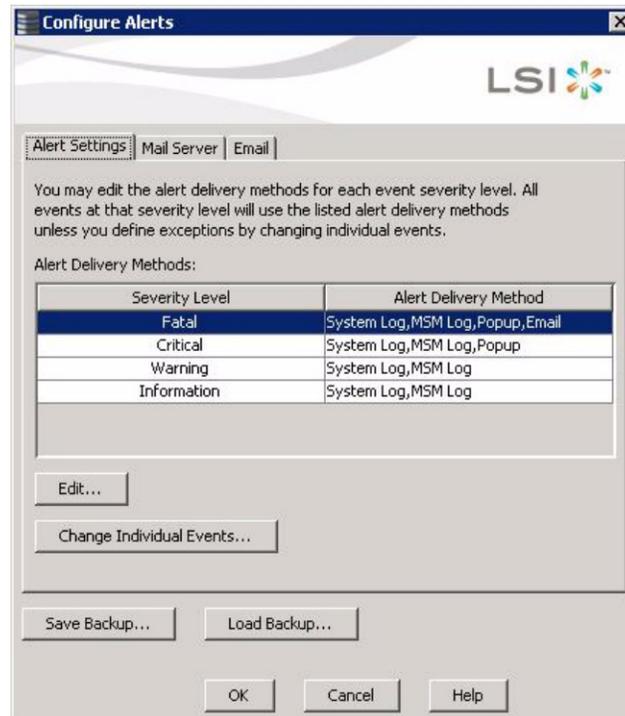
Figure 1-71   MegaRAID Storage Manager – Configure Alerts Window

---

Warning: Whenever you load a saved backup file, all unsaved changes made in the current session will be lost.

The **Mail Server** tab is where to enter the *sender* email address for alerts, the SMTP server name or IP address of the mail server to send the alerts, and user name and password fields (filled only when the SMTP server requires authentication, Figure 1-72).

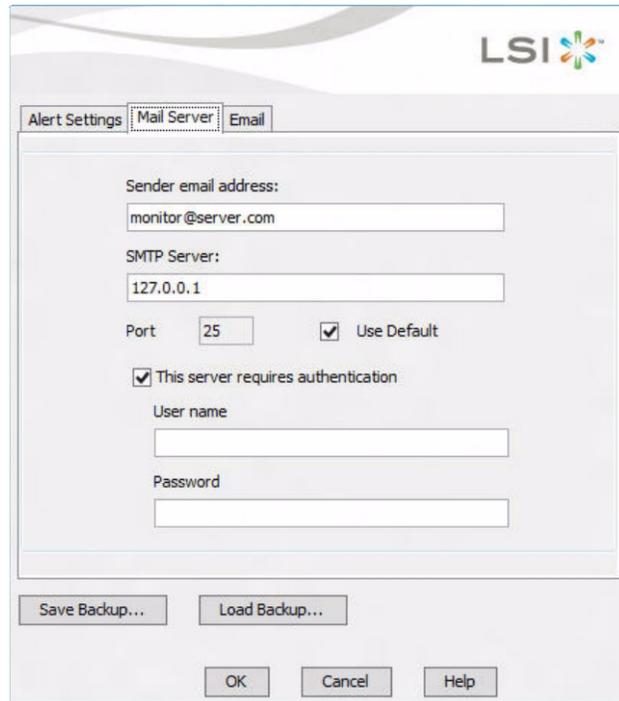**Figure 1-72**   MegaRAID Storage Manager – Mail Server Tab

The **Email** tab is where you go to add/remove email addresses for recipients of alert notifications (Figure 1-73). To configure an email account to receive alerts, enter the email address you want to add in the **New recipient email address** field and click **Add**. The email address should appear in the **Recipient email addresses** pane.

Figure 1-73   MegaRAID Storage Manager – Email Tab

Once the changes to the **Mail Server** tab and **Email** tabs have been made, click the **Test** button to make sure your configuration is correct. If satisfied, click **OK**.

Power Supply Monitoring

The fan base firmware will monitor all Power Supply Units (PSUs) installed in the system and generate SEL entries regardless of whether or not the alerts are enabled. This functionality cannot be turned off. To receive alerts, in addition to these instructions for entering new filters, correct configuration of the Intel BMC must also be performed. This can be done via the Intel Integrated BMC Web Console (see "Configuration Tab" on page 57). Specific instruction for the BMC configuration is not included here because it is site specific. Command strings are IPMI commands (`IPMItool` is a Linux-based utility, Windows uses `IPMIutil`).

When the fan base firmware monitors the PSU, it sends alerts to the BMC. This alone does not send the email. You will need to set up the BMC Web Console to have those emails delivered, and set platform event filters (PEF) 19 and 20. The S2600JF motherboard allows 20 platform event filters to be set. Intel uses the first 13. Setting filters 19 and 20 configures the BMC to realize that when a PSU alert comes in, an email should be sent.

PEF 5 sets the alert for PSU failure detected, and PSU predictive failure. A SEL entry will be recorded on both assertion and deassertion. An *alert* will only be sent when *asserted*. This filter is configured by Intel.

PEF 19 sets the alert for PSU input lost (AC/DC). A SEL entry will be recorded on both assertion and deassertion. An *alert* will only be sent when *asserted*.

PEF 20 sets the alert for PSU presence detected. A SEL entry will be recorded on both assertion and deassertion. An *alert* will only be sent when *deasserted*. These filters are configured by SGI.

Note: Error messages for power supplies may say "AC power lost" even when the power supply is a DC power supply.

Requirements

- fanbase_release_01.04.a.01 or later

- Shackleford_EFI_BMC-1.17.4151_BIOS-01.08.0003_ME-02.01.07.112_FRUSDR-1.10.02 or later

- IPMItool for Linux enabled (see "Enabling IPMI on a Linux System" on page 56) or IPMIutil for Windows (IPMItool available through SGI's support website at http://support.sgi.com, Windows instructions not given here. Refer to http://ipmiutil.sourceforge.net/.)

Viewing Existing Filters

Example using IPMItool to read filter 19:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x13 0x06 0x13 0x00
```

Example using ipmitool to read filter 20:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x13 0x06 0x14 0x00
```

Example using ipmitool to read all filters:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] pef list
```

Setting Filters

Example using IPMItool to set filter 19:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x12 0x06 0x13 0xC0 0x01 0x01 0x00 0xFF
0xFF 0x08 0xFF 0x6F 0x08 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00
```

Example using IPMItool to set filter 20:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x12 0x06 0x14 0xC0 0x01 0x01 0x00 0xFF
0xFF 0x08 0xFF 0xEF 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00
```

Clearing Filters

Example using IPMItool to clear filter 19:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x12 0x06 0x13 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00
```

Example using IPMItool to clear filter 20:

```
ipmitool [-I lanplus -H <BMC_IP_ADDRESS> -U <BMC_USERNAME> -P
<BMC_PASSWORD>] raw 0x04 0x12 0x06 0x14 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00
```
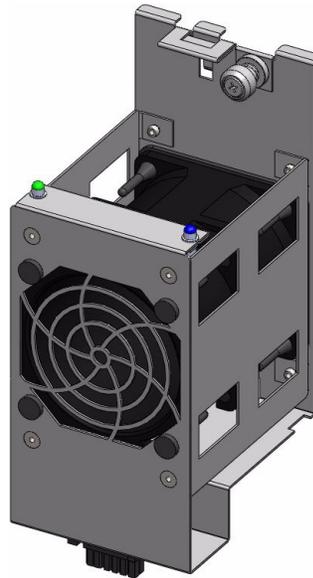
Fan Monitoring

Figure 1-74   Fan Module

Monitoring of the fan modules is done through the Fan Base Service Page. Alert emails for fan failures is done using the preconfigured Platform Event Filters designated by Intel (see "Select Events" on page 59) through the BMC. Using the Fan Base Service Page, failed fans can be set in a "Safe to Service" mode, a step necessary before changing out a fan module.
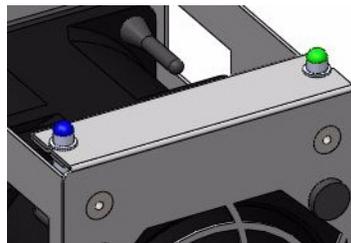
Fan LEDs

Figure 1-75   Fan Module LEDs

Like drives, fans also have a green/amber status LED and a blue locator LED. The green LED will be lit when a fan is operating normally. An amber LED will be lit if the fan is in fault. The locator LED is lit automatically when fans are set in a "Safe to Service" mode.

Fan Base Service Page

The fan baseboard is a circuit board at the heart of the chassis design. As such, it can be used to monitor hardware and issue commands to the hardware without having to use an operating system or even a server module (which is why it is useful for JBODs). The Fan Base Service Page is the customer interface for the fan baseboard, and can be accessed by connecting through the **MIS-S9D Proprietary Ethernet** port (Figure 1-76) and pointing a browser to: `192.168.0.3/service.xml`. This page can also be reached through the JBOD I/O module ethernet port, using its DHCP address: `<DHCP address>/service.xml`.

Figure 1-76   MIS-S9D Proprietary Network Interface

The Fan Base Service Page layout is based on a top-down view of a chassis, which is why there are different layouts for the server and JBOD versions of the page. Notably, the server page features boot drives and server modules (Figure 1-77), where the JBOD page has a 9th StorBrick with capacity drives and JBOD I/O modules (Figure 1-78).

From here you can view StorBrick status, power supply status, fan status, and set fans in a "**Safe to Service**" mode (i.e., off) for maintenance.

Warning: If the fan is NOT set in a "Safe to Service" mode, there are only 10 *seconds* available to exchange a fan. Without setting "Safe to Service," the platform will assume a fan has experienced *critical failure*, requiring an emergency shutdown for thermal requirements. Setting "Safe to Service" allows more time for replacement procedures (15 minutes) before initiating thermal shutdown.

Figure 1-77   Fan Base Service Page

Figure 1-78   MIS JBOD Service Page

RAID Cards and Battery Back-up Units Monitoring

If the component failing is a MegaRAID card or Battery Back-up Unit on a MegaRAID card, by default, fatal events in MegaRAID Storage Manager are displayed as email notifications. Based

on your configuration, the email notification contains system information and the controller's image details along with the event's description. Using this information, you can find out the system and the controller on which the fatal error occurred. For more information on configuring MegaRAID Storage Manager alerts, see Chapter 10 in LSI's *MegaRAID SAS Software User's Guide*.

JBOD Monitoring

Once assigned a DHCP address, the JBOD I/O modules can be used to access the Fan Base Service page by connecting a server/laptop to the JBOD ethernet port and directing a browser to `<DHCP address>/fb/service.xml` (see "Fan Base Service Page" on page 73).

Drive failures in the JBOD are monitored by MegaRAID Storage Manager. Otherwise, automatic alerting of fan failures and power supply failures is monitored by way of the JBOD I/O to the host server.

Set Up Complete

Congratulations! Set up and configuration of your MIS system is complete. Please continue configuration and use of your system by referring to *SGI Modular InfiniteStorage (MIS) 1.5 Platform User Guide, publication number 007-5916-xxx*. There you will find instructions on zoning, maintenance, and other pertinent information.

If necessary, refer to the troubleshooting steps below.

Troubleshooting

This section describes troubleshooting for the problems listed below, many which customers are able to perform without the assistance of SGI Field Technicians. In SGI's *Modular Infinite Storage (MIS) User Guide* (publication series **007-5818-00x** and **007-5916-00x**), Chapter 2, "System Interfaces," describes use of the control panel, BMC, and IPMI to monitor the overall system status and the status of specific components.

- "No Video" on page 77
- "Losing the System's Setup Configuration" on page 78

- "Missing Firmware Files" on page 78

- "Missing Firmware Files" on page 78

- "Cannot Receive Email Alerts Using BMC" on page 78

- "Path not found errors after installing Python for Windows" on page 81

- "Intel BIOS POST error messages and handling description" on page 81

- "Beep Codes" on page 85

- "Not all beep codes signal an error" on page 85

- "Fans don't spin when power button pressed" on page 86

- "Fans spin when power button is pressed, but no video display is seen" on page 86

- "BIOS or board logo appear, but OS load screen never appears" on page 86

- "OS load screen appears, but nothing further" on page 86

- "OS fully loads, but errors are seen" on page 86

- "Cannot boot after settings were changed in BIOS" on page 86

- "System Gets Stuck in a Reboot Cycle" on page 87

- "Server Diagnostic LED Decoding" on page 87

Other troubleshooting information is contained in "Related Publications" on page xxv (such as, *Intel® Remote Management Module 4 and Integrated BMC Web Console User Guide* (pdf)).

Important: If you require software to run or monitor the MIS platform, need technical assistance, or to contact SGI Customer Support, please see "Product Support" on page xxvi.

No Video

If the power is on but there is no video, remove all add-on cables (besides power & video). Use a different monitor to determine if the fault lies with it. Use the speaker to determine if any beep codes exist. Refer to "Beep Codes" on page 85, for details.

Losing the System's Setup Configuration

Make sure there is no fault with the power supplies. A fault with the power supply may cause the system to lose the CMOS setup information. If this does not fix the Setup Configuration problem, contact SGI for repairs.

Missing Firmware Files

There may come a time when you will need to update the zoning tool in order to support the firmware that is present on the StorBricks in a new MIS Server or JBOD machine. If this is the case, you will receive an error message that states either: **Unable to find directory that contains firmware files** or **Unable to find firmware file**, and below that, the version number of the firmware files necessary (example: **01.30.00.00**).

The firmware folders necessary for download will contain the version number in the folder name. For this example, the desired firmware folders will have a name similar to `storbrick-release-01.30.00.00 <date>`.

You will need to download the necessary firmware files and place them into the `/opt/Zones/Versions` folder for Linux and the `C:\Program Files (x86)\Zones\Versions` folder for Windows.

Cannot Receive Email Alerts Using BMC

In order to receive email alerts, the MIS Server must be networked to a SMTP mail server. Next, using the BMC, go to the **Configuration** page, and click on **Alert Email** (Figure 1-79).
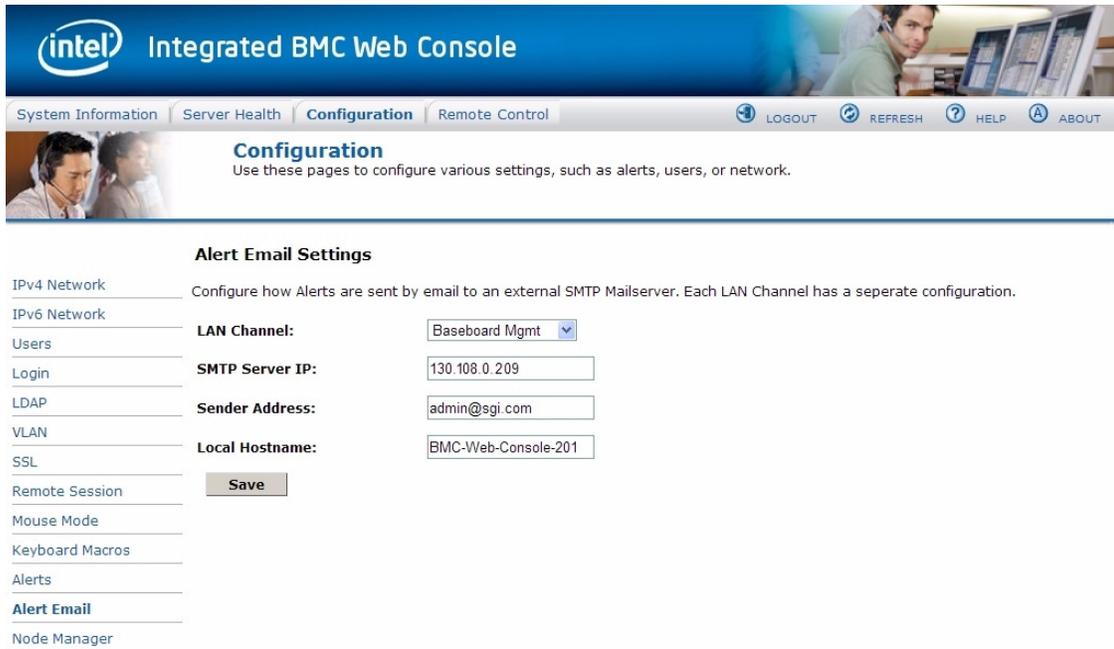
Figure 1-79   BMC Alerts Email Settings Page

The **LAN Channel** should be set to **Baseboard Mgmt**. The **SMTP Server IP** should be the IP address of the mail server to which the MIS platform is connected. **Sender Address** can be any email address configured on the SMTP server. **Local Hostname** can be any name to identify the machine sending the alert (limit of 18 characters). When finished, click the **Save** button at the bottom of the page. A pop-up will let you know that the changes have been saved (Figure 1-80).

Figure 1-80   BMC Alert Configuration Success Pop-up

Next, click on **Alerts** in the left-hand navigation pane (Figure 1-81).
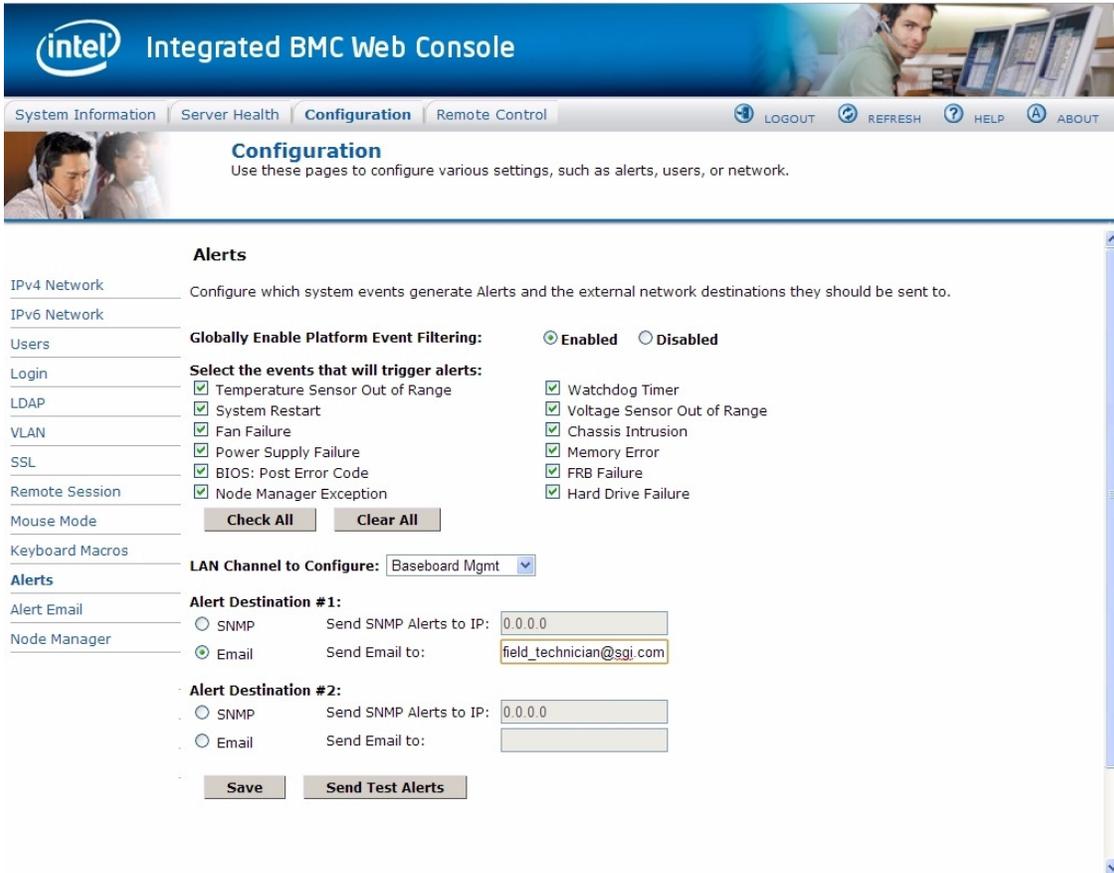
Figure 1-81   BMC Alerts Configuration Page

Make sure all the checkboxes for alerts contain a check for each alert to be sent. The **LAN Channel to Configure** should be set to **Baseboard Mgmt**. **Alert Destination #1** should be set to **Email**, and **Send Email to:** should be the email address of the account to receive the alerts. When finished, click the **Save** button at the bottom of the page. A pop-up will let you know that the changes have been saved. To test your configuration, click the **Send Test Alerts button**. You will receive a pop-up letting you know that the email was sent, and you will receive an email notifying you of a successful test.

Path not found errors after installing Python for Windows

Some Windows machines will need the variable path set for Python, and will display "Path not found" errors if not set. The path is set by doing the following:

1. Go to **Control Panel** and double-click the **System** icon.

2. Click on the **Advanced** tab.

3. Click the **Environment Variables** button at the bottom.

4. In the system variables box in at the bottom, find the entry `Path` and select it.

5. Click the **Edit** button and add to the end of the string: `C:\python##` where `##` is the version number of Python installed on the Windows machine.

6. Click **Apply** and **Okay**.

Python will now run normally.

Intel BIOS POST error messages and handling description

If you receive a code during the POST of booting by the Intel® Server Board, see Table 1-3 for the listing of codes for BIOS events messages.

Table 1-3   Intel BIOS POST Error Messages

Error Code	Error Message Response	Event Type
004C	Keyboard / interface error	Major
0012	CMIS date / time not set	Major
0048	Password check failed	Fatal
0141	PCI resource conflict	Major
0146	Insufficient memory to shadow PCI ROM	Major
0192	L# cache size mismatch	Fatal
0194	CPUID processor family are different	Fatal
0195	Front side bus mismatch	Major
5220	Configuration cleared by jumper	Minor

Table 1-3   Intel BIOS POST Error Messages **(continued)**

Error Code	Error Message Response	Event Type
5221	Passwords cleared by jumper	Major
8110	Processor 01 internal error (IERR) on last boot	Major
8111	Processor 02 internal error (IERR) on last boot	Major
8120	Processor 01 thermal trip error on last boot	Major
8121	Processor 02 thermal trip error on last boot	Major
8130	Processor 01 disabled	Major
8131	Processor 02 disabled	Major
8160	Processor 01 unable to apply BIOS update	Major
8161	Processor 02 unable to apply BIOS update	Major
8190	Watchdog timer failed on last boot	Major
8198	Operating system boot watchdog timer expired on last boot	Major
8300	Baseboard management controller failed self-test	Major
8305	Hot swap controller failed	Major
84F2	Baseboard Management Controller failed to respond	Major
84F3	Baseboard management controller in update mode	Major
84F4	Sensor data record empty	Major
84FF	System event log full	Minor
8500	Memory component could not be configured in the selected RAS mode	Major
8520	DIMM_A1 failed Self Test (BIST)	Major
8521	DIMM_A2 failed Self Test (BIST)	Major
8522	DIMM_A3 failed Self Test (BIST)	Major
8523	DIMM_A4 failed Self Test (BIST)	Major
8524	DIMM_B1 failed Self Test (BIST)	Major

Table 1-3   Intel BIOS POST Error Messages **(continued)**

Error Code	Error Message Response	Event Type
8525	DIMM_B2 failed Self Test (BIST)	Major
8526	DIMM_B3 failed Self Test (BIST)	Major
8527	DIMM_B4 failed Self Test (BIST)	Major
8528	DIMM_C1 failed Self Test (BIST)	Major
8529	DIMM_C2 failed Self Test (BIST)	Major
852A	DIMM_C3 failed Self Test (BIST)	Major
852B	DIMM_C4 failed Self Test (BIST)	Major
852C	DIMM_D1 failed Self Test (BIST)	Major
852D	DIMM_D2 failed Self Test (BIST)	Major
852E	DIMM_D3 failed Self Test (BIST)	Major
852F	DIMM_D4 failed Self Test (BIST)	Major
8580	DIMM_A1 Correctable ECC error encountered	Minor/Major after 10 events
8581	DIMM_A2 Correctable ECC error encountered	Minor/Major after 10 events
8582	DIMM_A3 Correctable ECC error encountered	Minor/Major after 10 events
8583	DIMM_A4 Correctable ECC error encountered	Minor/Major after 10 events
8584	DIMM_B1 Correctable ECC error encountered	Minor/Major after 10 events
8585	DIMM_B2 Correctable ECC error encountered	Minor/Major after 10 events
8586	DIMM_B3 Correctable ECC error encountered	Minor/Major after 10 events
8587	DIMM_B4 Correctable ECC error encountered	Minor/Major after 10 events

Table 1-3   Intel BIOS POST Error Messages **(continued)**

Error Code	Error Message Response	Event Type
8588	DIMM_C1 Correctable ECC error encountered	Minor/Major after 10 events
8589	DIMM_C2 Correctable ECC error encountered	Minor/Major after 10 events
858A	DIMM_C3 Correctable ECC error encountered	Minor/Major after 10 events
858B	DIMM_C4 Correctable ECC error encountered	Minor/Major after 10 events
858C	DIMM_D1 Correctable ECC error encountered	Minor/Major after 10 events
858D	DIMM_D2 Correctable ECC error encountered	Minor/Major after 10 events
858E	DIMM_D3 Correctable ECC error encountered	Minor/Major after 10 events
858F	DIMM_D4 Correctable ECC error encountered	Minor/Major after 10 events
8601	Override jumper set to force boot from lower alternate BIOS bank of flash ROM	Minor
8602	WatchDog timer expired (secondary BIOS might be bad)	Minor
8603	Secondary BIOS checksum fail	Minor
92A3	Serial port component was not detected	Major
92A9	Serial port component encountered a resource conflict error	Major
0xA000	TMP device not detected	Minor
0xA001	TMP device missing or not responding	Minor
0xA002	TMP device failure	Minor
0xA003	TMP device failed self test	Minor

Beep Codes

The BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered (for example, on each power-up attempt), but are not sounded continuously. Common supported codes are listed in "Intel BIOS POST error messages and handling description" on page 81 for details.

Another source of beep codes may be the LSI MegaRAID card. Table 1-4 contains a summary of the LSI MegaRAID card beep codes. These beep codes indicate activity and changes from the optimal state of your RAID array.

Table 1-4   Summary of LSI MegaRAID Card Beep Codes

Beep Code	LSI Firmware State	Cause (Depending on RAID Level)
3 seconds on, 1 second off	SPEAKER_OFFLINE_ENTRY	RAID 0: One or more drives offline. RAID 1: Two drives offline. RAID 5: Two or more drives offline. RAID 6: More than two drives offline.
1 second on, 1 second off	SPEAKER_DEGRADED_ENTRY	RAID 1: A mirrored drive failed. RAID 5: One drive failed. RAID 6: One or two drives failed.
1 second on, 3 seconds off	SPEAKER_HOTSPARE_ENTRY	A hot spare drive has completed the rebuild process and has been brought into the array.

Not all beep codes signal an error

Intel boards and systems are designed to indicate USB readiness by a series of beep codes during POST, before video becomes available. These beeps mean USB is powered and initialized.

Devices such as a pen drives or USB CD/DVD ROM drives attached to external USB port will generate a beep once the device is recognized, powered and initialized.

These beep codes do not signal any error. They signal USB and external device readiness during POST.

Fans don't spin when power button pressed

Is at least one power supply fan spinning? If yes, there is good power to the modules. Verify all required power cables are correctly plugged into the chassis.

If no, there is potential lack of clean power to the module. Swap power cables, try a different wall circuit, or try replacing a power supply module (see "Replacing a Power Supply" on page 154).

Fans spin when power button is pressed, but no video display is seen

Are there any beeps? If **yes**, beep codes are listed in Table 1-4 on page 85. If the answer is **no**, there may be a memory card error or an error with the processor. For either case, contact SGI Technical Support (see "Product Support" on page xxvi).

BIOS or board logo appear, but OS load screen never appears

This may be a problem with add-in cards in the server system. Contact SGI Technical Support (see "Product Support" on page xxvi).

OS load screen appears, but nothing further

This may be a problem with add-in cards in the server system. Contact SGI Technical Support (see "Product Support" on page xxvi).

OS fully loads, but errors are seen

Use operating system logging utility such as Windows Event Viewer or Linux dmesg to narrow the source of the error, and contact SGI Technical Support (see "Product Support" on page xxvi).

Cannot boot after settings were changed in BIOS

Certain changes in BIOS settings (such as chipset timing or latency, memory timing or latency, processor clock frequency, etc.) can cause a system to no longer boot. If you are able to enter the BIOS Setup by pressing F2, reset the BIOS to factory defaults by pressing F9. Save and exit the

BIOS Setup. If you cannot enter the BIOS Setup, contact SGI Technical Support (see "Product Support" on page xxi).

System Gets Stuck in a Reboot Cycle

If the platform gets stuck in a cycle where it is continuously rebooting without ever going into full power on, try replacing two of the power supplies, even if they are not reporting faults.

If a power supply has failed and does not correctly issue its fault (i.e., it *falsely* reports that it is still working), it will cause the platform to go into standby power mode, and the platform will try rebooting in order to power up. This can cause the platform to get stuck in a reboot cycle, and never actually successfully powering on. Replacing the faulty power supplies resolves this issue.

Server Diagnostic LED Decoding

On the server module motherboard are 8 diagnostic LEDs. The BIOS sends a value to the LEDs and the display can then be decoded using the following linked table (not reproduced here). During the system boot process, the BIOS executes several platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine is started, the BIOS displays the POST code on the POST diagnostic LEDs found on the back edge of the server board. To assist in troubleshooting a system hang during the POST process, the diagnostic LEDs can be used to identify the last POST process to be executed.

Note: These diagnostic LED codes are only used during system boot.

Each POST code is represented by eight diagnostic LEDs. The POST codes are divided into two nibblets, an upper and lower nibblet. The upper nibblet bits are represented by diagnostic LEDs #4, #5, #6, & #7. The lower nibblet bits are represented by diagnostic LEDs #0, #1, #2, & #3. The diagnostic LED #7 is the Most Significant Bit (MSB), and diagnostic LED #0 is the Least Significant Bit (LSB).

The table with the diagnostic codes starts on page 171 of *Intel Server Board S2600JF, Technical Product Specification*:
http://download.intel.com/support/motherboards/server/sb/473674_g31608_005_s2600jf_tps_r1_4.pdf.