IBM SAS RAID Controller Module

Host Systems Attachment Guide

IBM SAS RAID Controller Module

Host Systems Attachment Guide

Note

Before using this information and the product it supports, read the information in the "Notices" on page 169 section.

Eleventh Edition (October 2013)

Contents

Figures

Tables

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

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

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

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

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

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

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

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

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

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

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

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

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

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

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

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

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

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྒྲིག་མ་བྱས་གོང་། ་སྔར་གྱི་ཡིད་གཟབ་
བྱ་འདུ་མིན་ཡོད་པའི་འོད་སྡེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

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

Guidelines for trained service technicians

This section contains information for trained service technicians.

Inspecting for unsafe conditions

Use this information to help you identify potential unsafe conditions in that you are working on.

, as it was designed and manufactured, has required safety items to protect users and service technicians from injury. The information in this section addresses only those items. Use good judgment to identify potential unsafe conditions that might be caused by alterations or attachment of features or optional devices that are not addressed in this section. If you identify an unsafe condition, you must determine how serious the hazard is and whether you must correct the problem before you work on the product.

Consider the following conditions and the safety hazards that they present:

- Electrical hazards, especially primary power. Primary voltage on the frame can cause serious or fatal electrical shock.
- Explosive hazards, such as a damaged CRT face or a bulging capacitor.
- Mechanical hazards, such as loose or missing hardware.

To inspect the product for potential unsafe conditions, complete the following steps:

1. Make sure that the power is off and the power cords are disconnected.
2. Make sure that the exterior cover is not damaged, loose, or broken, and observe any sharp edges.
3. Check the power cords:
   - Make sure that the third-wire ground connector is in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and the frame ground.
   - Make sure that the power cords are the correct type.
   - Make sure that the insulation is not frayed or worn.
4. Remove the cover.
5. Check for any obvious alterations. Use good judgment as to the safety of any alterations.
6. Check inside the system for any obvious unsafe conditions, such as metal filings, contamination, water or other liquid, or signs of fire or smoke damage.
7. Check for worn, frayed, or pinched cables.
8. Make sure that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

Guidelines for servicing electrical equipment

Observe these guidelines when you service electrical equipment.

- Check the area for electrical hazards such as moist floors, nongrounded power extension cords, and missing safety grounds.
- Use only approved tools and test equipment. Some hand tools have handles that are covered with a soft material that does not provide insulation from live electrical current.
- Regularly inspect and maintain your electrical hand tools for safe operational condition. Do not use worn or broken tools or testers.
- Do not touch the reflective surface of a dental mirror to a live electrical circuit. The surface is conductive and can cause personal injury or equipment damage if it touches a live electrical circuit.
- Some rubber floor mats contain small conductive fibers to decrease electrostatic discharge. Do not use this type of mat to protect yourself from electrical shock.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Locate the emergency power-off (EPO) switch, disconnecting switch, or electrical outlet so that you can turn off the power quickly in the event of an electrical accident.
- Disconnect all power before you perform a mechanical inspection, work near power supplies, or remove or install main units.
- Before you work on the equipment, disconnect the power cord. If you cannot disconnect the power cord, have the customer power-off the wall box that supplies power to the equipment and lock the wall box in the off position.
- Never assume that power has been disconnected from a circuit. Check it to make sure that it has been disconnected.
- If you have to work on equipment that has exposed electrical circuits, observe the following precautions:
  - Make sure that another person who is familiar with the power-off controls is near you and is available to turn off the power if necessary.
  - When you work with powered-on electrical equipment, use only one hand. Keep the other hand in your pocket or behind your back to avoid creating a complete circuit that could cause an electrical shock.
  - When you use a tester, set the controls correctly and use the approved probe leads and accessories for that tester.
  - Stand on a suitable rubber mat to insulate you from grounds such as metal floor strips and equipment frames.
- Use extreme care when you measure high voltages.
- To ensure proper grounding of components such as power supplies, pumps, blowers, fans, and motor generators, do not service these components outside of their normal operating locations.
- If an electrical accident occurs, use caution, turn off the power, and send another person to get medical aid.

Safety statements

These statements provide the caution and danger information that is used in this documentation.

Important:

Each caution and danger statement in this documentation is labeled with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the *Safety Information* document.

For example, if a caution statement is labeled "Statement 1," translations for that caution statement are in the *Safety Information* document under "Statement 1."

Be sure to read all caution and danger statements in this documentation before you perform the procedures. Read any additional safety information that comes with your system or optional device before you install the device.

Statement 1

DANGER

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

To avoid a shock hazard:

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

To Connect:	**To Disconnect:**
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2

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

Do not:

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

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

Statement 21

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

About this guide

This guide provides information about attaching hosts to the SAS RAID Controller Module in the BladeCenter S Chassis. The first chapter provides an overview of host attachment concepts, specific considerations that affect more than one host, and an introduction to the SAS RAID Controller Module. Each subsequent chapter provides information on a specific host. Table 1 lists the hosts that you can attach to your storage unit and provides a link to the chapter for each host.

For the most current information on supported hosts and operating systems, review the interoperability information at:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5078491&brandind=5000020

Table 1. Hosts that are supported by the SAS RAID Controller Module

Host	Chapter
Linux	Chapter 2, "Chapter 2 x86-64 (Intel or AMD) blades Running Linux Host Attachment," on page 19
Windows	Chapter 3, "Chapter 3 x86-64 (Intel or AMD) Blades Running Windows Host Attachment," on page 51
VMware	Chapter 4, "Chapter 4 x86-64 (Intel or AMD) blades running VMware Host Attachment," on page 85
AIX / VIOS	Chapter 5, "Chapter 5 IBM Power Systems Running AIX / VIOS Host Attachment," on page 105

Conventions used in this guide

The following typefaces are used to show emphasis:

boldface

Text in **boldface** represents menu items and lowercase or mixed-case command names.

Italics

Text in *italics* is used to emphasize a word. In command syntax, it is used for variables for which you supply actual values.

`monospace`

Text in `monospace` identifies the data or commands that you type, samples of command output, or examples of program code or messages from the system.

Related publications

This section details additional documentation sources. These installation sections are provided in Portable Document Format (PDF) on the support CD that came with your RAID Controller.

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

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

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

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

Other IBM publications

You can download additional IBM publications from the IBM Systems Support Web site at:

http://www.ibm.com/systems/support/

The IBM publications center offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download free of charge. You can also order publications. The publications center displays prices in your local currency. You can access the IBM publications center through the following Web site:

http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

Note: Open the Web site in a new browser window by right clicking on the link and selecting ⌂Open in New Window.⌂

Related accessibility information

To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded for free from the Adobe Web site at:

http://www.adobe.com/support/downloads/main.html

Summary of Changes for IBM BladeCenter S SAS RAID Controller Module Host Systems Attachment Guide

This document contains structural, terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. This summary of changes describes new, changed, and deleted information for this release.

Version	New Information	Changed Information
Eleventh Edition (October 2013)	• Add information for SLES 11.3 support • Add information for VMware 5.1 update 1 support	• Some commands and instructions in Chapter 4 are updated • Multipath verification in a SAS booted host running SLES 11.3 • Concurrent controller maintenance procedure for Linux host updated
Tenth Edition (July 2013)	• Add information for RHEL 5.9 and 6.4 support	
Ninth Edition (March 2013)	• Add information for Windows Server 2012 support • Add information for VMware ESX/ ESXi 4.1u3 support	
Eighth Edition (October 2012)	• Add information about RHEL 6.3 support	
Seventh Edition (August 2012)	• Post-OS system installation command for SLES 11.2	• Change the command to build a new initrid image for SUSE Linux Enterprise • Multipath verification in a SAS booted host running RHEL 6.2

Sixth Edition (June 2012)	• Verifying & Setting LUN Parameters on VMWare Guest Operating Systems running Microsoft Windows • In Windows and Linux, for Blades using LSI SAS 2004 HBA (e.g. HS23 and HS23E), add the value settings of “Report Device Missing Delay” and “IO Device Missing Delay” in the Adapter Timing Properties. • Add information regarding BladeCenter HS23E support	• Change Changing Queue depth and Hot plug settings – for RHEL 6.x, 5.x, and SUSE Linux • Change RHEL 6.2 command line to build a new Linux initial ram-based root file system (initramfs) image
Fifth Edition (March 2012)	• Multipath verification in a SAS booted host running RHEL 6.2 • Add configuring the SAS HBA driver settings for BladeCenter HS23 • Add information of configuration regarding RHEL 6.2 support • Add information regarding BladeCenter HS23 support	• Change commands and notes for BladeCenter HS23 using inbox mpt2sas driver
Fourth Edition (December 2011)	• Add information regarding queue depth setting for busy response and performance issues in VMWare ESX 4.x • Add information regarding RHEL 6.1 and RHEL 5.7 support • Add SCSI controller setting as step 0 to ensure the queue depth configuration works properly while running RHEL 6.x as VMWare guest OS • Add commands of changing Qdepth setting for VMWare ESXi 5 • Add Concurrent Maintenance using the AMM in VMWare	• Change information of Post-Operating system installation activities for RHEL 5.7 support

Second Edition	• Add information regarding the PS70x blades • Add information regarding SLES11 support • Add Appendix C regarding WWN changes when upgrading LSI SAS HBA firmware on specific blade types	• The IBM support web site has changed. Material reflected in this document was assembled with site information that was available at the time. Some screen shots may look differently then the examples provided in some of the sections

•

Handling static-sensitive devices

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

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

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

Chapter 1. Chapter 1 Introduction

This chapter is an overview of host attachment for the IBM BladeCenter S SAS RAID Controller Module.

The first section contains host attachment requirements and conceptual overviews of key aspects of host attachment, with a focus on Serial Attached SCSI (SAS) attachment. Subsequent sections provide information on the SAS RAID Controller Module interfaces, models and features.

Introduction to host attachment

Host attachment is the process by which a host system, blade server, is configured to interoperate with external storage devices, the IBM BladeCenter SAS RAID Controller Module.

This section provides overviews of key aspects of host attachment, including requirements for attaching a host blade, overview of the SAS RAID Controller Module storage subsystem, and the IBM System Storage Multipath Subsystem Device Driver (SDD) path considerations. This section also provides conceptual details about SAS attachment.

Host attachment overview

The SAS RAID Controller Module provides a variety of host attachments so that you can consolidate storage capacity and workloads for open-systems hosts.

The SAS RAID Controller Module is designed to provide an IBM BladeCenter S chassis with an embedded RAID storage feature solution used as shared storage. The SAS RAID Controller Module is a SAS based consolidated reliable storage platform integrated within the BladeCenter S chassis that is targeted to provide boot and data drive capabilities for the blade servers. It is also provides cost effective shared storage for blade server applications. The SAS RAID Controller Module architecture supports additional capacity via expansion storage enclosures (Disk Storage Modules or DSMs) for environments that have high storage demands. The main SAS RAID Controller Module product value propositions are focused in the areas of overall simplification, end to end system management and BladeCenter eco-system integration. The SAS RAID Controller Module storage platform is highly dependent upon the BladeCenter S chassis DSMs to enable the internal BladeCenter connectivity model.

The SAS RAID Controller Module seamlessly integrates into the IBM BladeCenter S both mechanically and logically with the BladeCenter subsystems: legacy I/O fabric, system management hardware/software, power and cooling. The SAS RAID Controller Module provides RAID storage management control to disk drives contained in the DSMs for the IBM BladeCenter S chassis. It leverages the BladeCenter S internal infrastructure and the SAS fabric in the mid-plane of the BladeCenter S chassis providing SAS host server connectivity via blade server SAS HBA daughter cards.

Each blade server is capable of connectivity via a SAS HBA and the BladeCenter S SAS I/O fabric to each of the SAS RAID Controller Modules. Each blade server is provided a single PHY port SAS connection to each of the SAS Switches in the SAS

RAID Controller Modules. The SAS Switch is connected to the RAID controller side of the SAS RAID Controller Module via a 4 PHY wide SAS port, which when coupled with multi-path I/O software creates a double redundant attachment (multiple paths via the SAS wide ports and host server SAS path to each controller card).

General requirements for attaching a host

Before you attach a SAS RAID Controller Module to a host, review this list of general requirements for all hosts. Then, review the specific host requirements described in the section for each host.

Perform the following steps before you attach any host system to a SAS RAID Controller Module:

1. Review the *SAS RAID Module Interoperability Guide* to verify that the blades you will be configuring are supported with the SAS RAID Controller Module. This should include both hardware and software compatibility.
2. Review and understand the type of SAS HBA that will be used on the host blades which will be connected to the SAS RAID Controller Module. Various blades use different SAS HBAs.
3. *Review ServerProven compatibility* http://www.ibm.com/servers/eserver/serverproven/compat/us/
4. Review the *SAS RAID Controller Module Installation & User Guide*
5. If using the SAS RAID Controller Module with Microsoft Cluster Server (MSCS), make sure to review the section regarding host setup.
6. If SAS Booting a host, make sure to review the OS specific section regarding SAS Booting before attempting to setup SAS Boot from the SAS RAID Controller Module

Be sure to review all the compatibility guides. The most restrictive set is the one which should be relied upon. For instance if VMware 3 ESXi is supported on the HS21 blade in ServerProven, but it is not supported in the SAS RAID Controller Module Interoperability Guide, it should not be attempted to install VMWare 3 ESXi if that server will be connected to the SAS RAID Controller Module.

Introduction to IBM BladeCenter S SAS RAID Controller Module

This guide contains instructions for attaching host system blades with SAS expansion or connectivity cards to the IBM BladeCenter S SAS RAID Controller Modules.

The IBM BladeCenter S SAS RAID Controller Module provides a fully-integrated shared storage solution in an IBM BladeCenter S chassis. This guide contains instructions for attaching host system blades with SAS expansion or connectivity cards to the IBM BladeCenter S SAS RAID Controller Modules.

For additional information regarding the installation and configuration of the SAS RAID Controller Module refer to the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide*.

Data storage subsystems

Two subsystems are involved in IBM BladeCenter S data storage: the Disk Storage Module (DSM), and the SAS RAID Module. The Disk Storage Module (DSM) is an

enclosure holding up to six Disk Drive Modules (DDMs). There are a maximum of two DSMs installed in an IBM BladeCenter S chassis.

SAS RAID Module subsystems

The SAS RAID Module includes two subsystems: a RAID Controller subsystem and a SAS Switch subsystem. These subsystem cooperate to provide a connection between the Blade servers and the DSMs that allow the end user to design storage configurations and volumes for their data.

The Battery Backup Unit (BBU) is installed in the Media Tray in the front of the BladeCenter S Chassis. The BBUs provide protection of the cache memory in the SAS RAID Controller Modules.

In addition, a SAS HBA must be installed in each blade server for the blades to connect to the RAID Data Storage subsystem and modules. The figure below shows the physical layout of the IBM BladeCenter S chassis.

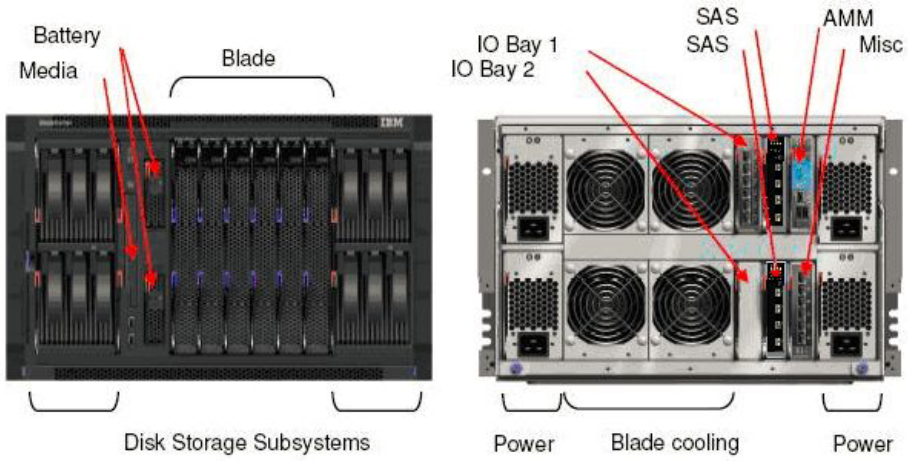


Figure 1. Diagram of IBM BladeCenter S Chassis

IBM BladeCenter S SAS RAID Controller Module Interfaces

This section describes the interfaces that can be used to manage the IBM BladeCenter S SAS RAID Controller Module

These interfaces include:

- IBM Storage Configuration Manager
- IBM Systems Director
- SAS RAID Controller Module Command-Line Interface (CLI)
- SAS RAID Controller Command Line Firmware Update Package

IBM Storage Configuration Manager

IBM Storage Configuration Manager is a system management application that enables you to use a Web browser to manage and configure IBM BladeCenter devices.

IBM Storage Configuration Manager runs as a Web server that communicates with managed devices. Managed devices include the following:

- IBM BladeCenter SAS Connectivity Module
- IBM BladeCenter S Disk Storage Module
- IBM BladeCenter S SAS RAID Controller Module

Note: As of IBM Storage Configuration Manager 2.20.0, IBM ServeRAID MR Controllers and IBM Integrated RAID Controllers are no longer supported devices in IBM Storage Configuration Manager. You can continue to manage these devices using the Storage Management feature in IBM Systems Director.

Important: IBM Storage Configuration Manager and IBM Systems Director cannot be installed on the same server.

For additional information on the installation and use of the IBM Storage Configuration Manager, go to:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5081393&brandind=5000016

IBM Systems Director

IBM Systems Director is a platform-management foundation that streamlines the way you manage physical and virtual systems across a heterogeneous environment. By using industry standards, IBM Systems Director supports multiple operating systems and virtualization technologies across IBM and non-IBM x86 platforms.

Through a single user interface, IBM Systems Director provides consistent views for viewing managed systems, determining how these systems relate to one another, and identifying the status of each system, thus helping to correlate technical resources with business needs. A set of common tasks included with IBM Systems Director provides many of the core capabilities required for basic management, which means instant out-of-the-box business value. These common tasks include discovery, inventory, configuration, system health, monitoring, updates, event notification and automation across managed systems.

IBM Systems Director's Web and command-line interfaces provide a consistent interface focused on driving these common tasks and capabilities:

- Discovering, navigating and visualizing systems on the network with the detailed inventory and relationships to the other network resources
- Notifying users of problems that occur and providing the ability to drill down to the source of the problem
- Notifying users when systems need updates and distributing and installing updates on a schedule
- Analyzing real-time data for systems and setting critical thresholds that notify the administrator of emerging problems
- Configuring settings of a single system and creating a configuration plan that can apply those settings to multiple systems

- Updating installed plug-ins to add new features and function to the base capabilities
- Managing the lifecycle of virtual resources

IBM Systems Director is designed to manage simple and complex environments, with multiple operating systems and platforms, up to 5000 managed systems. It supports the management of a variety of IBM and non-IBM hardware driving common tasks through the following platform management plug-ins and virtual resources. The systems supported include:

- IBM Power Systems™ management
  - HMC, IVM, and VIOS appliances
  - Power servers, Power blades, and LS41 and QS21 blade servers
  - AIX, IBM i, and Linux on POWER operating systems
- IBM BladeCenter and System x management
  - IBM BladeCenter chassis components, such as switch modules and server blades
  - System x systems and blade servers
  - VMware, Microsoft Virtual Server (MSVS), and Xen virtual servers
  - Windows and Linux operating systems on System x
- IBM System z management
  - z/VM hypervisor
  - Linux on System z operating system installed on z/VM virtual servers
  - Linux on System z running on a partition without z/VM
- IBM System Storage™ management
  - Integrated RIA controller (such as LSI)
  - Network storage, such as DS3000, DS4000, and DS6000™
  - Storage switches, such as IBM BladeCenter SAS, Brocade, Qlogic, Nortel and Cisco

SAS RAID Controller Module Command Line Interface (CLI)

The SAS RAID Controller Module command line interface (CLI) is an independent program that can be used to operate the RAID controller.

You must log in to the SAS RAID Controller Module via either telnet or SSH using your user ID and password. The SAS RAID Controller Module command line interface program starts automatically, and a `<CLI>` prompt appears. When you exit from the SAS RAID Controller Module command line interface program, the telnet/ssh session ends simultaneously.

For additional information regarding the use of the CLI interface, refer to the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide*.

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5078491

SAS RAID Controller Command Line Firmware Update Package

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

For additional information regarding the installation and use of this package refer to the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide* and the release notes included with each firmware update.

RAID implementation

A RAID implementation improves data storage reliability and performance.

Redundant Array of Independent Disks (RAID) is a method of configuring multiple disk drives in a storage subsystem for high availability and high performance. The collection of two or more physical disk drives presents the image of a single logical disk drive to the host system. In the event of a single device failure, data can be read or regenerated from the other disk drives in the array.

A RAID implementation enables fault-tolerant data storage by storing the data in different places on multiple disk drive modules (DDMs). By placing data on multiple disks, I/O operations can overlap in a balanced way to improve the basic reliability and performance of the attached storage devices.

When using the SAS RAID Controller Module, physical capacity can be configured as RAID 5, RAID 10, RAID 1, or RAID 0.

Note: RAID 0 is not redundant; however it is used to improve the basic performance of the attached storage devices.

Different RAID implementations may be used during the configuration of the storage pools depending upon the needs of the application. The following is a general overview of each storage pool type. For further information regarding how to configure a storage pool, refer to the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide*.

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5078491

Note: Even though there is a minimum defined in the following section for each RAID type, it is recommended when possible to use additional disk drive modules in pool configurations to improve response time.

RAID 5 Overview

RAID 5 is a method of spreading volume data across multiple disk drives. The IBM BladeCenter S SAS RAID Controller Module supports RAID 5 storage pools at a minimum of three (3) drives and to a maximum of twelve (12) drives in a single storage pool.

RAID 5 increases performance by supporting concurrent accesses to the multiple DDMs within each logical volume. Data protection is provided by parity, which is stored throughout the drives in the storage pool. If a drive fails, the data on that drive can be restored using all the other drives in the storage pool along with the parity bits that were created when the data was stored.

Also, if bad blocks develop on a drive, the redundancy of the storage pool can be used to restore the bad block data to a reserved area on the storage pool.

Uses

Provides high data throughput, especially for large files. Use RAID 5 for transaction processing applications because each drive can read and write independently. If a drive fails, the RAID controller uses the parity drive to recreate all missing information. Use also for office automation and online customer service that requires fault tolerance. Use for any application that has high read request rates but low write request rates.

Strong Points

Provides data redundancy, high read rates, and good performance in most environments. Provides redundancy with lowest loss of capacity.

Weak Points

Not well-suited to tasks requiring lot of writes. Suffers more impact if no cache is used (clustering). Drive performance will be reduced if a drive is being rebuilt. Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.

RAID 1 Overview

RAID 1 provides high availability by providing disk mirroring, which duplicates data between two disk drives. The IBM BladCenter S SAS RAID Controller Module supports RAID 1 storage pools at a minimum and maximum of two (2) drives per storage pool.

RAID 1 implementation provides data mirroring from one DDM to another DDM. Access to data is preserved as long as one disk in the mirrored pair remains available. In some cases, RAID 1 offers faster data read operations due to the fact that either of the disk drives in the pair can be used for the read operation. The total number of writes are doubled as every write must be performed to both drives. Since it consumes two drives to provide the same capacity as a single drive, RAID 1 storage pools may have less total capacity available than other RAID types.

Uses

Use RAID 1 for small databases or any other environment that requires fault tolerance but small capacity.

Strong Points

Provides complete data redundancy. RAID 1 is ideal for any application that requires fault tolerance and minimal capacity.

Weak Points

Requires twice as many drives. Performance is impaired during drive rebuilds.

RAID 0 Overview

RAID 0 is a method of spreading volume data across multiple disk drives. The IBM BladeCenter S SAS RAID Controller Module supports RAID 0 storage pools at a minimum of two (2) drives and to a maximum of twelve (12) drives in a single storage pool.

A RAID 0 implementation provides no data redundancy; however, due to striping volume data across multiple physical disk drives, data access performance for some work loads may be improved over other RAID types. Since none of the disk drive capacity is used for redundancy, RAID 0 storage pools allow for the highest amount of usable space for user data than other RAID types. However, if a single drive is lost, then all access to the storage pool will be lost. It is strongly recommended that the risks are understood before implementing a configuration using this type of storage pool.

Uses

Provides high data throughput, especially for large files. Any environment that does not require fault tolerance.

Strong Points

Provides increased data throughput for large files. No capacity loss penalty for parity.

Weak Points

Does not provide fault tolerance or high bandwidth. All data lost if any drive fails.

RAID 10 overview

RAID 10 provides higher availability by combining features of RAID 0 and RAID 1. The IBM BladeCenter S SAS RAID Controller Module supports RAID 10 storage pools at a minimum of four (4) drives and up to a maximum of twelve (12) drives in a single storage pool.

A RAID 10 implementation provides data mirroring from one DDM to another DDM. RAID 10 stripes data across half of the disk drives in the RAID 10 configuration. The other half of the array mirrors the first set of disk drives. Access to data is preserved as long as one disk in each mirrored pair remains available. In some cases, RAID 10 offers faster data read and write operations than RAID 5 because it does not need to manage parity. However, with half of the DDMs in the group used for data and the other half used to mirror that data, RAID 10 disk groups have less capacity than RAID 5 disk groups using the same number and capacity of disk drives.

Uses

Appropriate when used with data storage that needs 100 percent redundancy of mirrored drive groups and that also needs the enhanced I/O performance of RAID 0 (striped drive groups.) RAID 10 works well for medium-sized databases or any environment that requires a higher degree of fault tolerance and moderate to medium capacity.

Strong Points

Provides both high data transfer rates and complete data redundancy.

Weak Points

Requires twice as many drives as all other RAID levels except RAID 1.

Disk Drive Types

This section provides an overview of the two major types of Disk Drive Modules (DDMs) supported in the IBM BladeCenter S SAS RAID Controller Module. These drive types are Online SAS disk drives and Nearline SAS Disk drives.

Note: Disk drive modules using the SATA drive connection technology are not supported by the IBM BladeCenter S SAS RAID Controller Module.

For the complete list of supported drives, please refer to the *IBM BladeCenter S SAS RAID Module Interoperability Guide*.

Online SAS Disk Drive Modules

Online SAS Disk Drive Modules are disk drives that use the SAS drive connection technology to connect to the IBM BladeCenter S SAS RAID Controller Module.

These drives tend to have smaller capacity than Nearline SAS DDMs, however their rotational speeds are faster. This causes the access times for these drives often to be shorter than Nearline SAS DDMs. When storage pools are configured with these drive types, overall system performance may be higher than the performance observed when using Nearline SAS DDMs.

Nearline SAS Disk Drive Modules

Nearline SAS Disk Drive Modules are disk drives that use the SAS drive connection technology to connect to the IBM BladeCenter S SAS RAID Controller Module.

These drives tend to have higher capacity limits than Online SAS DDMs, however their rotational speeds are slower. This causes the access times for these drives often to be longer than for Online SAS DDMs. When storage pools are configured with these drive types, overall system performance may be less than the performance observed when using Online SAS DDMs. Users should consider the needs of their specific application before considering the use of these DDM types in their storage pool configurations.

Mixed Storage Pools

It is not recommended to mix Nearline SAS DDMs and Online SAS DDMs in the same storage pool. The overall storage pool performance may be reduced to the performance seen when Nearline SAS DDMs are used exclusively in a storage pool.

Using separate pools consisting of different drive types may be appropriate for some types of applications. Therefore having mixed types of drives in a single Disk Storage Module in the BladeCenter S Chassis is supported by the IBM BladeCenter S SAS RAID Controller Module with no performance penalty.

Logical configuration overview

The IBM BladeCenter S SAS RAID Controller Module allows for the configuration of multiple physical disk drive modules into one or more logical storage pools.

These storage pools can then be divided into multiple logical volumes that can be mapped to the host. This is a method of virtualization that allows the physical drives to be shared among more than one host. The illustration in the following figure provides an example of how the physical resources are combined and allocated to host systems.

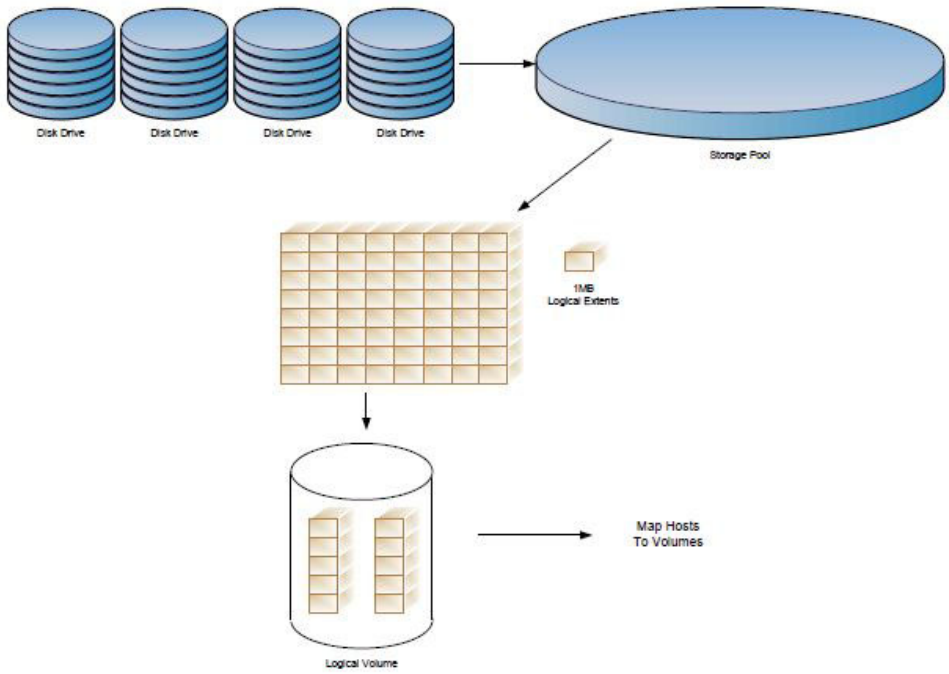


Figure 2. Logical Configuration Overview

IBM System Storage Multipath Subsystem Device Driver

The IBM System Storage Multipath Subsystem Device Driver (SDD) supports redundant connections between a disk storage server and a host server.

The SDD resides in the host server with the native disk device driver and takes advantage of redundant storage configurations to provide single-point failure protection, high data availability, and storage concurrent firmware download. It also provides a dynamic I/O load-balancing algorithm to reach the best I/O performance.

The SDD provides the following functions:

- Enhanced data availability
- Automatic path failover and failback
- Dynamic I/O load-balancing across multiple paths
- Multiple path selection policies for the host system
- Multiple path SAN boot on storage devices that support multipath I/O (MPIO)

Note: SAN boot is supported on the AIX, Windows, VMware, and Linux operating systems.

The term *SDD* represents both the SDD as the established multipath subsystem device driver and as the MPIO path control module, depending upon the operating system. The following table lists the multipath control modules for each of the listed operating systems.

Table 2. Example of multipath control modules

Operating System	Description	Acronymn
AIX	SDD Path Control Module	SDDPCM

Table 2. Example of multipath control modules (continued)

AIX	Native MPIO	Default PCM
Linux	Device Mapper-Multipath I/O	DM-MPIO
Windows	SDD Device Specific Module	SDDDSM
VMware	Native Multipath	NMP

As new operating systems are added, the SDD will be named according to the operating system.

For more information about the SDD, see:

http://www.ibm.com/systems/support/storage/software/sdd.

Host attachment path considerations

The list of path considerations of the host attachment

Path considerations affect the performance and availability of a storage image. For optimal performance, observe the following suggestions:

- Create pools that are owned by each controller
- Use additional physical disks per pool where possible
- Use spares when possible to increase protection against drive failures
- Determine the best RAID type for your application and requirements for redundancy and performance.
- Separate boot and data volumes into distinct pools when possible
- Limit the number of assigned LUNs
- Adopt appropriate queue depth settings
- In VMware make sure the Multipath setting is configured as shown below

Serial Attached SCSI host attachment

This section provides an overview of SAS attachment to an IBM BladeCenter S SAS RAID Controller Module, including architecture, topology, and LUN access modes.

SAS architecture

A SAS topology typically consists of initiators, targets and expanders. A SAS initiator is a device that originates command and data requests for target devices and receives responses for those requests from the same target devices. SAS target devices usually are controller devices that provide interfaces for management or provide logical units that receive command and data frames from SAS initiators and respond in kind to the requests. A SAS expander provides expansion from the point to point topology between initiator and target devices. An expander can be added in between an initiator and a target. This allows multiple initiators and targets to communicate with one another.

Each attempt to communicate requires the opening of a logical connection between the initiator and target, followed by an exchange of commands and possibly data, and a closing of the connection. When expanders are used, the topology of SAS is

analogous to a hub architecture. Because of this, anything that affects a single target, such as a link or bus reset, will affect all initiators and targets in the topology.

SAS overview for the SAS RAID Controller Module

Each SAS RAID Controller Module has four ports, also known as PHYs, all using a single worldwide port name (WWN); this is known as a wide SAS port.

In the SAS fabric created by the SAS RAID Controller Module configuration, a PHY on each SAS host bus adapter (HBA) has physical access to the same SAS wide port on one of the SAS RAID Controller Modules. Internal zoning configuration is used to provide a logical configuration path between the SAS HBA on the blade host and the SAS RAID Controller Module. This is the default for the configuration. If your setup requires changes to these defaults, it is recommended to contact IBM for assistance.

LUN considerations for SAS attachment

Worldwide names are used to associate a Logical Unit (LUN) for SAS attachment. For SAS attachment, LUNs are associated with the SAS adapter through the worldwide name (WWN) for the host adapter. Each SAS HBA has two PHYs available for connecting external to the host blade. Each PHY is associated with one of the SAS RAID Controller Modules.

Note: By default the SAS RAID Controller Module is setup to allow the host blades adapter to access the SAS wide port on the SAS RAID Controller Module and the four external wide SAS ports.

The maximum number of LUNs that can be assigned to a host is dependent on the host operating system type. The following table lists the maximum number of LUNs that are supported by the listed host.

Table 3. Maximum Supported LUNs per host operating system

Host operating system type	Max # of LUNs per host
AIX	16
Linux	16
Windows	16
VMware	16

The maximum queue depth that can be supported by a host is dependent on the host operating system type. The following table lists the maximum number of outstanding commands regardless of the number of LUNs that are supported by the listed host.

Table 4. Maximum Supported Queue per host operating system

Host operating system type	Max queue per host
AIX	64
Linux	64
Windows	64
VMware	64

The queue depth setting for the SAS RAID Controller Module should be set on the host blade server so that the combined total number of IO operations outstanding to the SAS RAID Controller Module cannot exceed the max queue per host defined in Maximum Supported Queue per host operating system table. This means that for each host, the queue depth should be calculated based on the number mapped LUNs to the host.

For example, to calculate the host queue depth per LUN if there are 12 LUNs mapped to a host and the maximum supported queue for that host is 64, divide 64 by 12, which equals 5, rounded down. The queue depth for the host should then be set to 5. For detailed information regarding how to set the host queue depth for a given operating system, refer to configuring of a SAS HBA driver in the following host specific chapters.

Note: For VMware, the queue depth setting is HBA, not LUN based, which differs from the other supported operating systems. Please refer toChapter 4, "Chapter 4 x86-64 (Intel or AMD) blades running VMware Host Attachment," on page 85, for additional information.

Important: In some configurations, the calculated queue depth may need further adjustment to achieve the optimal performance and fault tolerance characteristics. If issues are seen such as low throughput or a high number of BUSY responses returned from the SAS RAID Controller Module, additional tuning may be required.

Host Mapping

A host mapping defined on the SAS RAID Controller Module can access only those volumes that are defined in that mapping.

Any SAS host blade that has a host mapping defined on the SAS RAID Controller Module can access only those volumes that are defined in that mapping. A host mapping can contain up to a maximum of 16 volumes. The setup of a host mapping can be accomplished through the Command Line Interface (CLI) on the SAS RAID Controller Module or by using the IBM Storage Configuration Manager. An alert will be shown in the active alert list for all host blade WWNs that do not currently have a host mapping defined. It may not be apparent that a host mapping is being defined when using the IBM Storage Configuration Manager to configure the hosts and volumes for the SAS RAID Controller Module.

The following configuration actions can affect host mapping:

- When you define a new SAS host system in the IBM Storage Configuration Manager by specifying its worldwide name (WWN), the host mapping for that host system is automatically created. Initially the profile is empty. That is, it contains no volumes. In this state, the host cannot access any logical volumes including those that are already defined in the SAS RAID Controller Module. This action will remove the active alert in the system associated with the undefined WWN.
- When you add new logical volumes to a SAS host defined to the SAS RAID Controller Module, the new volumes are assigned to the host. The new volumes are created and are automatically added to the host mapping.
- When you assign existing volumes to SAS hosts, the volumes are added to the host mapping for that host.
- A SAS host cannot access any volumes until volumes are assigned to the host's WWN.

- To allow for multipathing, the logical volume must be assigned to both WWNs of the SAS host blade.
- When you remove a SAS host system using the IBM Storage Configuration Manager or the CLI, you delete the host and its host mapping.
- When you remove all volumes from a host mapping, the host mapping will remain with no volumes mapped to the host.
- If you replace a SAS controller card or if you are using a SAS connectivity card and the system board is replaced, you will have to redo the mapping for the blade to gain access to the volume again.

SAS worldwide name identification

The IBM BladeCenter S SAS RAID Controller Module uses a worldwide name (WWN) to uniquely identify a host port that is connected to a storage unit. The WWN consists of exactly 16 hexadecimal characters (0 - 9 and A - F). Each WWN is an 8 byte number derived from an IEEE OUI and vendor-supplied information.

The unique worldwide name can manually locate for host ports by performing the steps outlined in the chapter specific for each host later in this guide. To identify the WWN for the SAS RAID Controller Module, please refer to the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide*.

Prerequisites

The following sections discuss some of the operations that should be performed prior to attempting to connect a host blade to the IBM BladeCenter S SAS RAID Controller Module.

About this task

Procedure

1. Make sure that the BladeCenter S chassis, blade servers, SAS RAID Controller Modules, Ethernet switch modules, SAS expansion/connectivity cards and SAS drives are supported in combination with one another. The *IBM BladeCenter Interoperability Guide* provides a matrix showing all of the devices that have been tested with the IBM BladeCenter chassis and are known to be compatible. The *Interoperability Guide* is updated frequently. The guide is posted at http://www.ibm.com/systems/support/,
   - On the 'Support for IBM Systems ' page, select 'BladeCenter'.
   - On the ' Support and Downloads' page, select 'BladeCenter S Chassis' and “Documentation’, then ‘View your page’,
   - On the resulting page, select 'Interoperability Guide - IBM BladeCenter'.
2. Make sure that the AMM, blade server, Ethernet switch module, SAS expansion/connectivity card and SAS drive BIOS and firmware levels are supported in combination with the IBM BladeCenter S SAS RAID Controller Modules. The *IBM BladeCenter S SAS RAID Module Interoperability Matrix* provides a guide showing all of the devices that have been tested with the IBM BladeCenter S SAS RAID Controller Module and are known to be compatible. The SAS RAID Module Interoperability Matrix is updated periodically. The guide is posted at http://www.ibm.com/systems/support/.
   - On the ‘Support for IBM Systems’ page, select ‘BladeCenter’.
   - On the ‘Support and Downloads’ page, select ‘Search for a product’, and search for ‘43W3584’

- Check the box for 'IBM BladeCenter S SAS RAID Controller Module', then choose 'Documentation' and 'View your page'
- On the resulting page, select 'SAS RAID Module – Interoperability Guide'

3. For the latest Advanced Management Module firmware, SAS RAID Controller Module firmware, Ethernet switch firmware, SAS expansion/connectivity card firmware, blade server BIOS/BMC/Diagnostic/On board SAS controller BIOS/Firmware code, and device drivers, go to http://www.ibm.com/systems/support/, select BladeCenter S (BC-S) chassis or the appropriate blade server Machine Type and model and click on the download hyper link and see the software and device driver web page.
4. Make sure that an Advanced Management Module is installed in the BladeCenter chassis.
5. Make sure that an IBM BladeCenter Ethernet switch module or an IBM BladeCenter intelligent Copper Pass-through Module (iCPM) is installed in bay 1 of the BC-S chassis. Without the appropriate Ethernet switch module or iCPM in bay 1 of the BC-S chassis, the management connection to the SAS RAID Controller Modules for checking the status and configuring of the modules will not be possible. In addition, the modules might not be in the "optimal and bound" state. Also, verify that VLAN 4095 is set up and configured on the AMM and the SAS RAID Controller Modules.

Note: The IBM BladeCenter intelligent Copper Pass-through Module (iCPM), IBM option P/N 44W4483, is compatible with the SAS RAID Controller Module only if a standard Ethernet cable is used to connect ports 7 and 14 of the iCPM module. Furthermore, the IBM BladeCenter Copper Pass-through Module (CPM), IBM option P/N 73P6100, is not compatible with the SAS RAID Controller Module and should not be used in bay 1 of the BC-S chassis with SAS RAID Controller Modules installed.

6. If there are no blade servers in the BC-S chassis with an operating system installed, an external workstation is required for the initial setup of the BladeCenter chassis and the SAS RAID Controller Modules.
7. Review the *Installation and User's Guide* publications that were shipped with your BladeCenter S chassis, SAS RAID Controller Modules, blade servers, Ethernet switches and SAS expansion/connectivity card options.
8. Review the publications and release notes that were shipped with the IBM Storage Configuration Manager (SCM) software if SCM is going to be used to configure the SAS RAID Controller Modules.
9. Review the release notes that were included with the SAS RAID Controller Module firmware and any other firmware and device driver packages that will be used in the following procedures.

Considerations When Using a SAS Expansion Card on a System X or System P Host Blade

This section describes how to install an SAS Expansion Card on an LS (AMD), HS (Intel) or PS / JS (Power) host blade.

CAUTION:
Observe all ESD precautions and procedures while following these steps otherwise damage to the blade and or card may result.

Note: Only some host blades support the SAS Expansion adapter. For the most current support information, consult the *Blade Center Interoperability Guide*.

Tip: The SAS WWN is a 16 digit hexadecimal number printed on the SAS card (it is not available on SAS connectivity card, as the connectivity card uses the system board SAS controller). It is recommended that you record this number before installing the card as it will be used later when mapping LUNs to the host.

Note: Some hosts have an internal SAS Adapter. This will affect the installation of the Windows operating system if you intend to SAS Boot the host or use the internal adapter to run both the SAS RAID Controller Module and internal storage. Refer to the *Installation and Users Guide* for the host blade to determine if blade has an internal SAS adapter.

It is common to install the operating system on the logical drive. Then define volumes from the SAS RAID Module to this same blade. Then the blade does not reboot. If you encounter this issue, review the boot order in your SAS controller configuration.

If the host blade has an internal SAS adapter, it is necessary that the SAS expansion card driver be installed as an additional driver during the OS installation to ensure that the host can access the storage properly.

If the host has come preconfigured with both the internal and expansion card drivers updated then proceed with the OS installation and expansion card updates.

Note: The Bootable Media Creator tool can assist you updating firmware on a blade prior to installing an operating system. UpdateXpress Systems pack Installer can help you install or update drivers and firmwares once the operating system is installed. These tools can be found on the IBM Toolscenter web site:

the ServerProven compatibility

Considerations When Using a SAS Connectivity Card on an x86-64 blade or a PS / JS (System P) Host Blade

This section describes how to install an SAS Connectivity Card on an System X or System P host blade.

CAUTION:
Observe all ESD precautions and procedures while following these steps otherwise damage to the blade and or card may result.

Note: Only some of the Intel or AMD host blades running Linux support the SAS Connectivity Card. For the most current support information, consult the *Blade Center Interoperability Guide*.

Hosts using the SAS Connectivity Card utilize the internal SAS controller built into the motherboard of the host blade. The SAS Connectivity Card allows this internal HBA adapter to connect to the BladeCenter-S chassis SAS fabric.

Note: For hosts that use the SAS Connectivity Card, the internal hard drive and externally mapped drives are on the same storage bus. To configure the blade to boot correctly from the internal hard drive with the SAS Connectivity Card, the Onboard SAS Controller BIOS must be set to scan LUN0 only during the boot process and any external drives mapped to the host from the SAS RAID Controller Module must be mapped with LUN numbers greater than 0.

Chapter 2. Chapter 2 x86-64 (Intel or AMD) blades Running Linux Host Attachment

This section describes how to attach an Intel or Advanced Micro Devices (AMD) host blade running the Linux operating system to a SAS RAID Controller Module using SAS adapters.

This chapter contains the following sections:

- "Updating the Driver for SAS HBAs on x86-64 (Intel or AMD) Host Running Linux" on page 20
- "Updating the Firmware and BIOS on a SAS Expansion Card on x86-64 (Intel or AMD) Host Running Linux" on page 23
- For configuration of the SAS HBA BIOS, refer to Appendix A, "Appendix A: Configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host," on page 147
- "Configuring SAS Driver Settings on x86-64 (Intel or AMD) Host Running Linux" on page 24
- "Configuring Host System Settings on x86-64 (Intel or AMD) Host Running Linux" on page 26
- "Configuring the Device Mapper Multipathing Configuration File on x86-64 (Intel or AMD) Host Running Linux" on page 28
- "Configuration for Remote SAS Booting on x86-64 (Intel or AMD) Host Running Linux" on page 31

Before you attach a host, review the following information:

- For an overview of host attachment requirements, see "General requirements for attaching a host" on page 2 on page "General requirements for attaching a host" on page 2.
- For the most current information on supported hosts, operating systems, adapters, and switches, review the *IBM BladeCenter S SAS RAID Controller Module Interoperability Matrix*.

For additional SDD information, see the *IBM System Storage Multipath Subsystem Device Driver User's Guide* at

http://www.ibm.com/systems/support/storage/software/sdd

Notes:

- Host systems running the Linux operating system natively connected to the SAS RAID Controller Module support both single path and multipath connectivity.

Note: If this Linux installation is being set up on one of the supported virtualization environments, please refer to the section regarding the specific virtualization environment for host attachment details.

- Multipath connectivity is supported with the native Linux Device Mapper-Multipath I/O (DM-MPIO). For the most current list of supported OS levels and driver requirements, see the *IBM BladeCenter S SAS RAID Controller Module Interoperability Matrix*.

For additional information, go to the IBM System Storage Web site at

http://www.ibm.com/support/fixcentral/

Find and click the "**here"** link below the table.

- The steps in this section that are used to install and configure adapter cards are only examples. Your configuration might be different.
- Many Linux distributions enable administrators to configure their systems for automatic system updates. Administrators can configure these features to query for, and automatically install, all available, updates which can include updates to the kernel.

Tip: Consider turning off the automatic update feature. Some drivers that are supplied by IBM, such as HBA drivers, are dependent on a specific kernel and cannot function in the presence of a new kernel. HBA drivers must be compiled against specific kernels for optimal performance. By allowing automatic update of the kernel, you risk an unexpected impact to your host system.

Updating the Driver for SAS HBAs on x86-64 (Intel or AMD) Host Running Linux

This section describes how to update a SAS Expansion Card adapter driver on x86-64 (Intel or AMD) host blade that is running the Linux operating system. The following driver versions listed are only examples, the current firmware may be at a later version than shown in the following steps.

Procedure

1. Download the firmware file from the following URL onto your Linux server: http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020

   Select Product Family, then select 'Go'

   For Example: Product Family: BladeCenter LS22

Figure 3. Example of Product Family Search

Select the SAS Expansion card firmware update listed.

```
tar -xzf ibm_dd_mptsas_4.16.80.01_rhel5_32-64.tgz
```

2. Unpack the .tar file with the following command:

```
tar -xzf ibm_dd_mptsas_4.16.80.01_rhel5_32-64.tgz
```

3. Issue the following command to install the new package.

```
./install.sh --update --override
```

```
[root@zuni newcode]# tar xzf ibm_dd_mptsas_4.16.80.01_rhel5_32-64.tgz
[root@zuni newcode]# ls -l
total 4784
drwxrwxr-x 2 root root    4096 Feb 10 16:49 apps
-rw-r--r-- 1 root root 4802696 Feb 12  2009 ibm_dd_mptsas_4.16.80.01_rhel5_32-64.tgz
-rwxrwxr-x 1  501  501    2103 Jul 24  2007 install.sh
-rwxrwxr-x 1  501  501   19228 Jul 24  2007 LICENSE.fixid
-rwxrwxr-x 1  501  501    5463 Mar  6  2008 README.fixid
drwxrwxr-x 3 root root    4096 Feb 10 16:49 rhel5
drwxrwxr-x 2 root root    4096 Feb 10 16:53 SRPM
drwxrwxr-x 2  501  501    4096 Feb 10 16:36 tools
[root@zuni newcode]# ./install.sh --update --override --add-initrd

        Drivers will be installed/migrated to 2.6.18-53 version

------------------------------------------------------------------------
Checking kmod-lsi-mptlinux-4.16.80.01-1.x86_64.rpm
......
------------------------------------------------------------------------
kmod-lsi-mptlinux-4.16.80.01-1.x86_64.rpm installed successfully
SUCCESS
[root@zuni newcode]#
```

Figure 4. Example of Linux driver update

Note: The example shows an additional option to update the initrd image. If this is run, then the following step may be skipped.

4. The Linux initial RAM disk (initrd) image, may need to be rebuilt to update the newly installed driver in the image. To rebuild the image, consult the steps specific for the installed version of the Linux operating system.

   Important: If the driver has been updated on a host that is SAS booted and the host has already been configured for multi-pathing, please refer to"Configuration for Remote SAS Booting on x86-64 (Intel or AMD) Host Running Linux" on page 31, for host specific steps on updating the initrd image. If the host is not SAS booted, or is initially being setup for SAS booting and is still running in a single path configuration, then continue with the following steps.

   a. Back up the initial RAM disk (initrd) image by performing the following commands in the Linux shell.

      ```
      cd /boot
      mv initrd-`uname -r`.img initrd-`uname -r`.img.backup
      ```

   b. To build the new initrd image:

      Red Hat Enterprise Linux:

      ```
      mkinitrd -v /boot/initrd-`uname -r`.img `uname -r`
      ```

      SuSE Linux Enterprise Server:

      ```
      mkinitrd
      ```

5. Reboot the blade.
6. After the blade comes back up, run the following commands to verify that the driver is loaded and that it is being used during boot:
   - dmesg | grep -i fusion
   - cat /proc/mpt/version

   The output should be similar to the following figure.

```
[root@zuni ~]# dmesg | grep -i fusion
Fusion MPT base driver 4.16.80.01
Fusion MPT SAS Host driver 4.16.80.01
Fusion MPT SPI Host driver 4.16.80.01
Fusion MPT FC Host driver 4.16.80.01
Fusion MPT misc device (ioctl) driver 4.16.80.01
mptctl: Registered with Fusion MPT base driver
Fusion MPT LAN driver 4.16.80.01
[root@zuni ~]# cat /proc/mpt/version
mptlinux-4.16.80.01
  Fusion MPT base driver
  Fusion MPT SAS host driver
  Fusion MPT SPI host driver
  Fusion MPT FC host driver
  Fusion MPT ioctl driver
  Fusion MPT LAN driver
[root@zuni ~]#
```

Figure 5. Example of Linux output after driver update

Updating the Firmware and BIOS on a SAS Expansion Card on x86-64 (Intel or AMD) Host Running Linux

This section describes how to update a SAS Expansion Card adapter's firmware and BIOS on x86-64 (Intel or AMD) host blade that is running the Linux operating system. The following firmware versions listed are only examples, the current firmware may be at a later version than shown.

About this task

Note: The firmware versions listed are only examples, the current firmware may be at a later version than shown. The package may be different from the actual version shown as seen in the following figure.

Figure 6. Example of BIOS Discovery

Refer to the firmware package release notes to confirm that the correct firmware level is installed with the package level used.

Important: If installing version 2.71, or later, and coming from an earlier version on an HS22 blade, refer to Appendix C, "Appendix C: Procedure for MPTSAS FW upgrade of HS12, HS21-XM, HS21, HS22, HS22V, HX5 and LS20 blades," on page 161.

Note: A minimum driver version is required to update the firmware. If the minimum driver version has not been updated, please go to the section, "Updating the Driver for SAS HBAs on x86-64 (Intel or AMD) Host Running Linux" on page 20.

Procedure

1. As root, acquire the new code by going to the following URL and save the file (e.g. ibm_fw_mptsas_bc-sasexp-2.66_linux_32-64.bin) onto the Linux blade.

   http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020
2. From a terminal session on the Linux blade run the following commands:

   ```
   cd <to the location where the file was saved>
   chmod +x ibm_fw_mptsas_bc-sasexp-2.66_linux_32-64.bin
   ./ibm_fw_mptsas_bc-sasexp-2.66_linux_32-64.bin –s
   ```

   The output should be similar to the following figure.

```
[root@belen temp]# ./ibm_fw_mptsas_bc-sasexp-2.66_linux_32-64.bin -s
Checking for minimum version mptlinux-4.00.13.10 of /proc/mpt/versior
Active version of /proc/mpt/version is mptlinux-4.16.80.01

Minimum version detected, continuing....
This update is for the SAS Expansion Card (CFFv) for IBM BladeCenter

Controller 1 is a SAS Expansion Card (CFFv) for IBM BladeCenter.

Attempting to flash controller 1!

Updating firmware on Controller 1.  Please wait....
Update of controller 1 firmware completed successfully.

Updating BIOS on Controller 1.  Please wait....
Update of controller 1 BIOS completed successfully.

Updating FCODE on Controller 1.  Please wait....
Update of controller 1 FCODE completed successfully.

You must reboot your system to complete the firmware update process.
You do not need to reboot your system immediately.
```

Figure 7. Example output from Linux firmware update

Note: There may be a message stating "Controller 2 supported by a separate update". Disregard this message as it applies to further updates that are not included in this release.

3. Reboot the host.
4. As the host comes back up verify that it reflects the new level of SAS HBA firmware (for example 1.27.86.00) as seen at the bottom of the screen shot below.

Note: This update applies only to the LSILogic SAS1064, not the SAS1064E.

Configuring SAS Driver Settings on x86-64 (Intel or AMD) Host Running Linux

The following section describes how to perform required changes to the SAS driver settings when using x86-64 (Intel or AMD) host running Linux

Changing Queue depth and Hot plug settings

To edit the queue depth settings for host blades running the Linux operating system, perform the following steps.

About this task

Note: The actual value used will depend on the number of LUNs mapped to the host. See "Serial Attached SCSI host attachment" on page 12 to review how to calculate the correct settings, then return to this section.

Procedure

1. In a Linux shell, use vi to open an edit session of the file `/etc/modprobe.conf`.
2. Add the following line to the appropriate modprobe configuration file:

```
For SLES 10 and RHEL 5.x hosts: options mptsas
mpt_sdev_queue_depth=4 mpt_disable_hotplug_remove=1

For SLES 11 hosts: options mptsas mpt_sdev_queue_depth=4



For RHEL 6.x hosts with inbox LSI mptsas driver:
The queue depth setting will be stated in the following
section: Configuring Host System Settings on x86-64
(Intel or AMD) Host Running Linux

For BladeCenter HS23/HS23E with inbox LSI mpt2sas driver:
The queue depth setting will be stated in the following
section: Configuring Host System Settings on x86-64
(Intel or AMD) Host Running Linux
```

   Important: Make sure to update the value in the options line above. See "Serial Attached SCSI host attachment" on page 12 to review how to calculate the correct settings. If there is no entry for the mptsas driver already, add the line at the bottom of the file. Otherwise edit the line that already exists to match these options.

   The file should have an entry as highlighted as the following:

```
alias eth0 bnx2
alias eth1 bnx2
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptsas
alias scsi_hostadapter2 ata_piix
alias scsi_hostadapter3 usb-storage
options mptsas mpt_sdev_queue_depth=16 mpt_disable_hotplug_remove=1
```

3. Save the file
4. The Linux initial RAM disk (initrd) image needs to be rebuilt to pickup the changes made to the driver settings. To rebuild the image, consult the steps specific for the installed version of the Linux operating system.

   Important: If the driver has been updated on a host that is SAS booted and the host has already been configured for multipathing, please refer to Configuration for Remote SAS Booting on x86-64 (Intel or AMD) Host Running Linux, for host specific steps on updating the initrd image. If the host is not SAS booted, or is initially being set up for SAS booting and is still running in a single path configuration, then continue with the following steps.

   a. Back up the initial RAM disk (initrd) image or initial ram-based root file system (initramfs) image by performing the following commands in the Linux shell.

For Red Hat Enterprise Linux 6.x:

```
mv /boot/initramfs-`uname -r`.img initramfs-`uname -r`.img.bak
```

For Red Hat Enterprise Linux 5.x:

```
cd /boot
mv initrd-`uname -r`.img initrd-`uname -r`.img.backup
```

For SUSE Linux Enterprise:

```
cd /boot
mv initrd-`uname -r` initrd-`uname -r`.backup
```

b. To build the new initrd image:

For Red Hat Enterprise Linux 6.x:

```
dracut --force -v /boot/initramfs-`uname -r`.img `uname -r`
```

Red Hat Enterprise Linux:

```
mkinitrd -v /boot/initrd-`uname -r`.img `uname -r`
```

SUSE Linux Enterprise Server:

```
mkinitrd
```

5. Reboot the server.

Configuring Host System Settings on x86-64 (Intel or AMD) Host Running Linux

This section describes how to configure host system settings on x86-64 (Intel or AMD) host blade that is running the Linux operating system. The following firmware versions listed is only an example, the current firmware may be at a later version than shown.

About this task

SCSI mid-layer timeout: 60 seconds

Verify that the default values are correctly set. To verify the setting, change directory to the /sys/block/sdXX/device, where sdXX is one of the SAS RAID Controller Module devices. View the contents of the file named timeout. For example,

```
[ ... … ] # cd /sys/block/sdb/device
[ ... … ] # cat timeout
60
[ ... … ] #
```

Figure 8. Linux timeout settings

If the value is not set to 60, then use the following procedures to update the setting:

Procedure

1. **To change both the timeout and queue depth setting on the host using inbox mptsas or mpt2sas driver:**

   Note: Inbox mpt2sas driver is supported on BladeCenter HS23/HS23E.

   a. Change to the uDev rules directory as follows:

   ```
   cd /etc/udev/rules.d
   ```

For RHEL 6.x create the file named:

```
50-udev.rules
```

b. ADD the lines in the file:

```
ACTION=="add", SUBSYSTEM=="scsi", \
SYSFS{type}=="0|7|14", RUN+="/bin/sh -c 'echo 60 > /sys$$DEVPATH/timeout'"
ACTION=="add", SUBSYSTEM=="scsi", \
SYSFS{type}=="0|7|14", RUN+="/bin/sh -c 'echo 4 > /sys$$DEVPATH/queue_depth'"
```

Important: Make sure to update the value in the options line above. See "Serial Attached SCSI host attachment" on page 12 to review how to calculate the correct settings. If there is no entry for the mptsas/mpt2sas driver, add the line at the bottom of the file. Otherwise, edit the existing line to match these options.

c. Save the file and exit the editor.

d. Reboot the system and then verify the timeout and queue depth value as shown in Linux timeout settings figure.

2. **To change the timeout setting on SLES10.*x* or RHEL5.*x*:**

a. Change to the uDev rules directory as follows:

```
cd /etc/udev/rules.d
```

For SLES 10.x edit the file named:

```
50-udev-default.rules
```

For RHEL 5.x edit the file named:

```
50-udev.rules
```

b. Look for a line similar to:

```
ACTION=="add", SUBSYSTEM=="scsi" , \
SYSFS{type}=="0|7|14", RUN+="/bin/sh -c 'echo YY > \
/sys$$DEVPATH/timeout'"
```

Where YY may be a value other then 60. Set the value to 60 so that the line will look like the following:

```
ACTION=="add", SUBSYSTEM=="scsi" , \
SYSFS{type}=="0|7|14", RUN+="/bin/sh -c 'echo 60 > \
/sys$$DEVPATH/timeout'"
```

c. Save the file and exit the editor.

d. Reboot the system and then verify the timeout value as shown in Linux timeout settings figure.

3. **To change the timeout setting on SLES11.*x*:**

a. Change to the uDev rules directory.

```
cd /etc/udev/rules.d
```

b. Create the file 50-scsidisk.rules

```
vi 50-scsidisk.rules
```

c. Insert the following lines into the file.

```
ACTION=="add", SUBSYSTEM=="scsi" , \
SYSFS{type}=="0|7|14", RUN+="/bin/sh -c 'echo 60 > \
/sys$$DEVPATH/timeout'"
```

d. Save the file and exit the editor.

e. Reboot the system and verify the timeout value as shown in Linux timeout settings figure.

Configuring the Device Mapper Multipathing Configuration File on x86-64 (Intel or AMD) Host Running Linux

This section describes how to configure the Device Mapper Multipathing configuration file on x86-64 (Intel or AMD) host blade that is running the Linux operating system. The following firmware versions listed are only an example, the current firmware may be at a later version than shown.

Multipath.conf installation

This section describes the procedures of Multipath.conf installation.

About this task

The IBM BladeCenter S SAS RAID Controller Module uses the Linux Device Mapper (DM) multipath driver included with each Linux distribution for managing fail-over and fail-back of volumes between the two SAS RAID Controller Modules. However, the default configuration file (/etc/multipath.conf) needs to be replaced by one that has support for the SAS RAID Controller Module (device type 1820). To get the latest version of Linux Device Mapper (DM) Multipath configuration file that provides support for the SAS RAID Controller Module, go to the IBM support web site at:

http://www.ibm.com/support/docview.wss?uid=ssg1S4000107

The multipath configuration files and readmes are located at the bottom of the page.

Procedure

1. For RHEL 6.2 or above hosts
   a. Generate the DM multipath configuration file to /etc directory as multipath.conf.

      ```
      mpathconf --enable
      ```

   b. Confirm the multipath status is enabled by command mpathconf. See the mpathconf main page or run the mpathconf command with the `–help` option specified for more additional options.

      ```
      mpathconf
      mpathconf --find_multipaths y
      mpathconf --with_multipathd y
      ```

2. For Linux except for RHEL 6.2 and above hosts

   Perform the following steps to update the /etc/multipath.conf:

   a. Download the new DM multipath configuration file for the correct Linux operating system from IBM web site. Refer to the *IBM BladeCenter S SAS RAID Controller Module Interoperability Matrix* for the specific version of the multipath.conf file to use.

   b. Backup the existing /etc/multipath.conf:

      ```
      cp /etc/multipath.conf /etc/multipath.conf.org
      ```

   c. Copy the new DM multipath configuration file to /etc directory as multipath.conf

      ```
      cp <new DM multipath Config file name> \
      /etc/multipath.conf
      ```

Additional Settings for Red Hat Enterprise Linux

The following steps are additionally required for setting up multipath when using the RHEL operating system.

There are two RHEL multipath-tools packages - device-mapper-multipath and kpartx - that need to be at the correct level. The following procedure will verify that the minimum levels are installed.

To query the version of these packages, perform the following commands

```
rpm -qa | grep multipath
rpm -qa | grep kpartx
```

The version numbers for the device-mapper-multipath and kpartx packages that are shipped with Red Hat 5 update 2 are shown below:

```
[... ~]# rpm -qa | grep multipath
device-mapper-multipath-0.4.7-17.el5
[... ~]# rpm -qa | grep kpartx
kpartx-0.4.7-17.el5
[... ~]#
```

Note: The minimum version of device-mapper-multipath and kpartx packages that are supported with SAS RAID Controller Module are:

- device-mapper-multipath-0.4.7-12.el5_1.3
- kpartx-0.4.7-12.el5_1.3.

The multipath-tools packages can be downloaded from the Red Hat Support Network site, if needed. To install these packages, download them into a directory in the host system and perform the following commands from a Linux shell:

```
rpm -Uvh <device-mapper-multipath-PackageName.rpm> \
<kpartx-PackageName.rpm>
```

Once completed issue the following commands to verify that the tools are loaded:

```
rpm -qa | grep multipath
rpm -qa | grep kpartx
```

Verify that the version are now at the minimum levels. If the tools were successfully updated, reboot the host.

Following the reboot, to start the Linux Device Mapper (DM) multipath daemon and configure it to start automatically during future boots, perform the following commands:

```
service multipathd start
chkconfig multipathd on
```

Additional Settings for SUSE Linux Enterprise Server

The following steps are additionally required for setting up multipath when using the SLES operating system.

About this task

Procedure

1. Reboot the blade server.
2. Following the reboot, to start the Linux Device Mapper (DM) multipath daemon and configure it to start automatically during future boots, perform the following commands:

   ```
   service multipathd start
   chkconfig multipathd on
   ```

3. To avoid the following error messages on SLES10 Service Pack 2 or later, when accessing multipath tools, edit the prio_callout in the multipath.conf file.

   Note: These changes are already included in the multipath.conf version 3.03

   Example of error messages:

   ```
   # multipath -ll
   sde: Using deprecated prio_callout '/sbin/mpath_prio_alua /dev/%n' (controller setting)
   Please fixup /etc/multipath.conf
   sdm: Using deprecated prio_callout '/sbin/mpath_prio_alua /dev/%n' (controller setting)
   Please fixup /etc/multipath.conf
   ```

   a. Change to the /etc directory as follows:

      ```
      cd /etc
      ```

      Edit the file named:

      ```
      multipath.conf
      ```

   b. Look for this line:

      ```
      prio_callout "/sbin/mpath_prio_alua /dev/%n"
      ```

      Add a "#" to comment out that line and then add "prio alua" on the line below the commented line. See below for what the edits should look like:

      ```
      #prio_callout "/sbin/mpath_prio_alua /dev/%n"
      prio alua
      ```

   c. Save the file and exit the editor.

Multipath Configuration file setting considerations Linux HA Clustering Environments

If a Linux host will be setup for Linux HA clustering, it may be required to modify the multipath.conf file settings for the SAS RAID Controller Module so that proper HA failover occurs should one of the HA nodes fail to access the SAS RAID Controller Module. The following describes how to modify the settings.

The default settings that are used with the SAS RAID Controller Module are defined in the multipath.conf configuration file as follows:

```
...
    device {
        vendor                  "IBM"
        product                 "1820N00"
        ...
        no_path_retry           queue
    }
...
```

In the default configuration, the entry **no_path_retry**, is set to **queue** by default. This will cause the Linux host to continue to queue commands even when all paths to the SAS RAID Controller Module are offline. In non-HA environments, this allows for transient failures to occur where both paths may be offline for short periods of time. However, this may not be the desired behavior in a Linux HA Cluster environment. This setting can be modified to a value greater then zero to attempt a number of retries, or it may be set to fail, to cause the host to fail immediately if no path is available. Depending on the requirements of the configuration this setting may need to be modified to allow for expected operation.

Configuration for Remote SAS Booting on x86-64 (Intel or AMD) Host Running Linux

The following section describes how to configure Remote SAS Booting on x86-64 (Intel or AMD) host running Linux.

Refer to Appendix B, “Appendix B: SAS Boot Pre-Operating System Installation Activities,” on page 157, to validate that the system is ready to install a SAS booted operating system.

Operating system installation

Use the applicable procedures and instructions that are provided with your operating system software to configure the operating system on the boot volume that is mapped to the blade server. It is not the intention of this document to show how to install the operating systems or to select which software packages will be installed or required for the initial installation of the operating system.

Depending on the operating system version, you might have to provide the SAS expansion card device driver during the installation so that the operating system can recognize the mapped boot volume from the SAS RAID Controller Module. Follow the appropriate instructions for your operating system to specify the use of a SAS HBA device driver that is not included in the operating system image.

For Red Hat 5 installation only, the default disk partitioning will create / (root) and swap partitions using a Logical Volume Management (LVM) volume group. For installation to complete successfully you must edit the default boot partitions so that they are not managed by LVM. It is recommended to create all partitions manually not using LVM. It is further recommended to ensure that the “Force to be Primary partition” check box is checked when manually creating the / (root) and swap partitions. Please review carefully the post-installation steps because the tasks are slightly different depending on whether disk partitions are created using LVM or not.

Note: When installing a Linux operating system, knowledge of boot failure recovery using the rescue CD and editing the boot grub entry on-the-fly will be useful. Incorrect modifications to enable multipath might result in failure to boot into the Linux initrd image.

Post-Operating system installation activities

The following steps should be performed after the Linux operating system has been installed.

Important: After completing any topic outside this section, return to this section of the document to complete any remaining steps.

Before proceeding:

- update the SAS device driver and multipath driver as detailed in the section titled "Updating the Driver for SAS HBAs on x86-64 (Intel or AMD) Host Running Linux" on page 20.
- Update the host based settings as detailed in the section titled "Configuring SAS Driver Settings on x86-64 (Intel or AMD) Host Running Linux" on page 24.
- Enable multipath as detailed in the section titled "Configuring the Device Mapper Multipathing Configuration File on x86-64 (Intel or AMD) Host Running Linux" on page 28.

RHEL Specific Instructions

The following instructions are only used for RHEL based operating systems.

About this task

Note: The following instructions are only used for RHEL based operating systems. For SLES based operating systems, refer to "SLES Specific Instructions" on page 42.

Procedure

1. The following steps will update the multipath bindings file:

   To obtain the WWID of the boot volume, which should be /dev/sda, issue the following command. The boot disk can also be confirmed by issuing the 'df' command.

```
 [... ~]#/sbin/scsi_id -g -u -s /block/sda
36005076b0740c0ff0000000000000025
[... ~]#
```

Figure 9. Sample scsi_id output

   Note: For RHEL 6.2 or later, the command should be issued as below to obtain the WWID of boot volume.

```
[... ~]#/sbin/scsi_id -g -u -d /dev/sda
36005076b0740c0ff0000000000000025
[... ~]#
```

Figure 10. Sample scsi_id output in RHEL 6.2

   Edit /var/lib/multipath/bindings and verify or add the WWID as mpath0 as needed.

```
# Multipath bindings, Version : 1.0
# NOTE: this file is automatically maintained by the multipath
program.
# You should not need to edit this file in normal circumstances.
#
# Format:
# alias wwid
#
mpath0 36005076b0740c0ff0000000000000025
```

Figure 11. A sample of the /var/lib/multipath/bindings file.

Note: For RHEL 6.2 or later, Edit /etc/multipath/bindings and verify or add the WWID as mpath0 as needed.

```
# Multipath bindings, Version : 1.0
# NOTE: this file is automatically maintained by the multipath
program.
# You should not need to edit this file in normal circumstances.
#
# Format:
# alias wwid
#
mpath0 3500c5000660ce43
```

Figure 12. A sample of the /etc/multipath/bindings file.

Note: For RHEL 6.2 or later, if the devices are currently running single path, then it is advised to add the WWID in the /etc/multipath/wwids file.

```
[root@RSSM6-3 ~]# cat /etc/multipath/wwids
# Multipath wwids, Version : 1.0
# NOTE: This file is automatically maintained by multipath and
multipathd.
# You should not need to edit this file in normal circumstances.
#
# Valid WWIDs:
/36005076b0741aaff4f0dc28900001c9f/
[root@RSSM6-3 ~]#
```

Figure 13. A sample adding the WWID in the/etc/multipath/wwids file

2. Skip the following steps if you created the disk partitions using Logical Volume Management (LVM),

   Edit /etc/fstab replacing existing entry for / (root) and swap partitions (and other partitions created on the boot volume during the initial operating system installation) with /dev/mapper/mpath0px where x in the number that corresponds to the disk partition number. The /etc/fstab file example below shows the modifications to the file using mpath0p1 and mpath0p2 for /dev/sda1 and /dev/sda2, respectively.

```
[... ~]# cat /etc/fstab
/dev/mapper/mpath0p1    /           ext3    defaults        1 1
#LABEL=/                /           ext3    defaults        1 1
tmpfs                   /dev/shm    tmpfs   defaults        0 0
devpts                  /dev/pts    devpts  gid=5,mode=620  0 0
sysfs                   /sys        sysfs   defaults        0 0
proc                    /proc       proc    defaults        0 0
#LABEL=SWAP-sda21       swap        swap    defaults        0 0
/dev/mapper/mpath0p2    swap        swap    defaults        0 0
```

Figure 14. A modified /etc/fstab file when not using LVM

Note: The p1 and p2 suffix to "mpath0" refer to the partitions on /dev/sda. In the above /etc/fstab file modification example, the df command would have shown:

```
[... ~]# df
Filesystem       1K-blocks    Used      Available Use% Mounted on
/dev/sda1         11904588    2465784   8824320   22%  /
```

Figure 15. df command

And the "swapon –s " command would have shown:

```
[... ~]# swapon -s
Filename         Type            Size    Used    Priority
/dev/sda2        partition       3068404 0       -1
```

Figure 16. swapon –s

Another example of the modified /etc/fstab file is shown below. The mpath devices /dev/mapper/mpath0p1, /dev/mapper/mpath0p2 and /dev/mapper/mpath0p3 are used to replace /dev/sda1, /dev/sda2 and /dev/sda3 devices for the /boot, / (root) and swap partitions, respectively.

```
[... ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted
on
/dev/sda3             32586216   3186572  27717640  11% /
/dev/sda1               101086     13368     82499  14% /boot
tmpfs                  1492312         0   1492312   0% /dev/shm
[... ~]# swapon -s
Filename                        Type            Size    Used  Priority
/dev/sda2                       partition       8193140 0     -1

[... ~]# cat /etc/fstab
/dev/mapper/mpath0p3     /           ext3    defaults        1 1
#LABEL=/                 /           ext3    defaults        1 1
/dev/mapper/mpath0p1     /boot       ext3    defaults        1 2
#LABEL=/boot             /boot       ext3    defaults        1 2
tmpfs                    /dev/shm    tmpfs   defaults        0 0
devpts                   /dev/pts    devpts  gid=5,mode=620  0 0
sysfs                    /sys        sysfs   defaults        0 0
proc                     /proc       proc    defaults        0 0
/dev/mapper/mpath0p2     swap        swap    defaults        0 0
#LABEL=SWAP-sda2         swap        swap    defaults        0 0
```

Figure 17. Another example of modified /etc/fstab file when not using LVM

3. If using LVM for the / (root) and swap disk partitions, only edit the /boot entry in /etc/fstab. Since the / (root) and swap partitions are mounted on LVM partitions, they will be set up correctly by default. For example, if the df and swapon -s command output are as follows, the modifications to the /etc/fstab would be as shown below:

```
[... ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      38533760   3187220  33357524   9% /
/dev/sda1               101086     11875     83992  13% /boot
tmpfs                  1557848         0   1557848   0% /dev/shm
```

```
[... ~]# swapon -s
Filename                        Type        Size  Used  Priority
/dev/mapper/VolGroup00-LogVol01         partition 2031608     0
 -1
```

```
 [... ~]# cat /etc/fstab
/dev/VolGroup00/LogVol00 /              ext3    defaults        1 1
/dev/mapper/mpath0p1     /boot          ext3    defaults        1 2
#LABEL=/boot             /boot          ext3    defaults        1 2
tmpfs                    /dev/shm       tmpfs   defaults        0 0
devpts                   /dev/pts       devpts  gid=5,mode=620  0 0
sysfs                    /sys           sysfs   defaults        0 0
proc                     /proc          proc    defaults        0 0
/dev/VolGroup00/LogVol01 swap           swap    defaults        0 0
```

Figure 18. A modified /etc/fstab file when using LVM

4. (LVM only) Edit the /etc/lvm/lvm.conf file as follows:
   - Locate the filter section in /etc/lvm/lvm.conf file
   - If there is already a filter section active, add `"a|/dev/mapper/mpath|"` to the filtered list.
   - If there is no filter section active, then add a filter with the following:

```
filter = ["a|/dev/mapper/mpath|","a|/dev/sda|","r|.*|"]
```

- Locate the types section in the /etc/lvm/lvm.conf file and add the following line:

```
types = [ "mpath", 16 ]
```

```
... ... ...

# A filter that tells LVM2 to only use a restricted set of
devices.
# The filter consists of an array of regular expressions.  These
# expressions can be delimited by a character of your choice, and
# prefixed with either an 'a' (for accept) or 'r' (for reject).
# The first expression found to match a device name determines if
# the device will be accepted or rejected (ignored).  Devices
that
# don't match any patterns are accepted.

# Be careful if there are symbolic links or multiple filesystem
# entries for the same device as each name is checked separately
against
# the list of patterns.  The effect is that if any name matches
any 'a'
# pattern, the device is accepted; otherwise if any name matches
any 'r'
# pattern it is rejected; otherwise it is accepted.

# Don't have more than one filter line active at once: only one
gets used.

# Run vgscan after you change this parameter to ensure that
# the cache file gets regenerated (see below).
# If it doesn't do what you expect, check the output of 'vgscan -
vvvv'.

# By default we accept every block device:
# filter = [ "a/.*/" ]

# Exclude the cdrom drive
# filter = [ "r|/dev/cdrom|" ]

# When testing I like to work with just loopback devices:
# filter = [ "a/loop/", "r/.*/" ]

# Or maybe all loops and ide drives except hdc:
# filter =[ "a|loop|", "r|/dev/hdc|", "a|/dev/ide|", "r|.*|" ]

# Or for SAS RAID Controller Module multipath
filter =[ "a|/dev/mapper/mpath|", "a|/dev/sda|", "r|.*|" ]

# Use anchors if you want to be really specific
# filter = [ "a|^/dev/hda8$|", "r/.*/" ]

# Advanced settings.

... ... ...

# List of pairs of additional acceptable block device types found
# in /proc/devices with maximum (non-zero) number of partitions.
# types = [ "fd", 16 ]

types = [ "mpath", 16 ]

# If sysfs is mounted (2.6 kernels) restrict device scanning to
... ... ...
```

Figure 19. A snippet of the modified /etc/lvm/lvm.conf file

Note:

– This will modify how LVM can detect LVM managed volumes. If LVM is managing non-multipath devices, then the filter section will need to be modified to also include the additional volumes managed.
– The device /dev/sda must be included in the filter section. Without this device, when rebuilding initrd LVM would not see any LVM partitions and would not configure LVM.

Attention: Skip steps 5 and 6 in RHEL 6.2 or later to use default settings.

5. Copy /sbin/mkinitrd file to /sbin/mkinitrd.mpath and edit that file so that mpath entries are correctly included and rebuild the initrd image.
6. The following changes need to be made to /sbin/mkinitrd.mpath:
   - Line 991 (Approx):

     ```
     use_multipath=1
     ```

   - Line 1330 (Approx): Comment out the following three lines:

     ```
     #for wwid in $root_wwids ; do
     #    emit "/bin/multipath -v 0 $wwid"
     #done
     ```

   And add the following line:

   ```
   emit "/bin/multipath -v 0"
   ```

   The result at line 1330 should look like the following when completed:

```
    … … … … …

if [ "$use_multipath" == "1" ]; then
    emit "echo Creating multipath devices"
    #for wwid in $root_wwids ; do
    #    emit "/bin/multipath -v 0 $wwid"
    #done
    emit "/bin/multipath -v 0"
    emit "dmsetup ls --target multipath --exec 'kpartx -a -p p'"
fi
   … … … … …
```

Figure 20. The result at line 1330

Note: Above change is already included in RHEL5.7 or above.

7. Use /sbin/mkinitrd.mpath to build a new Linux initrd image as follows (Note: this command should be entered on a single line not as two lines as shown):

   ```
   /sbin/mkinitrd.mpath -f -v --with=dm-round-robin \
   /boot/initrd-`uname -r`.mpath.img.gz `uname -r`
   ```

   Note: Whenever the initrd image must be rebuilt, the edited mkinitrd.mpath must be used. Otherwise, an invalid initrd image will be created and may result in the system not booting successfully.

   For RHEL 6.2 or later, the following command should be used instead to build a new Linux initrd image. (Note: this command should be entered on a single line not as two lines as shown):

   ```
   dracut --force -v /boot/initramfs-`uname -r`.img `uname -r`
   ```

8. Edit /boot/grub/menu.lst to boot to the new Linux initrd image that is created in the above step. Make a copy of the lines that already exist after hiddenmenu. Modify the “title” and “initrd” lines as shown below to provide a new title and point to the Linux initrd image with multipath enabled for the

boot volume. In addition, depending on whether LVM was used during the disk partitioning or not, the "kernel" line may need to be modified. If LVM is not used, the root parameter in the "kernel" line must be modified to point to a /dev/mapper/mpath_pX device that replaces the /dev/sdaX device of the / (root) partition (e.g. change /dev/sda1 to /dev/mapper/mpath0p1 or /dev/sda3 to /dev/mapper/). If LVM is used, leave the root parameter intact as it should already point to a volume in a volume group (e.g. /dev/VolGroup00/LogVol00).

Note: If the RHEL OS was installed under UEFI mode, then the path of boot menu file would be /boot/efi/EFI/redhat/grub.conf

```
… … … … …
title Red Hat Enterprise Linux Server mpath (2.6.18-274.el5)
 root (hd0,0)
 kernel /vmlinuz-2.6.18-274.el5 ro root=/dev/mapper/mpath0p1 rhgb
verbose
 initrd /initrd-2.6.18-274.el5.mpath.img.gz
```

Figure 21. Modified /boot/grub/menu.lst file when not using LVM for RHEL5.7

```
… … … … …
title Red Hat Enterprise Linux Server mpath (2.6.18-92.el5)
 root (hd0,0)
 kernel /boot/vmlinuz-2.6.18-92.el5 ro root=/dev/mapper/mpath0p1
rhgb verbose
 initrd /boot/initrd-2.6.18-92.el5.mpath.img.gz
title Red Hat Enterprise Linux Server (2.6.18-53.el5)
 root (hd0,0)
 kernel /boot/vmlinuz-2.6.18-53.el5 ro root=LABEL=/ rhgb quiet
 initrd /boot/initrd-2.6.18-53.el5.img
```

Figure 22. A sample of the modified /boot/grub/menu.lst file when not using LVM

```
… … … … …
title Red Hat Enterprise Linux Server mpath (2.6.18-92.el5)
 root (hd0,0)
 kernel /vmlinuz-2.6.18-92.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet
 initrd /initrd-2.6.18-92.el5.mpath.img.gz
title Red Hat Enterprise Linux Server (2.6.18-92.el5)
 root (hd0,0)
 kernel /vmlinuz-2.6.18-92.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet
 initrd /initrd-2.6.18-92.el5.img
```

Figure 23. A sample of the modified /boot/grub/menu.lst file when using LVM

9. Before rebooting the blade server to enable multipath on the boot volume, take a moment to make sure that all of the steps described above are performed correctly. Any mistakes or omissions may mean that you will not be able to boot into Linux and you will have to use the Linux rescue CD to recover.
10. Once rebooted, verify that the multipath –ll command produces output similar to this example:

```
# multipath -ll
mpath0 (36005076b0740c0ff0000000000000025) dm-0 IBM,1820N00
[size=15G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
\_ 0:0:0:0 sda 8:0   [active][ready]
```

Figure 24. The multipath_command_produces_output

11. Verify that the blade server is configured correctly using the following commands. In each of these commands, mpath0pX devices should be seen instead of /dev/sdaX.

    ```
    df
    swapon –s
    ```

    With LVM enabled on the boot volume, the output should be similar to this. Note that the /dev/mapper/mpath0p1 device is displayed instead of the /dev/sda1.

```
[... ~]# df
Filesystem           1K-blocks    Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      38533760  3271976  33272768   9% /
/dev/mapper/mpath0p1    101086    27276     68591  29% /boot
tmpfs                  1557848        0   1557848   0% /dev/shm
[... ~]# swapon -s
Filename                                Type       Size    Used
Priority
/dev/mapper/VolGroup00-LogVol01         partition  2031608 0    -1
[... ~]#
```

Figure 25. The output with LVM

Without LVM, the output should be similar to this:

```
[... ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted
on
/dev/mapper/mpath0p3  36554540   3197732  31469976  10% /
/dev/mapper/mpath0p1    101086     21364     74503  23% /boot
tmpfs                  1557848         0   1557848   0% /dev/shm
/dev/sdb1              1991948   1827432    164516  92%
/media/BADCRUZER
[... ~]# swapon -s
Filename                        Type            Size    Used
Priority
/dev/mapper/mpath0p2            partition       4096564 0       -1
[... ~]#
[... ~]# ls /dev/mapper/
control  mpath0  mpath0p1  mpath0p2  mpath0p3
[... ~]#
```

Figure 26. The output without LVM

12. The second path to the boot volume can now be added to the system using the normal SAS RAID Controller Module processes such as SCM or the SAS RAID Controller Module CLI. Other data volumes can also be mapped to both

ports of the blade server SAS adapters at this time. To rescan for devices dynamically on Linux, use the following command:

```
for i in `ls -1d /sys/class/scsi_host/*`; do
    echo $i/scan; echo "- - -" > $i/scan;
done
```

13. When the second path to the boot volume is seen by the Linux DM multipath daemon, the multipath –ll command should show two available paths to the boot volume as follows. If the number of available paths is not shown correctly, verify the mapping of volumes to SAS adapter ports using the SAS RAID Controller Module CLI interface or the SCM client and then reboot the server.

```
[... ~]# multipath -ll
mpath0 (36005076b0740c0ff0000000000000025) dm-0 IBM,1820N00
[size=15G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
\_ 0:0:0:0 sda 8:0   [active][ready]
\_ round-robin 0 [prio=10][enabled]
\_ 0:0:1:0 sdb 8:16  [active][ready]
```

Figure 27. The multipath –ll command

If there are more than one volume mapped to the blade server, one would see them displayed as shown below.

```
[... ~]# multipath -ll
\mpath1 (36005076b07412fff48f0e27500000009) dm-1 IBM,1820N00
[size=40G][features=1 queue_if_no_path][hwhandler=0]
\_ round-robin 0 [prio=50][enabled]
 \_ 0:0:0:1 sdb 8:16  [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 0:0:1:1 sdd 8:48  [active][ready]
mpath0 (36005076b07412fff48ed04c100000003) dm-0 IBM,1820N00
[size=40G][features=1 queue_if_no_path][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 0:0:0:0 sda 8:0   [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 0:0:1:0 sdc 8:32  [active][ready]
[... ~]#
```

Figure 28. More than one volume - multipath command

14. (Optional) If using LVM, the device /dev/sda can now be removed from the filter section as multipath is now being used to manage the root volume. If this is done the mkinitrd.mpath script needs to be run again to update the Linux initrd image with the new LVM settings. Reboot the server to the new Linux initrd image.

SLES Specific Instructions

Perform the following steps to complete the installation of SLES Linux operating system on a SAS RAID Controller Module boot volume.

About this task

Note: The following instructions are only used for SLES based operating systems. For RHEL based operating systems, refer to "RHEL Specific Instructions" on page 32.

Steps 1, 6, 7, 8, 9, and 10 are performed only when the rebuilding of initial RAM disk (initrd) is needed.

Procedure

1. Edit multipath.conf and turn off 'user_friendly_names' by commenting the line out as shown below.

```
    … … … …
defaults {
    polling_interval    30
    failback            immediate
    no_path_retry       5
    rr_min_io           100
```

```
    path_checker        tur
#    user_friendly_names yes
   … … … …
```

Figure 29. A snippet of the modified /etc/multipath.conf in SLES

   Note: This option will need to be turned back on later in step 9.

2. Perform the following command to get the WWID of your boot volume (e.g. mpath 0)
   - For SLES 10.x:

     ```
     /sbin/scsi_id –g –u –s /block/sda
     ```

```
[... ~]#/sbin/scsi_id -g -u -s /block/sda
36005076b0740c0ff0000000000000025
[... ~]#
```

Figure 30. Example output of scsi_id command for SLES 10

   - For SLES 11.1:

     ```
     /lib/udev/scsi_id -g -u -d /dev/sda
     ```

```
[... ~]# /lib/udev/scsi_id -g -u -d /dev/sda
35000c5000b930b3f
[... ~]#
```

Figure 31. Example output of scsi_id command for SLES 11.1

- For SLES 11.2:

  ```
  /lib/udev/scsi_id --whitelisted –device=/dev/sda
  ```

```
[... ~]# /lib/udev/scsi_id --whitelisted -device=/dev/sda
35000c5000b930b3f
[... ~]#
```

Figure 32. Example output of scsi_id command for SLES 11.2

- For SLES 11.3:

  ```
  /lib/udev/scsi_id --page=0x83 --whitelisted --device=/dev/sda
  ```

```
linux-xslr:~ # /lib/udev/scsi_id --page=0x83 --whitelisted --device=/dev/sda
3500000e1131087e0
linux-xslr:~ # _
```

Figure 33. Example output of scsi_id command for SLES 11.3

3. Edit the /var/lib/multipath/bindings file and add an alias for mpatha as the WWID. If the binding line does not exist, create one.

   Note: For SLES 11.2 or later, edit the /etc/multipath/bindings file

```
# Multipath bindings, Version : 1.0
# NOTE: this file is automatically maintained by the multipath
program.
# You should not need to edit this file in normal circumstances.
#
# Format:
# alias wwid
#
mpatha 36005076b0740c0ff0000000000000025
```

Figure 34. Example edit of multipath bindings file

4. Add “dm-multipath dm-round-robin” multipath modules to the INITRD_MODULES line in the /etc/sysconfig/kernel.

```
## Path:        System/Kernel
## Description:
## Type:        string
## Command:     /sbin/mkinitrd
#
# This variable contains the list of modules to be added to the
initial
# ramdisk by calling the script "mkinitrd"
# (like drivers for scsi-controllers, for lvm or reiserfs)
#
INITRD_MODULES="ata_piix mptsas processor thermal fan reiserfs
edd dm-multipath dm-round-robin"
    … … … … …
```

Figure 35. A snippet of the modified /etc/sysconfig/kernel file

5. Make sure that the / (root) and swap device are referenced in /etc/fstab by their by-id device node entries instead of /dev/sd* type names. An example of an /etc/fstab file is shown below. Note that the / (root) and swap devices both begin with /dev/disk/by-id/

```
/dev/disk/by-id/scsi-36005076b07412fff48ed04ed00000006-part2 /
reiserfs   acl,user_xattr        1 1
/dev/disk/by-id/scsi-36005076b07412fff48ed04ed00000006-part1 swap
swap       defaults              0 0
proc                 /proc               proc       defaults
0 0
sysfs                /sys                sysfs      noauto
0 0
debugfs              /sys/kernel/debug   debugfs    noauto
0 0
usbfs                /proc/bus/usb       usbfs      noauto
0 0
devpts               /dev/pts            devpts
mode=0620,gid=5     0 0
```

Figure 36. An example of /etc/fstab file in SLES10

6. Backup the exiting initrd file

   ```
   cp /boot/initrd-`uname -r` /boot/initrd-`uname -r`-orig
   ```

7. Create the new bootloader with mkinitrd

   ```
   mkinitrd –f mpath
   ```

   Note: For SLES 11.2 or later, use the following line.

   ```
   mkinitrd -f multipath
   ```

8. Edit /boot/grub/menu.lst and add in a boot by-id for root and resume as shown below. Also modify secondary boot initrd.

   Example changes are in bold. The first boot entry was added to the file.

```
# Modified by YaST2. Last modification on Thu Oct  9 14:35:42 UTC
2008
default 0
timeout 8
##YaST - generic_mbr
gfxmenu (hd0,1)/boot/message
##YaST - activate

###Don't change this comment - YaST2 identifier: Original name:
linux###
title SUSE Linux Enterprise Server 10 mpath SP2
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.16.60-0.21-smp root=/dev/disk/by-
id/scsi-36005076b07412fff48ed04ed00000006-part2 vga=0x317
resume=/dev/sda1 splash=silent showopts
    initrd /boot/initrd-2.6.16.60-0.21-smp

###Don't change this comment - YaST2 identifier: Original name:
linux###
title SUSE Linux Enterprise Server 10 SP2
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.16.60-0.21-smp root=/dev/disk/by-
id/scsi-36005076b07412fff48ed04ed00000006-part2 vga=0x317
resume=/dev/sda1 splash=silent showopts
    initrd /boot/initrd-2.6.16.60-0.21-smp-orig

###Don't change this comment - YaST2 identifier: Original name:
failsafe###
title Failsafe -- SUSE Linux Enterprise Server 10 SP2
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.16.60-0.21-smp root=/dev/disk/by-
id/scsi-36005076b07412fff48ed04ed00000006-part2 vga=normal
showopts ide=nodma apm=off acpi=off noresume edd=off 3
    initrd /boot/initrd-2.6.16.60-0.21-smp
```

Figure 37. A sample of the modified /boot/grub/menu.lst in SLES 10

9. Re-enable user_friendly_names in multipath.conf file by remove the # that was placed in front of user_friendly_names earlier in this process.

   Important: When ever the initrd image is built, the user_friendly_names must be commented out before building the initrd image, then uncommented before rebooting.

10. Reboot the host. Make sure the first boot image is loaded (the first option in the menu.lst above)
11. Check to see that multipath has picked up and partitioned your boot device by performing the following commands in the blade server telnet session or Command Line terminal window:

    ```
    multipath –ll
    ls /dev/mapper
    df
    swapon –s
    ```

```
 [... ~]# multipath -ll
mpatha (36005076b07412fff48ed04ed00000006) dm-0 IBM,1820N00
[size=40G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 2:0:0:0 sda 8:0   [active][ready]
[... ~]# ls /dev/mapper
control  mpatha  mpatha-part1  mpatha-part2
[... ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted
on
/dev/dm-2             39831932   2622784  37209148   7% /
udev                   1545864       152   1545712   1% /dev
[... ~]# swapon-s
Filename                 Type        Size        Used  Priority
/dev/dm-1                partition   2104472     0     -1
```

Figure 38. Example output for checking SLES multipath configuration

12. The second path of the boot volume can now be added to the system using the normal SAS RAID Controller Module processes such as SCM or SAS RAID Controller Module CLI. Other data volumes can also be mapped to both ports of the blade server SAS HBA at this time.
13. Reboot the blade server to get the second path and additional volumes recognized by the blade server.
14. When the second path to the boot volume is seen by the Linux DM multipath daemon, the multipath –ll command should show two available paths to the boot volume as follows. If the number of available paths is not shown correctly, check the volume(s) to SAS adapter port mapping using the SAS RAID Controller Module CLI interface or the SCM client and reboot the server.

```
[... ~]# multipath -ll
mpatha (36005076b07412fff48ed04ed00000006) dm-0 IBM,1820N00
[size=40G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 2:0:0:0 sda 8:0   [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 2:0:1:0 sdb 8:16  [active][ready]
[... ~]#
```

Figure 39. The multipath –ll command

If there are more than one volume mapped to the blade server, one would see them displayed as shown below.

```
[... ~]# SAS RAID Controller Module-Sles10:~ # multipath -ll
mpathb (36005076b07412fff48f0e2bd0000000a) dm-0 IBM,1820N00
[size=40G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 2:0:0:1 sdb 8:16  [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 2:0:1:1 sdd 8:48  [active][ready]
mpatha (36005076b07412fff48ed04ed00000006) dm-1 IBM,1820N00
[size=40G][features=0][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 2:0:0:0 sda 8:0   [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 2:0:1:0 sdc 8:32  [active][ready]
[... ~]#
```

Figure 40. More than one volume mapped to the blade server-the multipath –ll command

Troubleshooting

This section covers currently known issues with using the IBM BladeCenter S SAS RAID Controller Module with the host blades running the Linux operating system.

Concurrent controller maintenance procedure

When performing some maintenance procedures on the SAS RAID Controller Module, one path to data volumes will become not available temporarily. These procedures include:

1. Replace one of the controllers.
2. Shutdown one of the controllers to service mode and then reboot it.
3. Power off one of the controllers in AMM and then power it on.
4. Reboot one of the controllers.

To ensure the host I/O will not be disturbed by the maintenance, please make sure that all paths are restored after the SAS RAID Controller Module has been rebooted or replaced.

After the maintenance operation is complete, first verify the controllers are in bound state by issuing the following commands:

```
<CLI> list controller
Current Machine Local Time: 08/12/2013  02:35:17 PM
 ____________________________________________________________________
|   Ctlr#    |   Controller   |       Status       |  Ports  |  LUNs   |
|____________|________________|____________________|_________|_________|
|          0 |          Ctlr0 |            PRIMARY |       1 |       0 |
|          1 |          Ctlr1 |          SECONDARY |       1 |       0 |
|____________|________________|____________________|_________|_________|
```

Figure 41. Commands

Secondly, check the host blade multipathing has restored all available paths to both SAS RAID Controller Modules. To perform this check on the host blade run the following command as root:

```
~> multipath –ll
```

The output of the command should be similar to the following, showing two paths to each volume:

```
mpath0 (36005076b074060ff49a7ad800000003d) dm-0 IBM,1820N00
[size=40G][features=1 queue_if_no_path][hwhandler=0]
\_ round-robin 0 [prio=50][active]
 \_ 1:0:8:0  sda 8:16  [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 1:0:9:0  sdc 8:176 [active][ready]
mpath1 (36005076b074060ff48e10daa00000020) dm-1 IBM,1820N00
[size=2.0G][features=1 queue_if_no_path][hwhandler=0]
\_ round-robin 0 [prio=50][enabled]
 \_ 1:0:8:1  sdb 8:48  [active][ready]
\_ round-robin 0 [prio=10][enabled]
 \_ 1:0:9:1  sdd 8:208 [active][ready]
```

If the output shows only one path or a mix of paths to the SAS RAID Controller Modules, then run the following command to restore the redundant paths:

```
~> multipath
```

Verify that after running the above command all paths become available using the following command:

```
~> multipath –ll
```

Multipath verification in a SAS booted host running RHEL 6.2

When performing maintenance that causes a reboot on the SAS booted host running RHEL 6.2, it is possible that part of the multipath entries may not be restored after rebooting.

After the maintenance operation is complete, verify that the host blade multipathing has restored all available entries. To perform this verification on the host blade, check all the multipath entries are correctly configured in /dev/mapper.

If the output of the multipath entries looks similar to the following (only showing part of the configured entries):

```
[root@RSSM mapper]# ls /dev/mapper
control      mpathcp2      mpathhp3      mpathlp4      mpathop4
mpatha      mpathcp3      mpathhp4      mpathmp1      mpathp
mpathapl      mpathcp4      mpathjp4      mpathmp3      mpathpp1
mpathap2      mpathdp2      mpathlp1      mpathop1      mpathpp2
mpathap3      mpathhp1      mpathlp2      mpathop2      mpathpp3
mpathcp1      mpathhp2      mpathlp3      mpathop3      mpathpp4
```

Download and install the updated device-mapper-multipath packages to fix this issue. Go to Red Hat Customer Portal website at http://rhn.redhat.com/errata/RHBA-2012-0946.htmlfor more information.

Verify that after the packages are installed the above command, all entries restored correctly under /dev/mapper:

```
[root@RSSM mapper]# multipath
[root@RSSM mapper]# ls
control      mpathbp3      mpathdp1      mpathep4      mpathgp2
mpatha      mpathbp4      mpathdp2      mpathf      mpathgp3
mpathap1      mpathc      mpathdp3      mpathfp1      mpathgp4
mpathap2      mpathcp1      mpathdp4      mpathfp2      mpathh
mpathap3      mpathcp2      mpathe      mpathfp3      mpathhp1
mpathb      mpathcp3      mpathep1      mpathfp4      mpathhp2
mpathbp1      mpathcp4      mpathep2      mpathg      mpathhp3
mpathbp2      mpathd      mpathep3      mpathgp1      mpathhp4
```

Multipath verification in a SAS booted host running SLES 11 SP3

When performing maintenance that causes a reboot on the SAS booted host running SLES 11 SP3, part of the multipath entries may not be restored after rebooting.

After the maintenance operation is complete, verify that the host blade multipathing has restored all available entries. To perform this verification on the host blade, check all the multipath entries are correctly configured in /dev/mapper.

```
linux-pwbp:~ # ls /dev/mapper/ -l
total 0
crw-rw---- 1 root root 10, 236 Jul 25 16:37 control
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathb_part1 -> ../dm-11
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathb_part2 -> ../dm-12
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathb_part3 -> ../dm-13
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathb_part4 -> ../dm-14
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathc_part1 -> ../dm-19
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathc_part2 -> ../dm-20
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathc_part3 -> ../dm-21
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathc_part4 -> ../dm-22
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathd_part1 -> ../dm-15
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathd_part2 -> ../dm-16
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathd_part3 -> ../dm-17
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathd_part4 -> ../dm-18
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathe_part1 -> ../dm-23
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathe_part2 -> ../dm-24
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathe_part3 -> ../dm-25
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathe_part4 -> ../dm-26
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathf_part1 -> ../dm-31
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathf_part2 -> ../dm-32
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathf_part3 -> ../dm-33
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathf_part4 -> ../dm-34
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathg_part1 -> ../dm-27
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathg_part2 -> ../dm-28
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathg_part3 -> ../dm-29
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathg_part4 -> ../dm-30
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathh -> ../dm-10
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathh_part1 -> ../dm-35
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathh_part2 -> ../dm-36
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathh_part3 -> ../dm-37
lrwxrwxrwx 1 root root       8 Jul 25 16:38 mpathh_part4 -> ../dm-38
```

If the output of the multipath entries looks similar to the above (only showing part of the configured entries), please issue the following two commands to restore all the multipathing entries.

```
multipath -F
multipath
```

Chapter 3. Chapter 3 x86-64 (Intel or AMD) Blades Running Windows Host Attachment

This section describes how to attach an Intel or Advanced Micro Devices (AMD) host blade running the Windows operating system to a SAS RAID Controller Module using SAS adapters.

This chapter includes the following sections:

- "Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running Windows"
- "Updating the Firmware and BIOS on a SAS Expansion Card on x86-64 (Intel or AMD) Host Running Windows" on page 57
- For configuration of the SAS HBA BIOS, refer to Appendix A, "Appendix A: Configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host," on page 147
- "Configuring the SAS HBA Driver on x86-64 (Intel or AMD) Host Running Windows" on page 61
- "Configuring SDD DSM on x86-64 (Intel or AMD) Host Running Windows" on page 62
- "Configuration for SAS Booting on x86-64 (Intel or AMD) Host Running Windows" on page 64
- "System Configuration Settings for use with Microsoft Windows Clustering" on page 67
- "Modification of Windows Performance settings" on page 80

Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running Windows

This section describes how to update the driver for a SAS HBA on x86-64 (Intel or AMD) host blade that is running the Windows operating system. The following is an outline of the steps that will be performed during this section.

About this task

- Download the applicable firmware file from the support and downloads website. It is recommended that you download it to the host desktop.
- Follow the README instructions for installation.
- After installation you will be prompted to reboot to complete the driver installation. When the host has rebooted you can check the driver level by entering the Device Manager view from the Management option for the host.

Note: The following versions listed are only examples, the current version available may be at a later version than shown.

Procedure

1. Download the applicable firmware file from the support and downloads website. It is recommended that you download it to the host desktop. Download the file from the following URL http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020

   Select Product Family, then select **'Go'**

Figure 42. Example of Product Family Search

Select the SAS Expansion card firmware update listed.

2. Unzip the file and copy the .exe file onto the desktop.

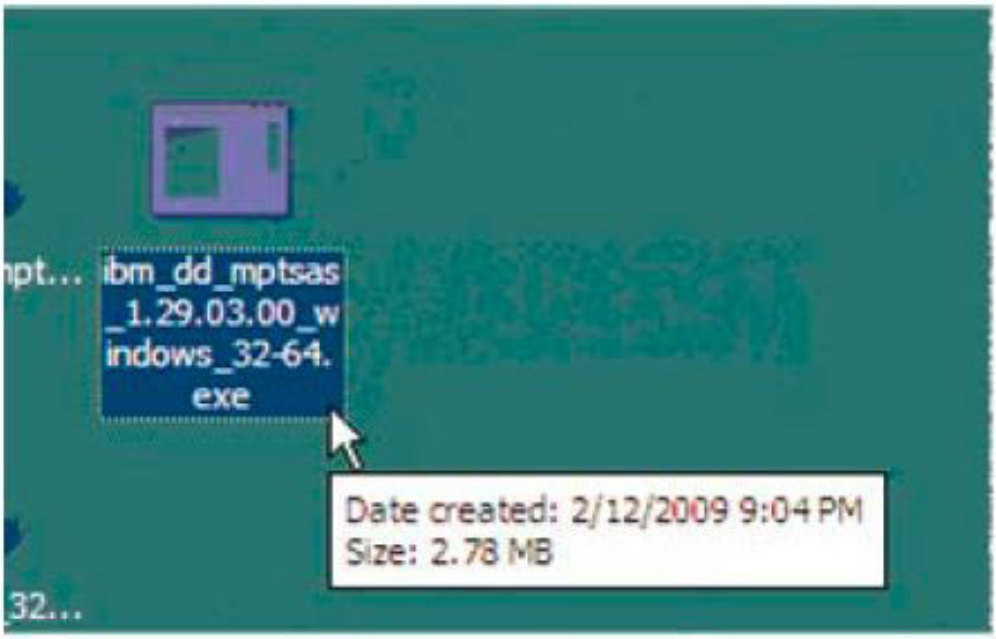


Figure 43. Example firmware file

3. Double click on the .exe file to begin the code load.
4. Select Perform Update and click on the Next button.

Figure 44. Select Perform Update

5. Click on the Update button.

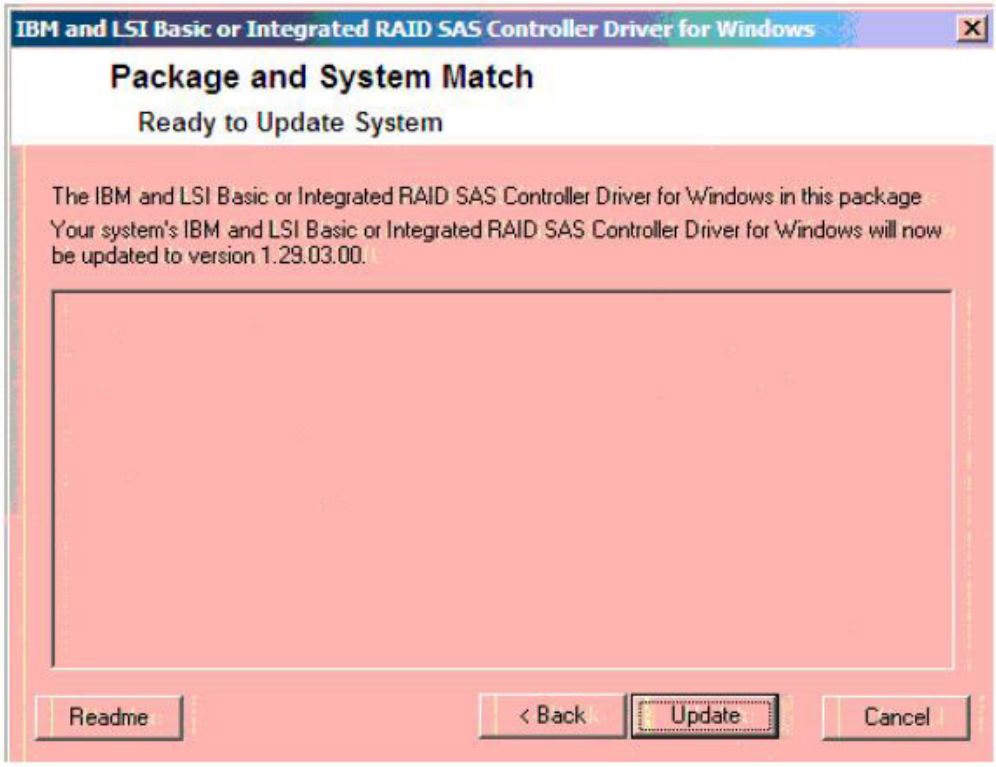


Figure 45. Click Update

6. Click on the Exit button.

Figure 46. Click on the Exit button

7. Reboot the blade.
8. To verify the level right click on My Computer and select Manage. In the left pane of the Manage screen click on Device manager. In the right pane click the (+) sign next to 'SCSI and RAID controllers,' (in Windows Server 2008/2012 it is called 'Storage Controllers,') to display the controllers on your system. Right click on the controller and select Properties.

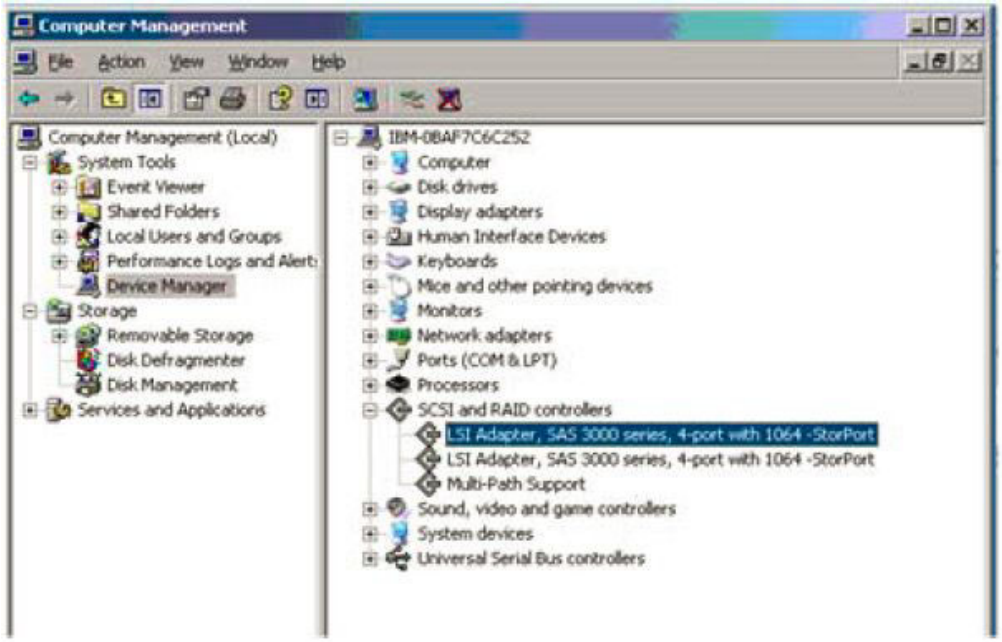


Figure 47. To verify the level right

9. In the properties screen select the Driver tab. The driver level should be listed as 1.29.3.0 as seen below.

Figure 48. Example of the Windows driver version

Note: This is an example of driver version 1.29.3.0 and may not reflect the most current version supported.

Updating the Firmware and BIOS on a SAS Expansion Card on x86-64 (Intel or AMD) Host Running Windows

This section describes how to update the firmware and BIOS for a SAS Expansion Card on x86-64 (Intel or AMD) host blade that is running the Windows operating system.

About this task

- Download the applicable BIOS and Firmware Update for the SAS Expansion Card (CFFv) for IBM BladeCenter exe file from the support and downloads website. It is recommended that you download the file to the host desktop for easy access.
- Follow the README instructions for installation contained on the support page.
- After installation you will be prompted to reboot the host. As the host reboots you will see the new BIOS and Firmware levels.

Important: If installing version 2.71, or later, and coming from an earlier version on an HS22 blade, refer to Appendix C, "Appendix C: Procedure for MPTSAS FW upgrade of HS12, HS21-XM, HS21, HS22, HS22V, HX5 and LS20 blades," on page 161

Note: The following versions listed are only examples, the current version available may be at a later version than shown.

Procedure

1. Download the applicable firmware file from the support and downloads website. It is recommended that you download it to the host desktop. Download the file from the following URL: http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020
   a. Select Product Family, then select 'Go'

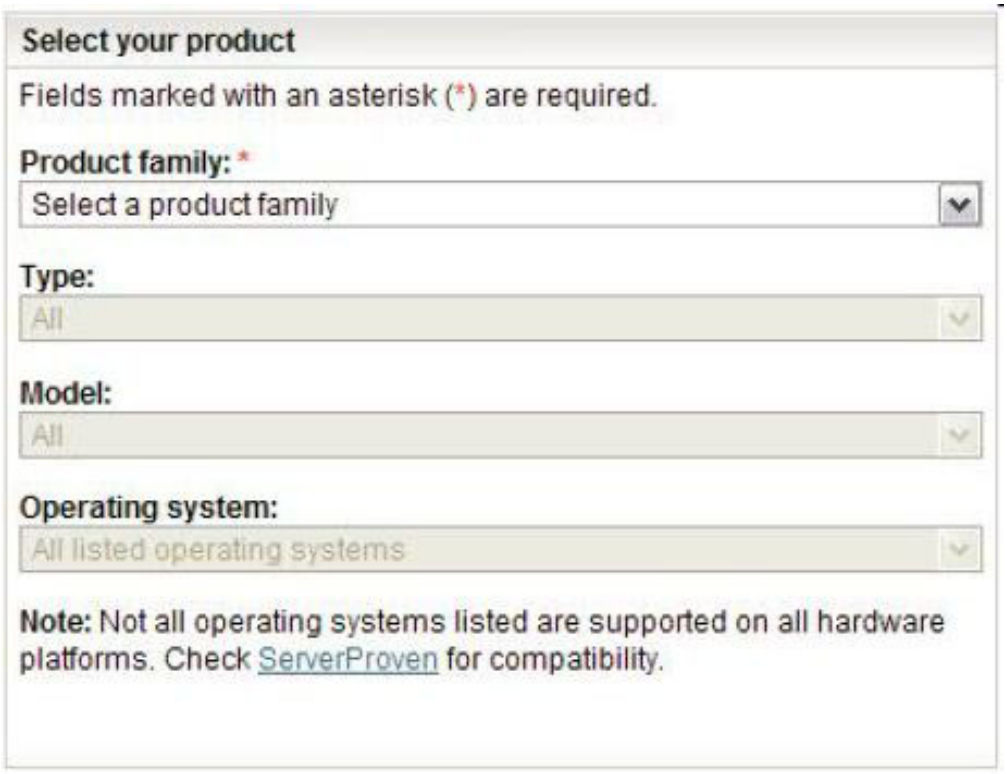


Figure 49. Example of Product Family Search

b. Select the SAS HBA card driver update listed.
c. Save the appropriate .zip file onto your laptop and extract (unzip) it.
d. After unzipping there will be three files enclosed.

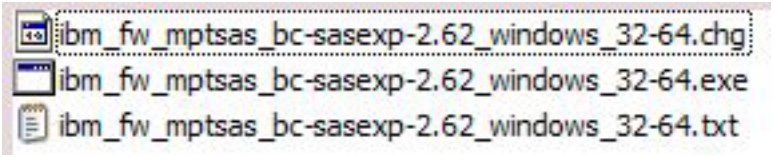


Figure 50. Enclosed three files

e. Copy the file ibm_fw_mptsas_bc-sasexp-2.62_windows_32-64.exe onto the desktop of the Windows blade desktop.

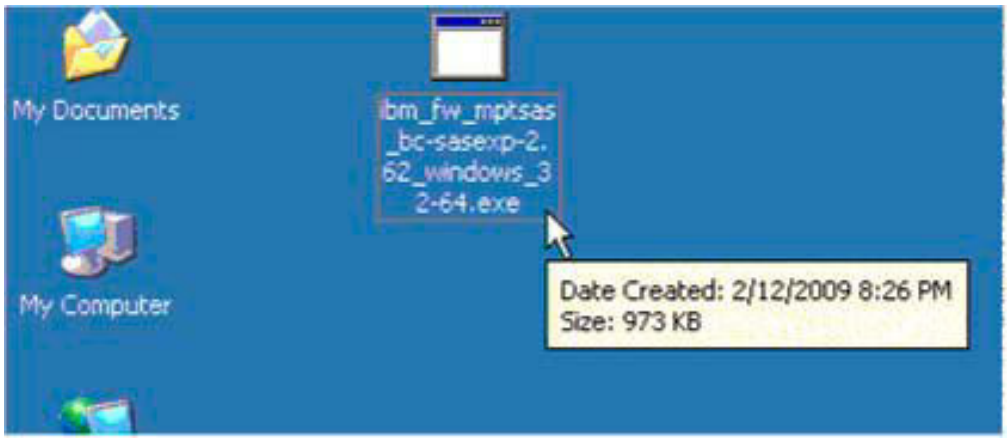


Figure 51. ibm_fw_mptsas_bc-sasexp-2.62_windows_32-64.exe

2. From the Windows blade desktop double click on the ibm_fw_mptsas_ bc-sasexp-2.62_windows_32-64.exe file to initiate the code load.
3. Select Perform Update and click on the Next button.

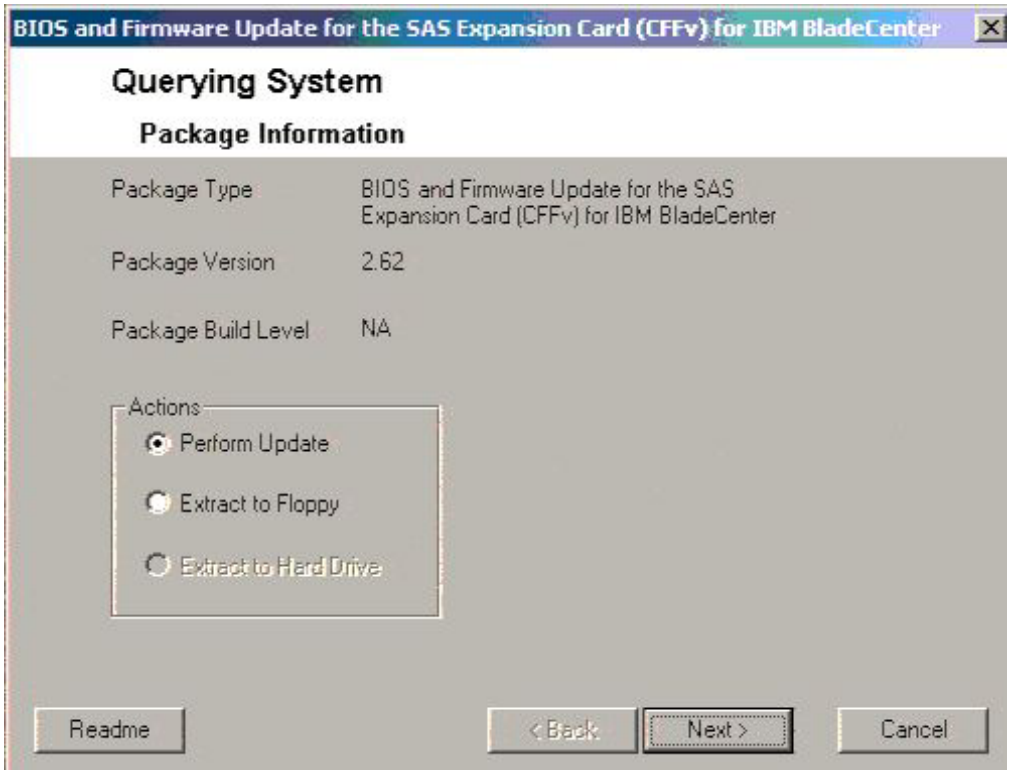


Figure 52. Select Perform Update

4. Click on the Update button.

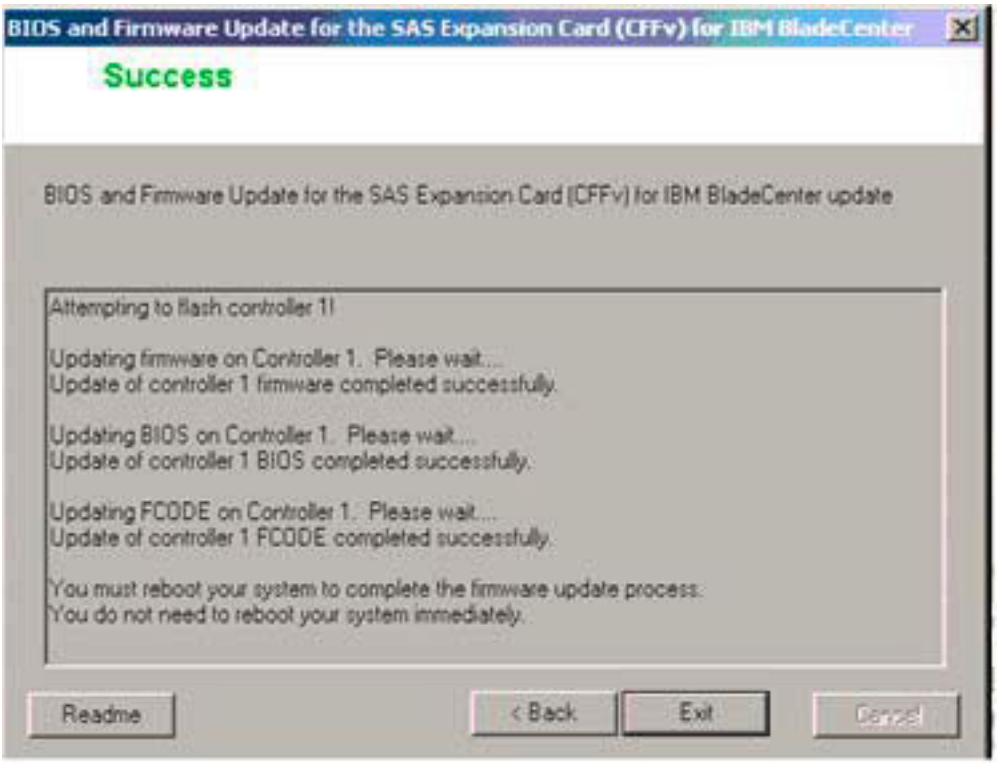


Figure 53. Example of screen output during firmware update

5. Click on the Exit button and reboot the blade.
6. As the host comes back up verify that it reflects the new level of SAS HBA firmware 1.27.82.00 as seen at the bottom of the screen shot below.

```
LSI Corporation MPT SAS BIOS
MPTBIOS-6.26.00.00 (2008.10.14)
Copyright 2000-2008 LSI Corporation.


Searching for devices at HBA 0...
SLOT ID  LUN VENDOR   PRODUCT          REVISION   INT13 SIZE \ NV
---- --- --- -------- ---------------- ---------- ----- ---------
  1          LSILogic SAS1064-IR       1.27.82.00  NV 2D:00

LSI Corporation MPT boot ROM, no supported devices found!
```

Figure 54. Example of BIOS version

Note: This is an example of BIOS version 6.26.00 and FW 1.27.82 and may not reflect the most current revision supported.

Configuring the SAS HBA Driver on x86-64 (Intel or AMD) Host Running Windows

The following section describes how to perform required changes to the SAS driver settings when using x86-64 (Intel or AMD) host running Windows.

Changing Queue Depth for Microsoft Windows

To edit the queue depth settings for host blades running the Microsoft Windows operating system, perform the following steps.

About this task

Note:

- The actual value used depending on the number of LUNs mapping to the host. See "Serial Attached SCSI host attachment" on page 12for more information on how to calculate the correct settings, and then back to this section.
- The SAS HBA driver level needs to be verified with different parameter and route settings for changing the queue depth. To verify the driver level, see "Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running Windows" on page 51 for more information. Check the Properties screen of "SCSI and RAID controllers" (or "Storage Controllers" in Windows Server 2008/2012) in Device manager. The driver level should be listed in the Driver tab.

Procedure

1. Start the registry editor command by entering the following command from the Windows command prompt.

   ```
   regedit
   ```

2. Save a backup copy of the current registry before making any changes, by selecting the highest level key and then selecting File -> Export.
3. Navigate to the following key:

   ```
   For driver of LSI_SAS,
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSI_SAS\Parameters\Device
   For driver of LSI_SAS2,
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSI_SAS2\Parameters\Device,
   ```

4. Right-click DriverParameter and select Modify from the menu.
5. Add the parameter of the SAS registry entry.
   a. LSI_SAS with driver version 1.33.01 (or later); LSI_SAS2 with driver version 2.00.29 (or later).

      Add **MaxSASQueueDepth=4** (default 64) after the last entry. Update the value if the entry already exists.

      The number is decided by the number of LUNs assigned to the host. Ex: MaxSASQueueDepth = 4 while setting 16 LUNs to the host.

   b. LSI_SAS with driver version prior to version 1.33.01; LSI_SAS2 with driver version prior to version 2.00.29.

      Add **MaximumTargetQueueDepth=4** after the last entry. Update the value if the entry already exists.

      Important: Make sure to update the value in the registry entry above. See "Serial Attached SCSI host attachment" on page 12 for more information on how to calculate the correct settings.

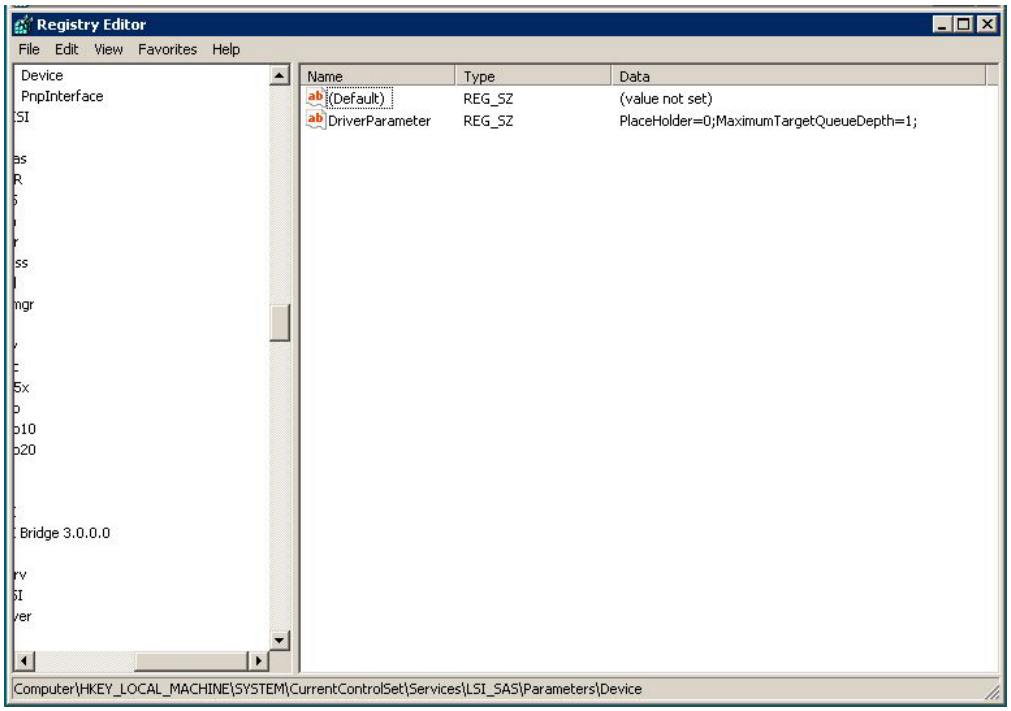


Figure 55. Example Registry Settings Screen for Windows

6. Save changes and exit the registry editor.
7. Reboot the host blade for the changes to be applied.

Configuring SDD DSM on x86-64 (Intel or AMD) Host Running Windows

This section describes how to configure SDD DSM on x86-64 (Intel or AMD) host blade that is running the Windows operating system.

Important:

- The previous version of SDD must be un-installed prior to installing the updated version. If there is no previous version of SDD, then skip the SDD uninstall instructions.
- If the host is SAS Booted and is operating with 2 SAS RAID Controller Modules, then one of the controllers will need to be turned off prior to uninstalling SDD. This can be accomplished by using the AMM to power off the controller or use SCM or the CLI to shutdown the controller to service mode. The system will failover and the remaining controller will go into SURVIVOR state.
- SDD DSM requires a minimum of Windows Server 2003 SP2
- There are Microsoft Hotfixes that must be installed on Windows Server 2003 and 2008 prior to installing SDD. Those Hotfixes are as follows:
  - For Windows Server 2003 with SP2
    - KB941276: A Windows Server 2003-based computer stops responding when the system is under a heavy load and when the Storport driver is used
      - http://support.microsoft.com/kb/941276
    - KB934739: The Plug and Play subsystem may not detect an external storage device when it is reconnected in Windows Server 2003
      - http://support.microsoft.com/kb/934739
  - For Windows Server 2008/2012 32 bit version only

- KB967349: Access to an MPIO-controlled storage device fails on a Windows Server 2008 based computer after you disconnect and then reconnect all data cables
  - http://support.microsoft.com/kb/967349

To uninstall the previous version of SDD

- If the host is SAS booted please see the important note above regarding the extra steps to take before uninstalling the SDD driver.
- To uninstall the existing SDD code, go to the Add/Remove Programs section of the host Control Panel. Select Subsystem Device Driver DSM and click on the Change/Remove option. After uninstalling the host will need to be rebooted.

To install the latest version of SDD

- Download the latest applicable version of SDD from the support and download website. It is recommended that you download the driver to the desktop for easy access.
- Follow the README instructions located on the web at the following URL

http://www.ibm.com/support/docview.wss?rs=540&context=ST52G7&dc=D430&uid=ssg1S4000350

- After driver installation the host will need to be rebooted

Note: If you are running a SAS booted host in a dual controller chassis you can turn on the controller that was previously turned off prior to the update after the host reboots. You may need to rescan the disks or reboot the host again after the second controller becomes bound to ensure all paths to the storage are restore.

- After the host has rebooted you can check the SDD version by entering the command prompt in the Subsystem Device Driver DSM programs list and typing the following:

```
datapath query version
```

Figure 56. Example of datapath query version command

Note: This is an example of SDDDSM version 2.4.2.1-2 and may not reflect the most current revision supported.

Configuration for SAS Booting on x86-64 (Intel or AMD) Host Running Windows

This section describes how to configure x86-64 (Intel or AMD) host blade that is running the Windows operating system for SAS booting.

Refer to Appendix B, "Appendix B: SAS Boot Pre-Operating System Installation Activities," on page 157, to validate that the system is ready to install a SAS booted operating system.

Operating system installation

Use the applicable procedures and instructions that are provided with the Windows operating system software to configure the operating system on the boot volume that is mapped to the blade server. It is not the intention of this document to show how to install the operating system or to select which software applications that will be installed or required for the initial installation of the operating system.

Depending on the operating system version, you might have to provide the SAS expansion card device driver during the installation so that the operating system can recognize the mapped boot volume from the IBM BladeCenter S SAS RAID Controller Module. Follow the appropriate instructions for your operating system to specify the use of a SAS adapter device driver that is not included in the operating system image.

Note: When installing the Windows operating system, knowledge of the recovery console using the installation CD and editing the boot entry on-the-fly will be useful. Incorrect modifications to enable multipath might result in failure to boot into the Windows image.

Post-Operating system installation activities

Perform the following steps to complete the installation of Microsoft Windows operating system on the IBM BladeCenter S SAS RAID Controller Module boot volume.

About this task

Important: After completing any section outside this section, return to this section of the document to complete any remaining steps.

Perform the following Steps:

Procedure

1. Update the SAS device driver as detailed in the section titled"Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running Windows" on page 51.
2. Update the host based settings as detailed in the section titled "Configuring the SAS HBA Driver on x86-64 (Intel or AMD) Host Running Windows" on page 61.
3. Install the System Storage Multipath Windows Subsystem Device Driver Device Specific Module (SDDDSM) as detailed in the section titled "Configuring SDD DSM on x86-64 (Intel or AMD) Host Running Windows" on page 62.

4. Use the SCM client or the CLI interface to map the boot volume to the second SAS port in the blade server. Create additional volumes and mapped them to both SAS ports.
5. Reboot the server. Log into the blade server and start the Subsystem Device Driver DSM command prompt window by selecting Start -> All Programs -> Subsystem Device Driver DSM -> Subsystem Device Driver DSM. When the "Select Subsystem Device Driver" command prompt window is displayed, type "datapath query adapter." You should see 2 paths & 2 active paths for each volume (LUN) that is mapped to the blade server. In the example below, a host, with 1 volume (LUN) mapped to both SAS ports, shows 2 paths of which all are active in the SDD command prompt window. The datapath query device and datapath query version can be used to provide more information on the paths per device and SDD DSM version.

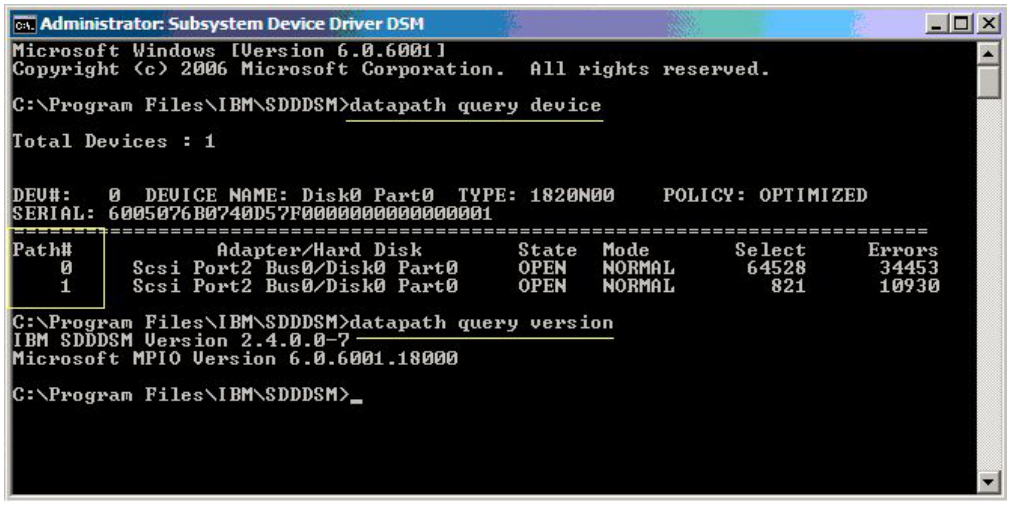


Figure 57. Subsystem device driver DSM command prompt window – datapath query device/version

6. In the Disk Drives folder of the Microsoft Device Manager window of the Microsoft Windows Server 2008/2012 hosts, there should be one 1820N00 Multi-Path for each of the volumes that are mapped to the blade server from the SAS RAID Controller Module. The Windows Server 2008/2012 Device Manager does NOT display the 1820N00 SCSI disk device entries. To review the 1820N00 SCSI disk device entries that the blade server see, use the Microsoft Windows registry editor and look at the content of the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\disk\ Enum key. There should be two 1820N00 SCSI disk devices entries for each volume that is mapped to the blade server (See An example of \HKLMACHINE \SYSTEM\CurrentControlSet\Services\disk\Enum key figure).

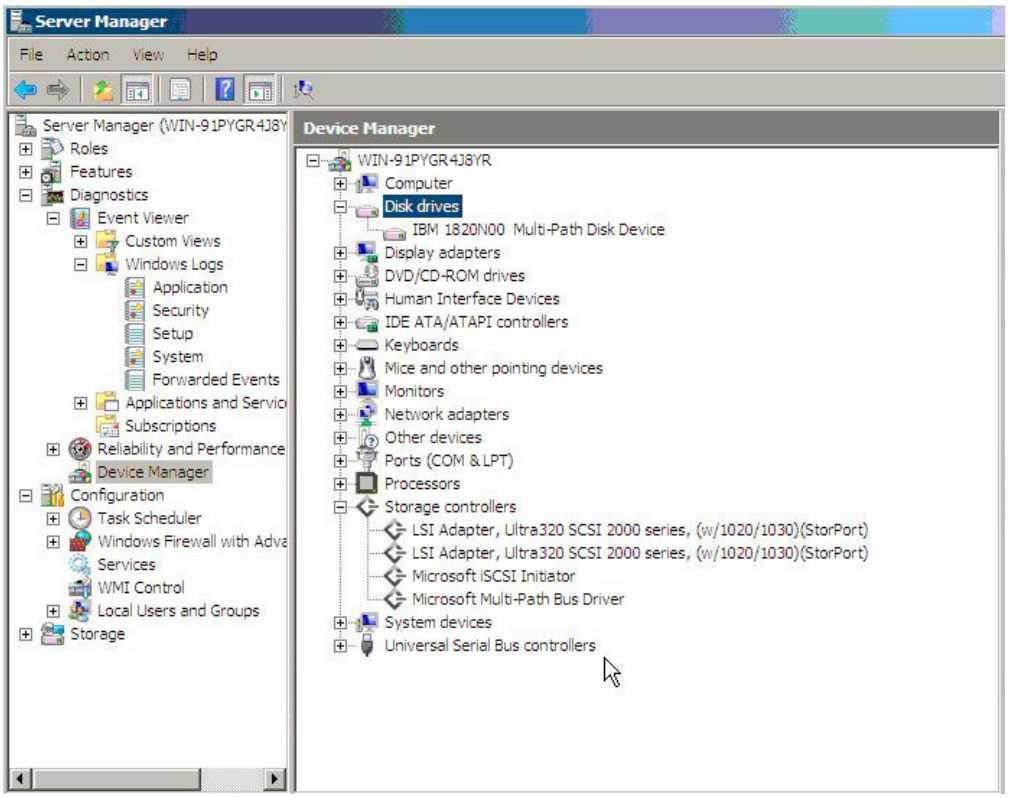


Figure 58. Computer Management window showing SAS RAID Controller Module volumes in Windows Server 2008/2012 hosts

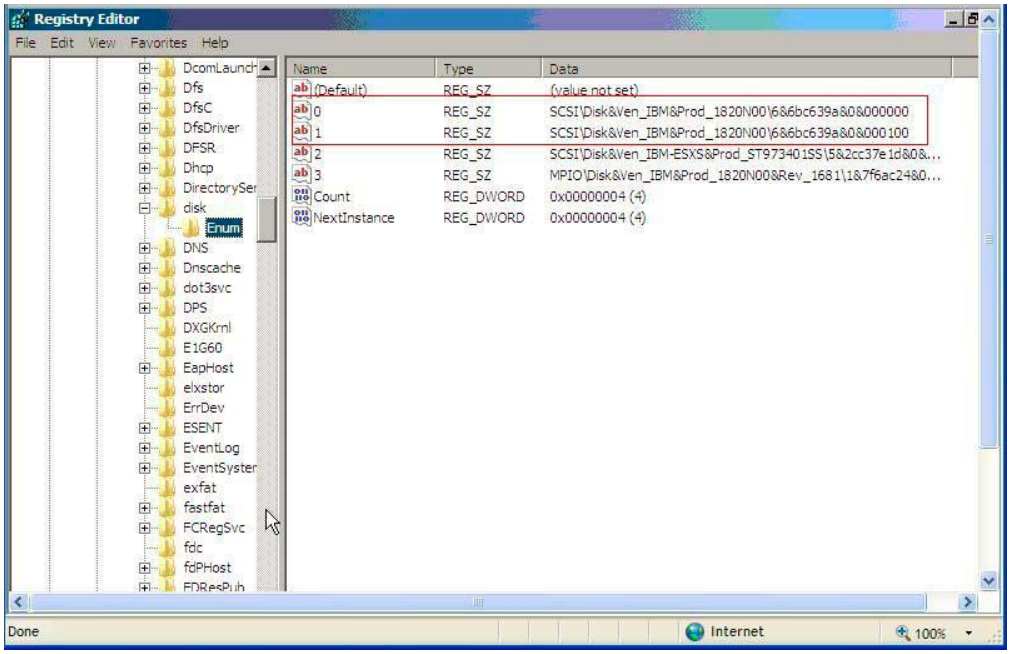


Figure 59. An example of \HKLMACHINE \SYSTEM\CurrentControlSet\Services\disk\Enum key

7. In the Disk Drives folder of the Microsoft Device Manager window of the Microsoft Windows Server 2003 hosts, there should be one 1820N00 Multi-Path

and two IBM 1820N00 SCSI disk device entries (one per volume path) for each of the volumes that is mapped to the blade server from the SAS RAID Controller Module.

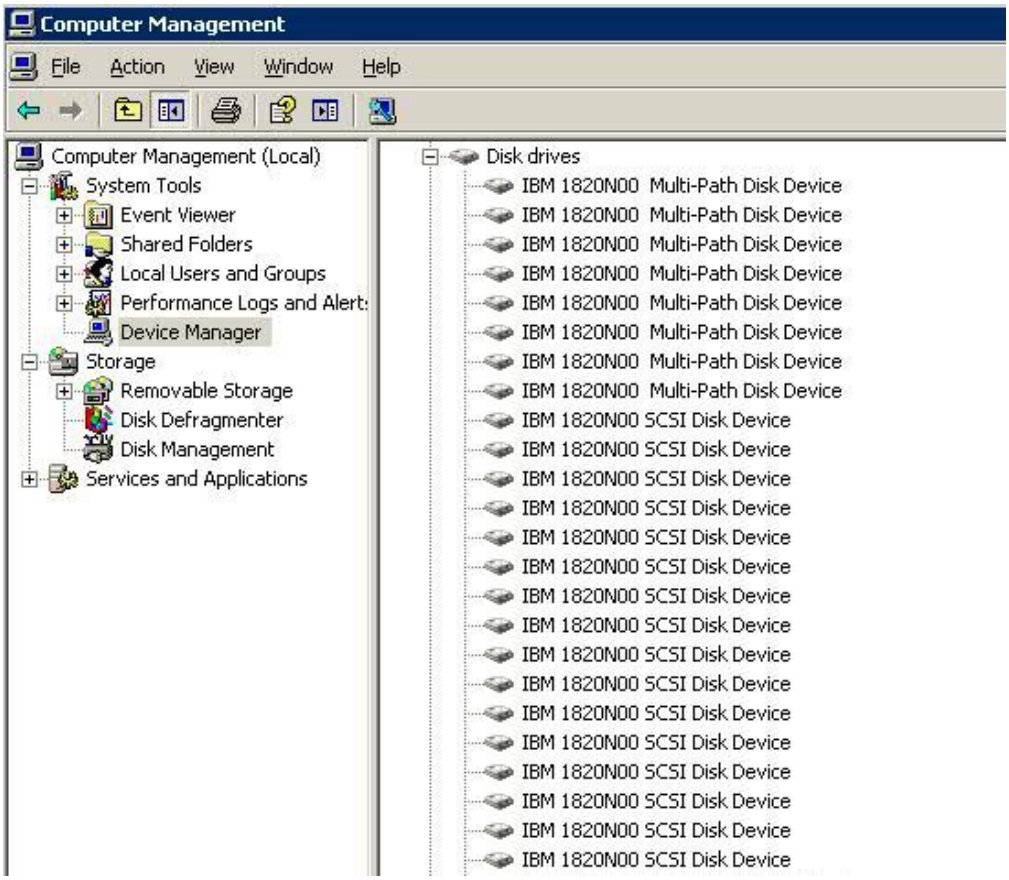


Figure 60. Computer Management window showing SAS RAID Controller Module volumes in Windows Server 2003 hosts

8. Install the latest Windows operating system updates and other hot-fixes as required.

System Configuration Settings for use with Microsoft Windows Clustering

This section describes the steps to configure the SAS Expansion Card (CFFv) for IBM BladeCenter and the SAS Connectivity Card (CIOv) for IBM BladeCenter to support blades that are configured for Microsoft Cluster Service. It also includes the settings changes for the Ethernet switch in the BladeCenter S chassis, and additional Windows host system settings.

Configuring SAS HBA BIOS Settings

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

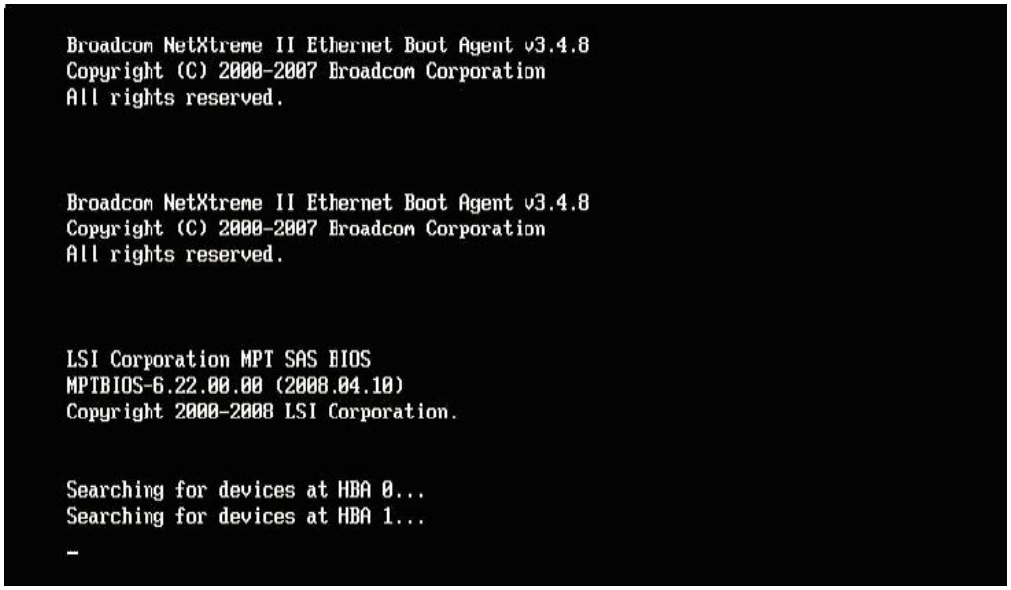


Figure 61. Example of a hung boot screen

Figure 44: Example of a hung boot screen

Important: For blades that have the SAS Expansion Card or a boot disk connected through the SAS Expansion Card, you must apply Microsoft Hotfix 886569 for Microsoft Cluster Service to be able to manage the storage volumes. You can download Microsoft Hotfix 886569 at http://support.microsoft.com/kb/886569. The steps you need to perform to configure the SAS Expansion Card and the Onboard SAS Controller BIOS depend on your boot disk type and external adapter type. Determine which steps you need to follow based on the boot option and the type of external SAS interface card you have installed:

- "Configuring blades with an internal boot disk and SAS Expansion Card" on page 69
- "Configuring blades with a boot disk connected through the SAS Expansion Card" on page 72
- "Configuring blades with the SAS Connectivity Card" on page 75

Configuring blades with an internal boot disk and SAS Expansion Card

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

Procedure

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

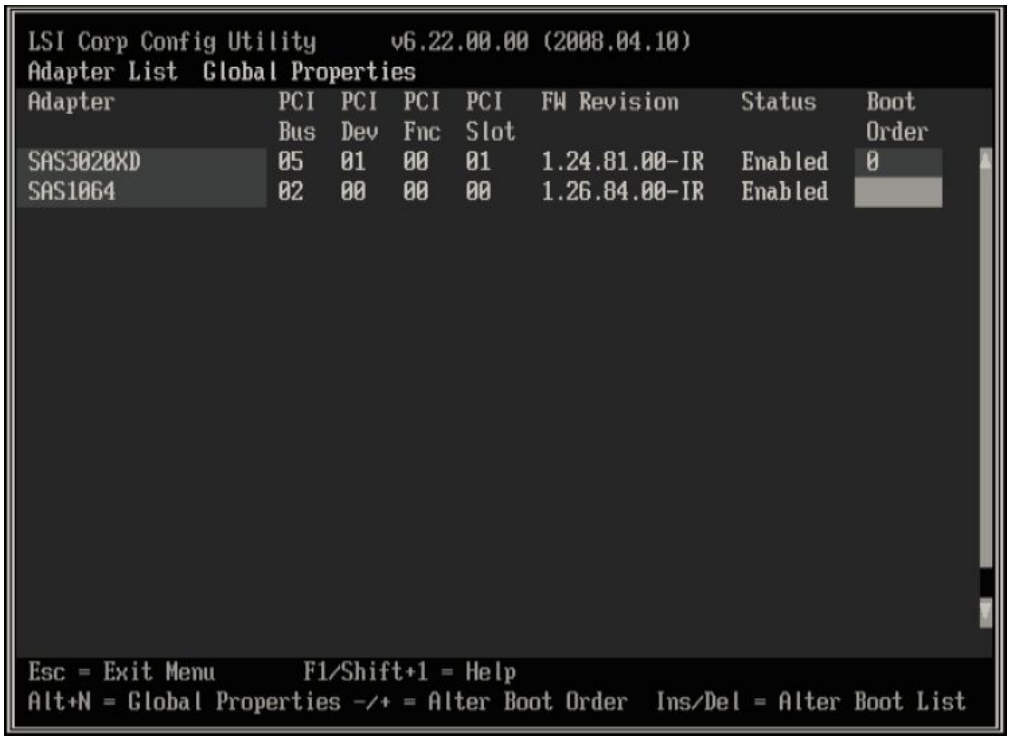


Figure 62. Adapter List screen showing Onboard SAS Controller and SAS Expansion Card

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

Figure 63. Disabling boot support for the SAS Expansion Card

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

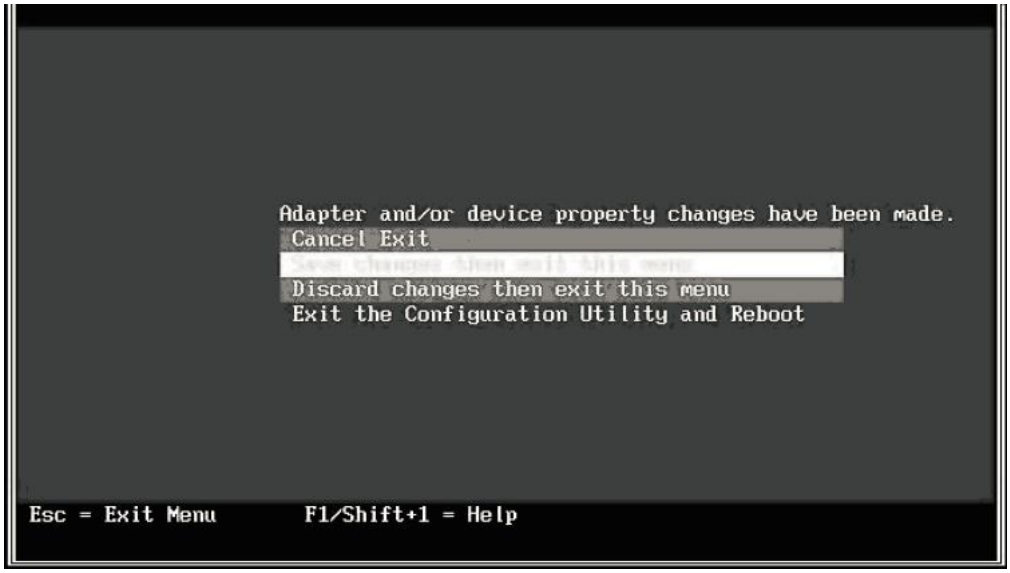


Figure 64. Saving configuration changes for the SAS Expansion Card

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

following figure shows the correct boot order.

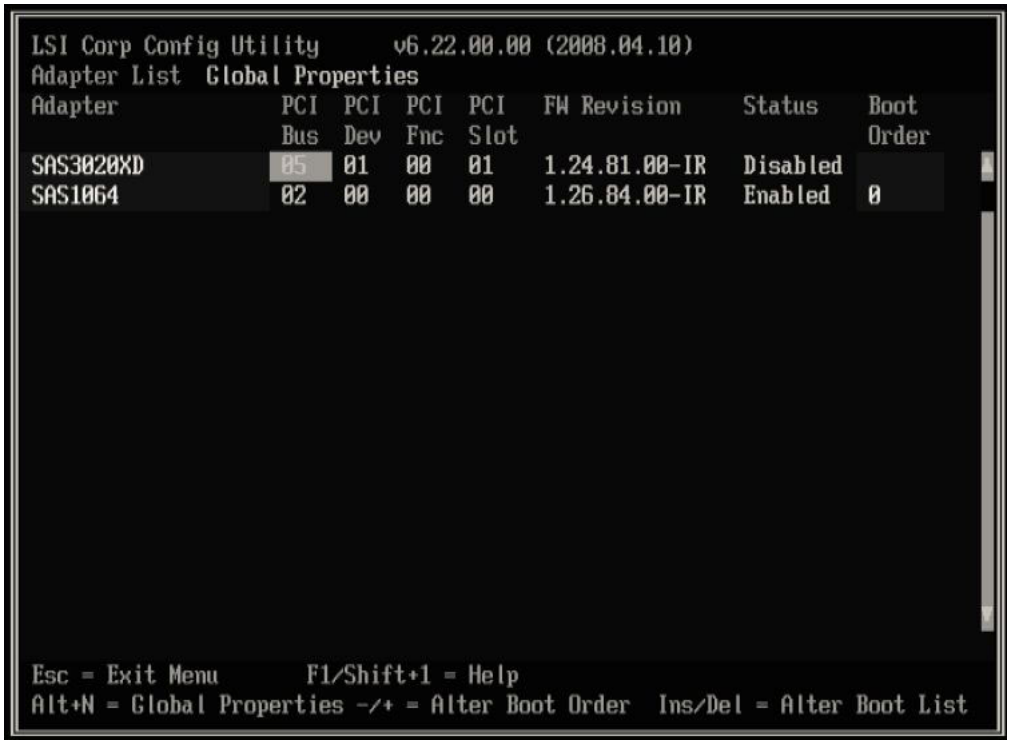


Figure 65. Setting boot order to 0 for Onboard SAS Controller

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

Figure 66. Saving the BIOS setting and rebooting

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

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

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

About this task

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

Procedure

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

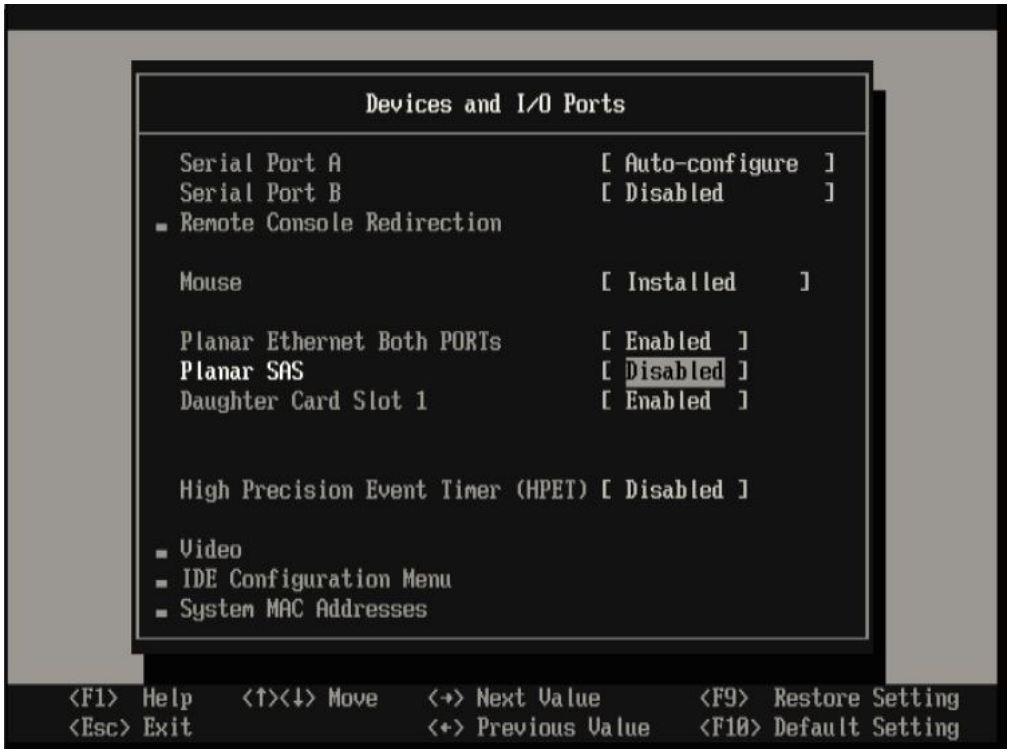


Figure 67. Devices and I/O Ports screen

2. Press Esc to exit the Devices and I/O Ports screen.
3. When the `<<<Press Ctrl-C to start LSI Logic Configuration Utility>>>` prompt displays during system boot, press Ctrl+C to enter the LSI Logic Configuration Utility. The Adapter List screen displays, similar to below figure. Adapter List screen showing SAS Expansion Card.

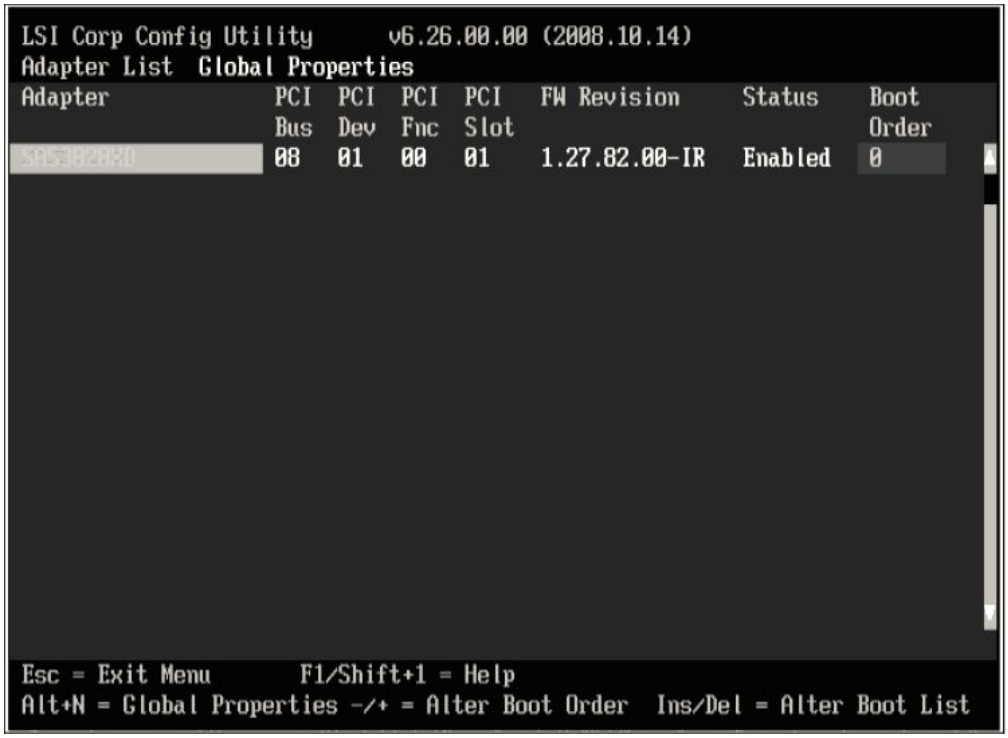


Figure 68. Adapter List screen showing SAS Expansion Card

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

Figure 69. Adapter Properties screen showing enabled BIOS and OS boot support

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

Figure 70. Advanced Adapter Properties screen

6. Use the arrow keys to select Advanced Device Properties, then press Enter. The Advanced Device Properties screen displays as shown in the following figure.

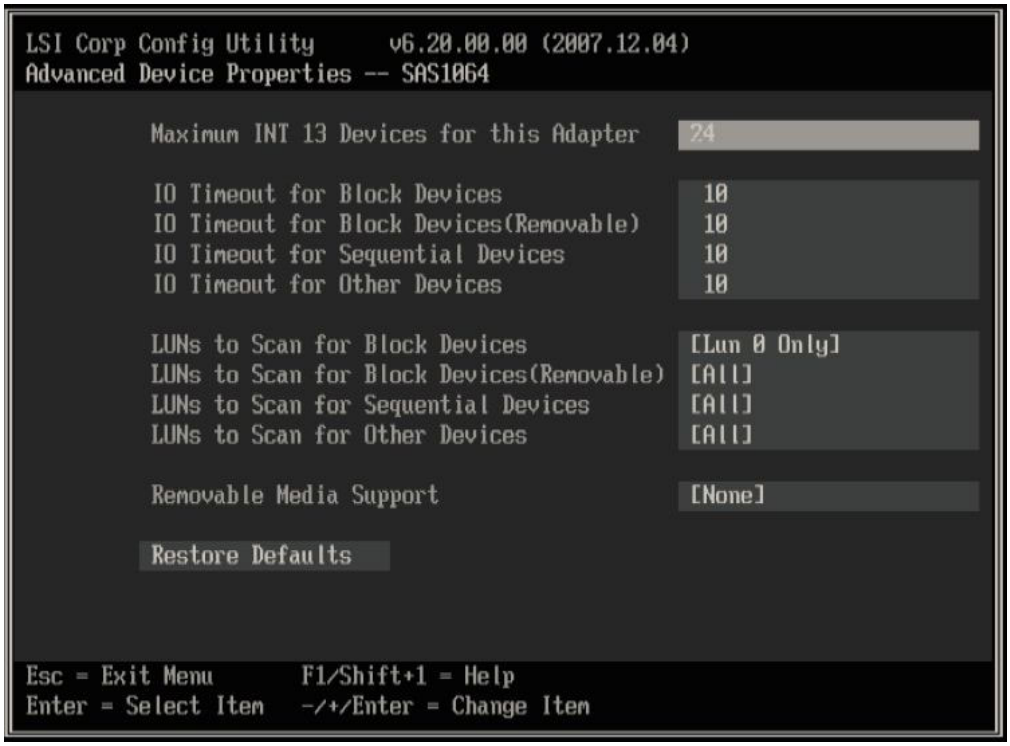


Figure 71. Advanced Device Properties screen

7. Use the arrow keys to navigate to **LUNs to Scan for Block Devices** and set it to **[Lun 0 Only]**.
8. Press Esc to exit the Adapter Properties screen until the utility asks you to save the configuration as shown in Figure: Saving configuration changes for the SAS Expansion Card. Use the arrow keys to `select Save changes then exit this menu`, then press Enter.
9. Press Esc to exit the Adapter List screen. Use the arrow keys to select `Exit the Configuration Utility and Reboot`, then press Enter.
10. Exit the BIOS as shown in Saving the BIOS setting and rebooting figure.

Configuring blades with the SAS Connectivity Card

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

About this task

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

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

Procedure

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

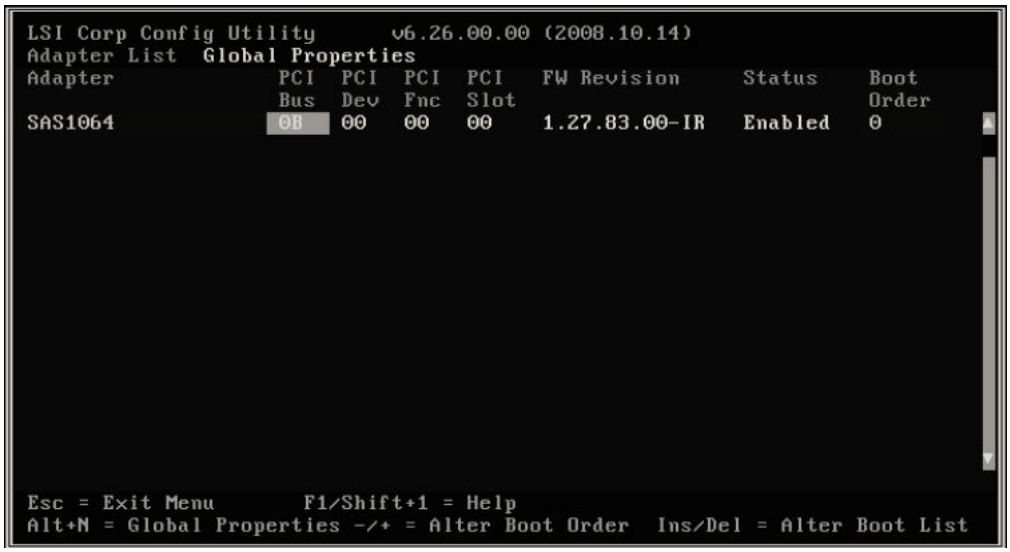


Figure 72. Adapter List screen showing the Onboard SAS Controller

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

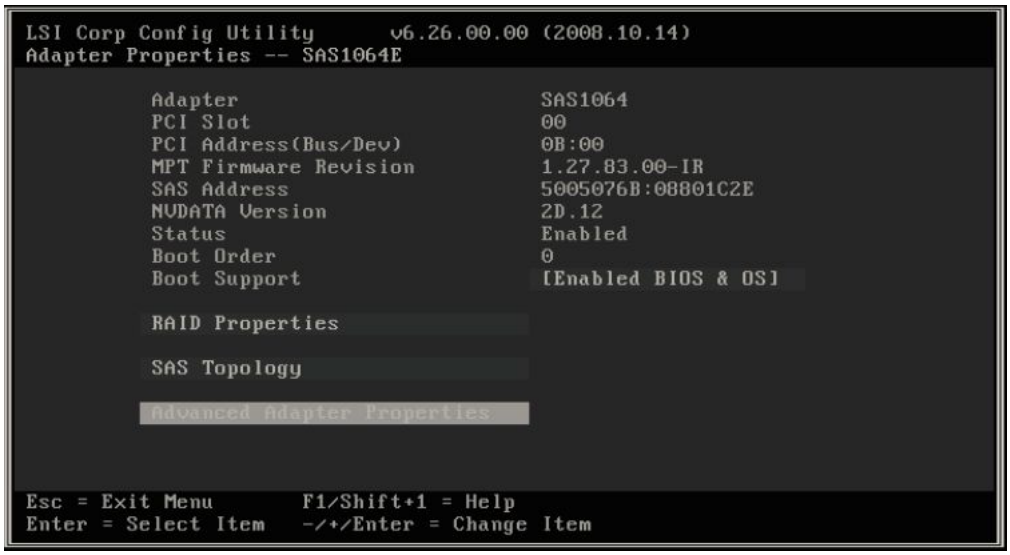


Figure 73. Adapter Properties screen for the Onboard SAS Controller

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

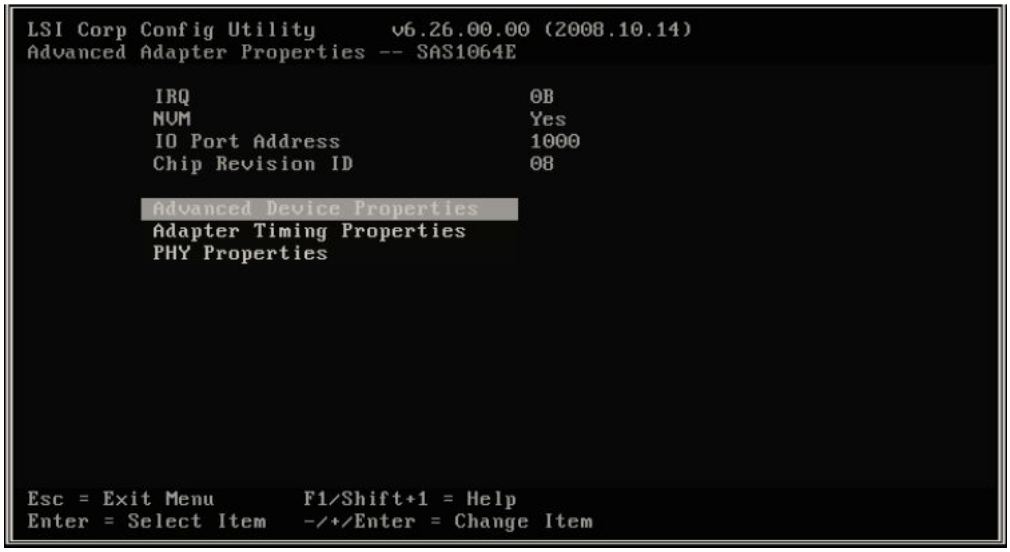


Figure 74. Advanced Adapter Properties screen

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

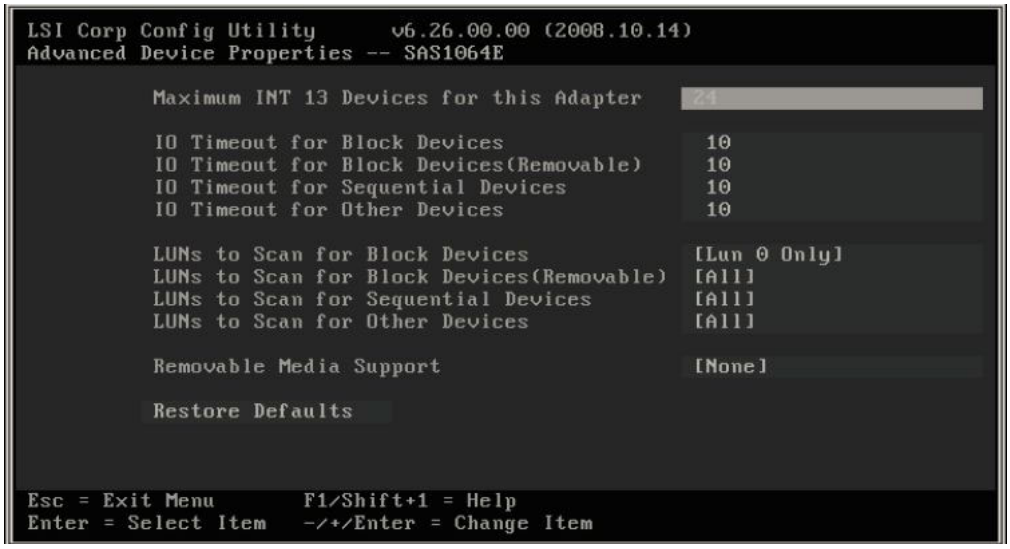


Figure 75. Advanced Device Properties screen

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

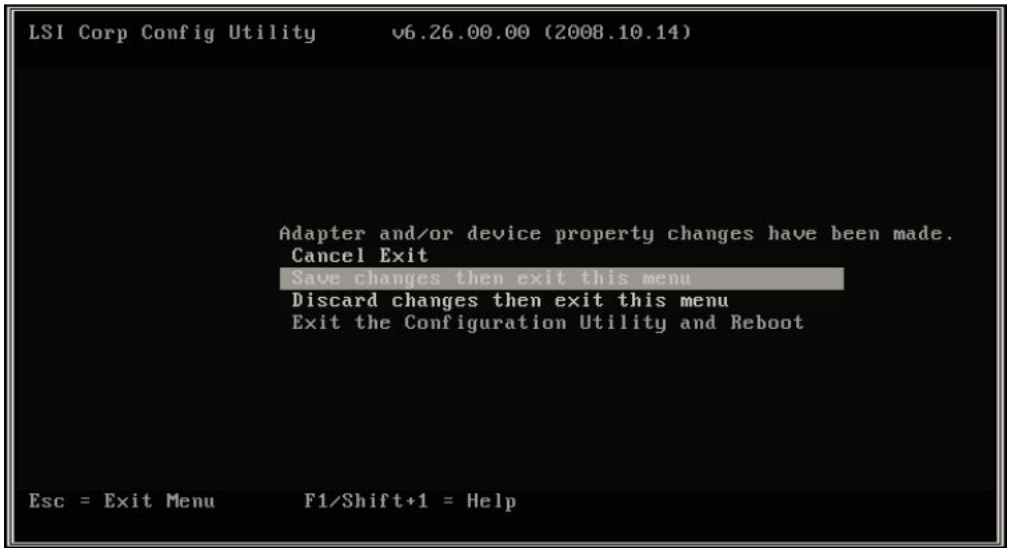


Figure 76. Saving configuration changes for the Onboard SAS Controller

8. Use the arrow keys to select Save changes then exit this menu, then press Enter. The Adapter List screen displays again.
9. Press Esc to exit the Adapter List screen. Use the arrow keys to select Exit the Configuration Utility and Reboot, then press Enter as shown in Saving the BIOS setting and rebooting figure.

Disabling IGMP snooping

Internet Group Management Protocol (IGMP) snooping is the process of listening to IGMP network traffic. In a cluster configuration, you should disable IGMP snooping to prevent node failover issues. Any Ethernet switch module that support this function, should verify that the function is disabled. Perform the following steps to disable IGMP snooping.

Note: The following example uses the Server Connectivity Module for IBM BladeCenter (39Y9324). Other Ethernet switch modules that support this feature may require a separate procedure. Refer to the Ethernet switch module configuration documentation for specific procedures.

Disabling IGMP snooping through Telnet

This section demonstrates how to disable IGMP snooping through Telnet.

Procedure

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

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

   b. Enter the username and password.

- The default username is: USERID
- The default password is: PASSW0RD (the sixth position is the numeral zero)

c. When prompted for the **Inactive session timeout value**, select **no timeout**.

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

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

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

8. Press d to disable IGMP snooping.

Disabling IGMP snooping through a web session

This section demonstrates how to disable IGMP snooping through a web session.

Procedure

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

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

   b. Enter the username and password.
      - The default username is: USERID
      - The default password is: PASSW0RD (the sixth position is the numeral zero)

   c. When prompted for the I**nactive session timeout value**, select **no timeout**.

      Note: Remember to log out when you have completed your session. If you do not log out, the system shows an error the next time you try to log in.
2. From the I/O Module Tasks Configuration menu, select the Ethernet module from the Advanced Management Module and select Advanced Configuration.
3. Select Start Web Session.
4. From the navigation panel, select Miscellaneous settings → Uplink/Group.
5. For IGMP settings, select Disable from the list of options.

Private Network Setup

When creating your cluster environment, it is required to have at least two networks, a public network and private network. Cluster validation may still pass with only a public network enabled. However, one may encounter problems with live migration.

To set up the private network, enable the second network adapter on your blade/node. Go to **Properties** for this adapter and click on **Internet Protocol (TCP/IP)** and then click on the **Properties** button. Create a static IP address and subnet for the node that is a different range than the public network, for example a 10.x.x.x and 255.0.0.0. Repeat for all nodes in your cluster.

Modification of Windows Performance settings

The following section describes how to modify the Windows drive performance settings to obtain the optimal performance when using the SAS RAID Controller Module.

Many RAID controllers implement write caching and ignore the settings in the OS. The IBM BladeCenter S SAS RAID Controller Module honors the selections within the OS and applies those settings to the drive arrays. The SAS RAID Controller Module depends upon proper OS configuration to enable/disable performance and write caching.

How to make the policy changes

This section describes how to make the policy changes.

Procedure

1. Right-click on My Computer.
2. Choose "Manage".
3. Click on "Disk Management".
4. Right-click "Disk X".
5. Select Properties.

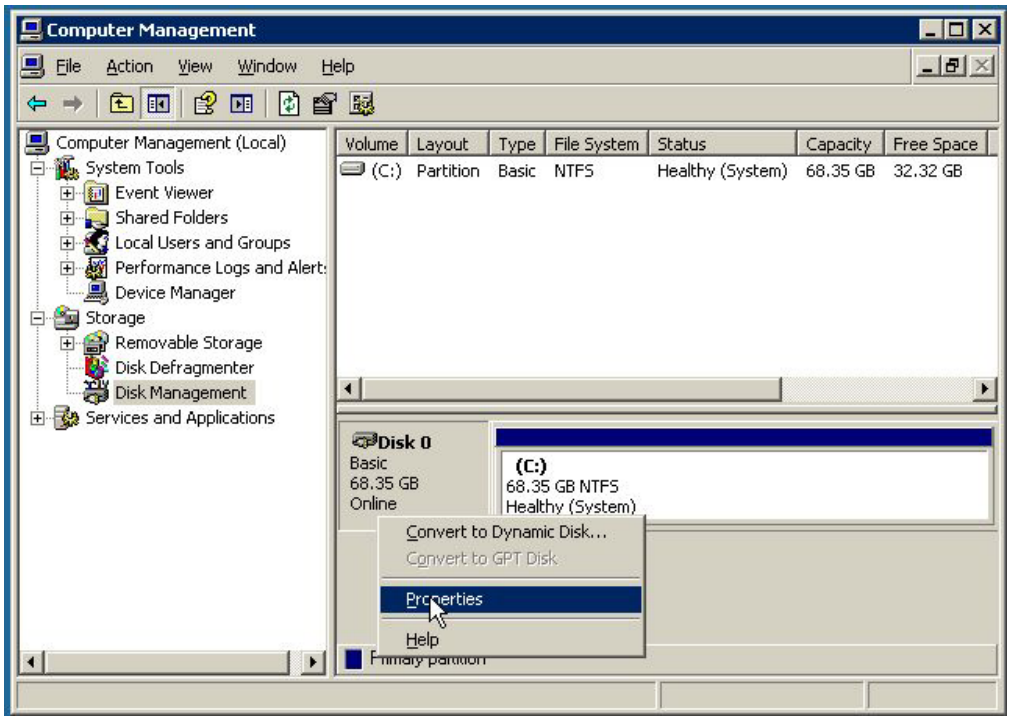


Figure 77. Computer Management / Disk Management Window

6. Click on the Policies Tab.
7. For Windows Server 2003, make sure the following boxes are checked.
   a. Enable write caching on the disk.
   b. Enable advanced performance.

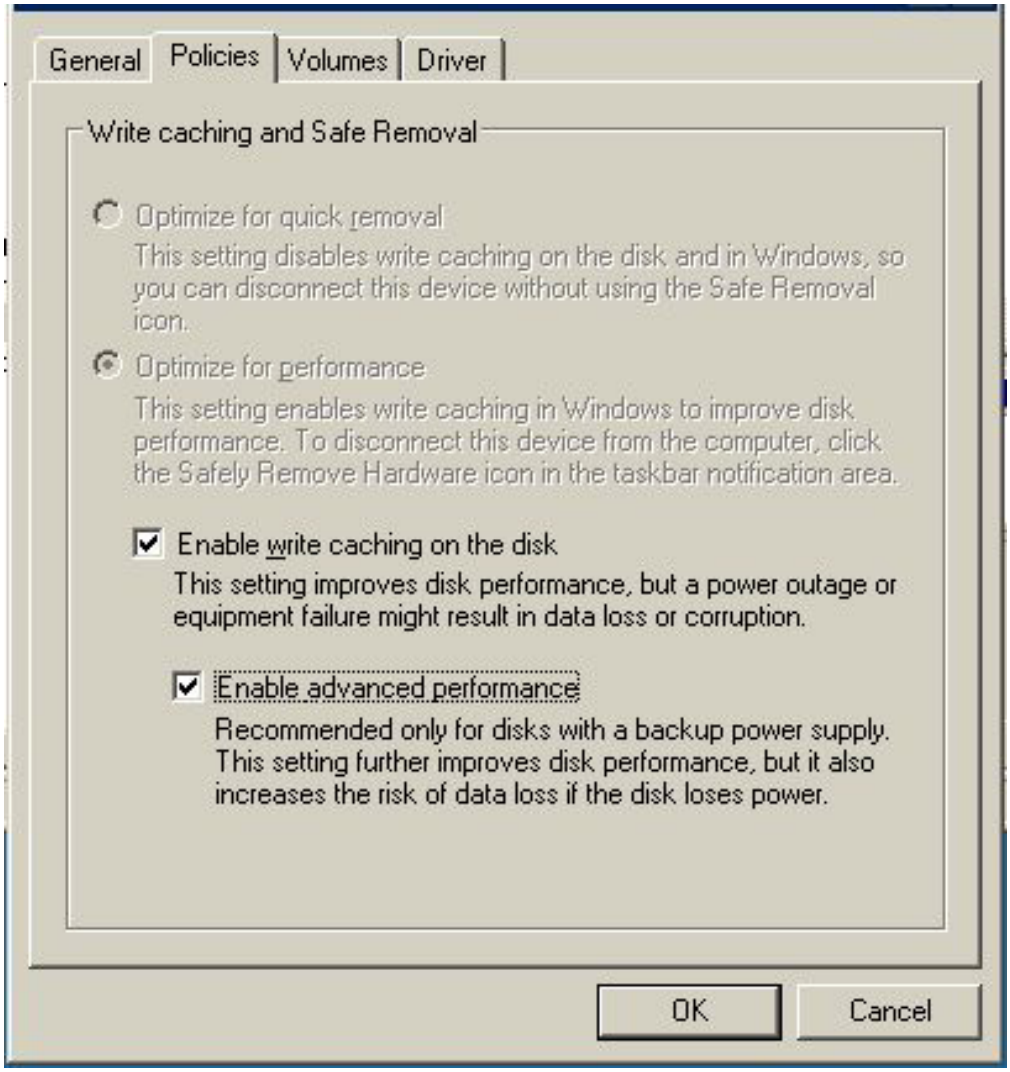


Figure 78. Windows Server 2003 Policy window with correct settings

c. Select OK to apply the settings.

8. For Windows Server 2008/2012, make sure the following boxes are checked.
   a. Enable write caching on the device.
   b. Select "Turn off Windows write-cache buffer flushing on the device".

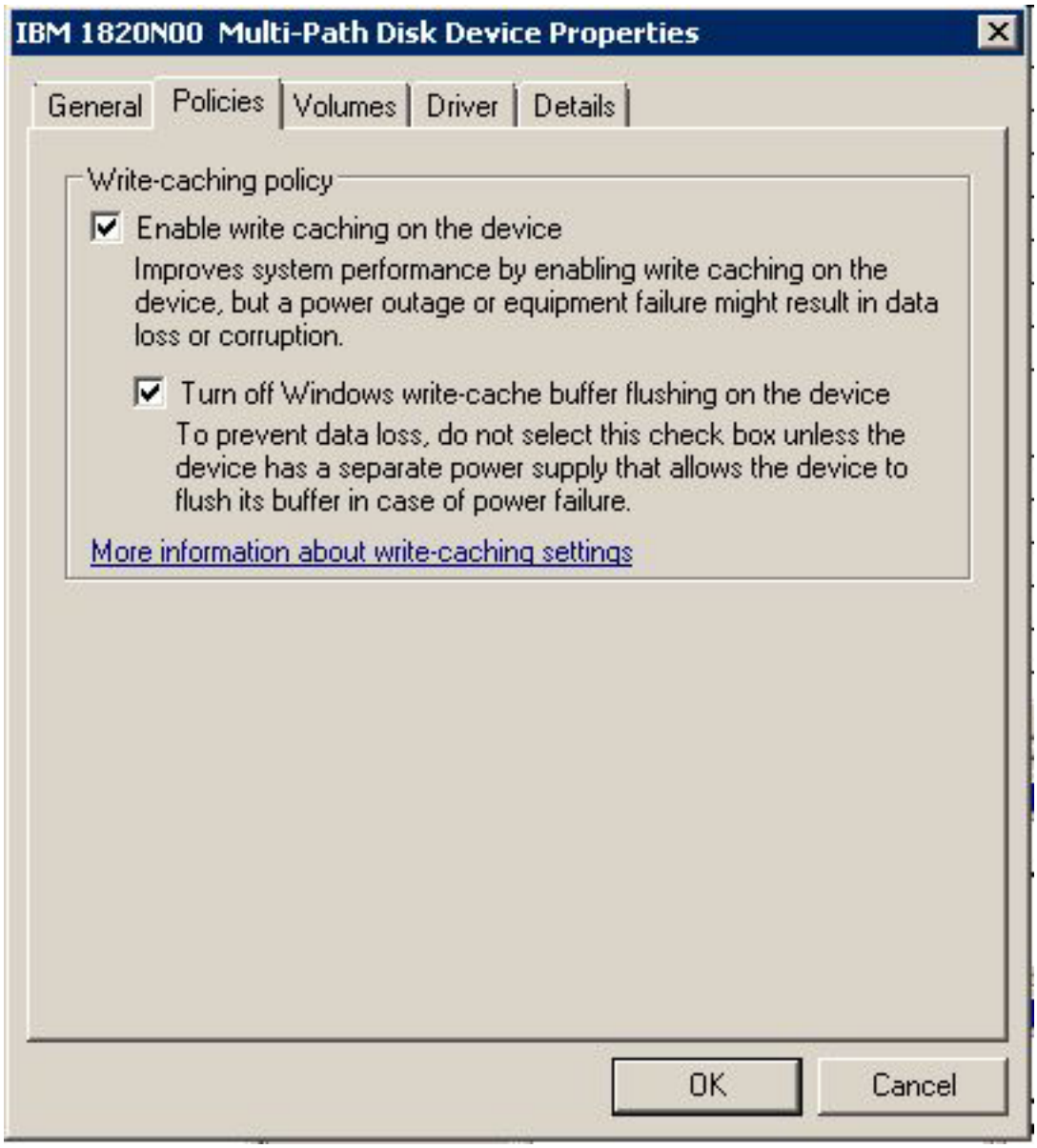


Figure 79. Windows Server 2008/2012 Policy window with correct settings

c. Select OK to apply the settings.

9. Repeat step 4 – 8 for each mapped drive.

Chapter 4. Chapter 4 x86-64 (Intel or AMD) blades running VMware Host Attachment

This chapter describes how you attach an Intel or Advanced Micro Devices (AMD) host blade running the VMware operating system to an IBM BladeCenter S SAS RAID Controller Module using SAS adapters.

Note: VMware maintains a Hardware Compatibility List which is available at:

http://www.vmware.com/resources/compatibility/search.php

This chapter contains the following sections:

Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running VMware

The SAS HBA driver comes packaged in the ESX Server distribution CDs and they are installed as part of the ESX Server installation process. However, if a newer driver is released, below are the steps to install.

- Steps to install driver (rpm patch)
  1. Install the driver rpm using the option "rpm -Uhv --force"
  2. Run "esxcfg-boot -b"
  3. Reboot the system
  4. Check the driver version loaded by issuing command

     `cat /proc/mpt/version"`
- Installing async drivers on ESXi 4.x and ESX 4.x
  1. Please refer to VMware Knowledge Base article 1032936 for instructions

     http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1032936
  2. After the update finished, please refer to VMware Knowledge Base article 1027206 to check the driver version

     http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027206
- Installing async drivers on ESXi 5.x
  1. Please refer to VMware Knowledge Base article 2005205 for instructions

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2005205

2. After the update finished, please refer to VMware Knowledge Base article 1027206 to check the driver version

   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027206

Updating the FW/BIOS on a SAS Expansion Card on x86-64 (Intel or AMD) Host Running VMware

This section describes how to update the firmware and BIOS on the SAS Expansion Card on x86-64 (Intel or AMD) host running VMware. A floppy disk drive or a floppy disk image mounted using the AMM Remote Control will be required to perform these steps.

About this task

Important: If installing version 2.71, or later, and coming from an earlier version on an HS22 blade, refer to Appendix C: Procedure for MPTSAS FW upgrade of HS12, HS21-XM, HS21, HS22, HS22V, HX5 and LS20 blades.

Note: The following versions listed are only examples; the current version available may be at a later version than shown.

Procedure

1. Download the applicable firmware file from the support and downloads website. It is recommended that you download it to the host desktop. Download the file from the following URL

   http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020

   Select Product Family, then select 'Go'

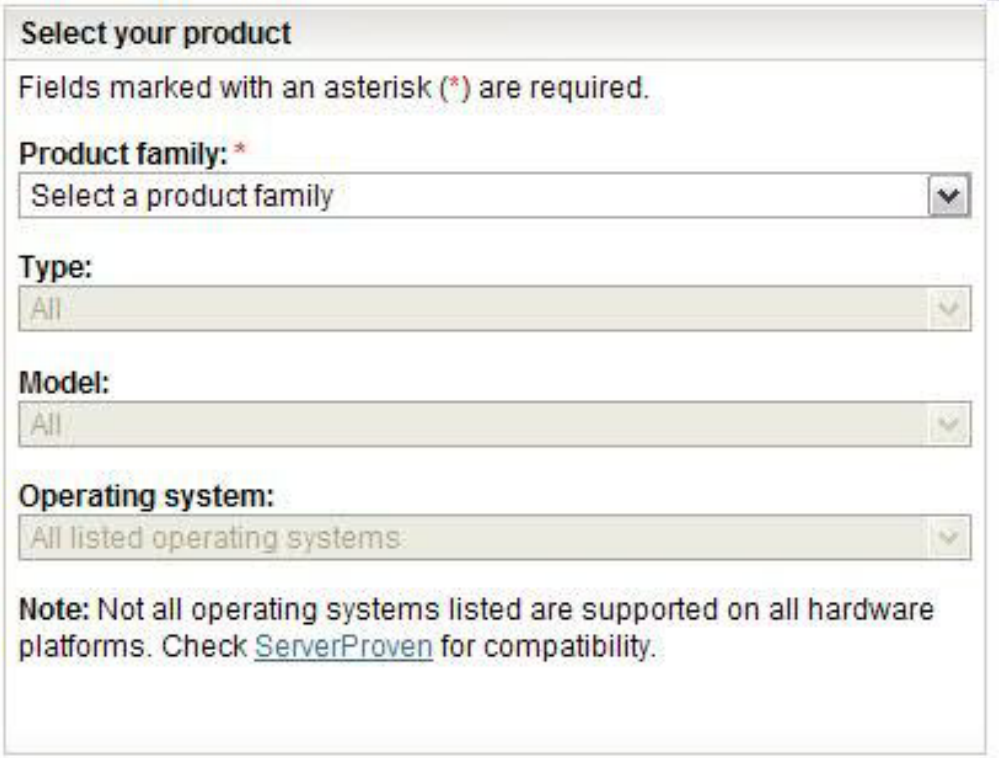


Figure 80. Example of Product Family Search

Select the SAS HBA firmware update.

2. Copy the image to a floppy disk or make the image available for remote mounting using the media tray on the AMM.
3. Assign the media tray to the host blade. If using a floppy drive, connect it to the media tray.
4. Reboot the host blade server.
5. When the blade boots, make sure the blade boots from the floppy disk with the firmware update image. The following screen captures are examples of what should be seen during the floppy disk boot and firmware update.

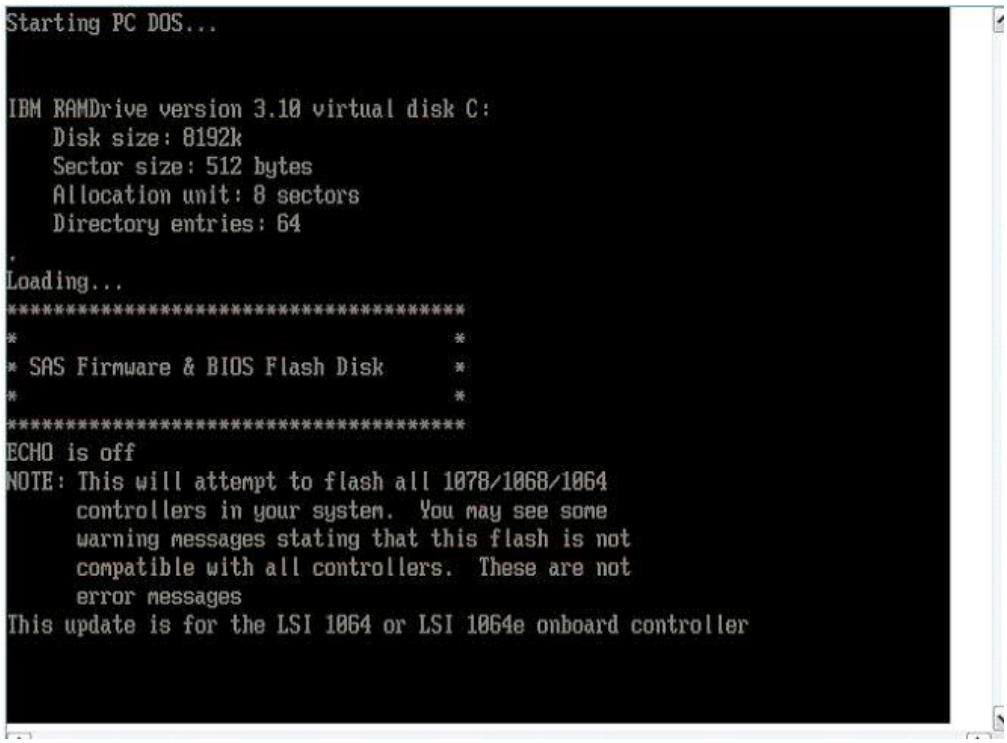


Figure 81. Example of SAS HBA firmware floppy disk boot

6. Once the update is complete disconnect the floppy drive and reboot the server.

Figure 82. Example of SAS HBA BIOS version

Note: This is an example of BIOS version 6.26.00 and FW 1.27.82 and may not reflect the most current revision supported.

Configuring Host System Settings on x86-64 (Intel or AMD) Host Running VMware

The following section describes how to perform required changes to the SAS driver settings when using x86-64 (Intel or AMD) host running VMware.

Changing Queue Depth for VMware

To edit the queue depth settings for host blades running VMware, perform the following steps.

About this task

Note:

- Ensure the following steps are performed to correctly configure VMWare for use with the IBM SAS RAID Controller Module.
- For ESXi 5.x and ESX/ESXi 4.x, Queue depth is based on number of LUNS mapped, so in the above case this would assume 8 LUNs mapped. For a total of no more than 64 outstanding commands at one time on the HBA.
- Additional system tuning may be required to reach an optimal configuration of the system. It is recommended that customer wishing to further tune their system contact IBM technical services for additional tuning options and customization.
- For BladeCenter HS23/HS23E with inbox LSI mpt2sas driver: when executing below commands, please change the module name and the associated parameters from mptsas to mpt2sas.

ESXi 5.x

1. Execute esxcli system module parameters list to get module names.
2. For mptsas driver, execute:

   esxcli system module parameters set -p mpt_sdev_queue_depth=8 -m mptsas

   For mpt2sas driver, execute:

   esxcli system module parameters set -p mpt2sas_sas_queue_depth=8 -m mpt2sas
3. Reboot the host blade to take the change effect
4. For mptsas driver, execute:.

   esxcli system module parameters list -m mptsas to verify the change

   For mpt2sas driver, execute:

   esxcli system module parameters list -m mpt2sas to verify the change
5. For setting of the dynamic queue configuration issue the following commands:

   esxcfg-advcfg -g /Disk/SchedNumReqOutstanding

   esxcfg-advcfg -g /Disk/QFullThreshold

   esxcfg-advcfg -g /Disk/QFullSampleSize

   esxcfg-advcfg -g /Disk/DelayOnBusy

   The recommended values for these settings are as follows:

   SchedNumReqOutstanding, set to the queue depth setting from above

   QFullThreshold, set to the queue depth setting from above

   QFullSampleSize, set to 64

   DelayOnBusy, set to 2000

Use the command esxcfg-advcfg -s <value> <parameter> to change these settings. These settings are changed dynamically, and do not require a server reboot.

Note:

- If the queue depth is not set correctly or the system is overly busy due to the IO load, there may be a BUSY response returned for commands. This status will appear in the vmkernel log like the following:

  ```
  "vmhba0:C0:T1:L0" H:0x0 D:0x8 P:0x0 Possible sense data: 0x0 0x0 0x0
  ```

ESX/ESXi 4.x

1. Execute esxcfg-module –l to get module names (should be mptsas)
2. Execute esxcfg-module –s “mpt_sdev_queue_depth=8 mpt_disable_hotplug_remove=1” mptsas
3. Execute esxcfg-module -g mptsas to confirm that the settings have been applied
4. Execute esxcfg-boot –b to make sure the parameters are setup for boot

   Note: In ESXi 4.x, there is no need with this command esxcfg-boot –b as it is included in the standard shutdown procedure to get the initrd recreated automatically.
5. Reboot the host blade to make for the above settings to take effect.
6. For setting of the dynamic queue configuration issue the following commands:

   esxcfg-advcfg -g /Disk/SchedNumReqOutstanding

   esxcfg-advcfg -g /Disk/QFullThreshold

   esxcfg-advcfg -g /Disk/QFullSampleSize

   esxcfg-advcfg -g /Disk/DelayOnBusy

   The recommended values for these settings are as follows:

   SchedNumReqOutstanding, set to the queue depth setting from above

   QFullThreshold, set to the queue depth setting from above

   QFullSampleSize, set to 64

   DelayOnBusy, set to 2000

   Use the command esxcfg-advcfg -s <value><parameter> to change these settings. These settings are changed dynamically, and do not require a server reboot.

   Note: If the queue depth is not set correctly or the system is overly busy due to the IO load, there may be a BUSY response returned for commands. This status will appear in the vmkernel log like the following:

   ```
   "vmhba0:C0:T1:L0" H:0x0 D:0x8 P:0x0 Possible sense data: 0x0 0x0 0x0
   ```
7. In the ESX(I) GUI, the above for setting may also be set by going to Configuration-> Software->Advanced Settings-> Disk, as shown in Figure 67 below:

   Disk shares, may also be used for tuning the system, however, they are not discussed here and customers are recommended to contact IBM/VMWare support to discuss options regarding using this tuning feature.

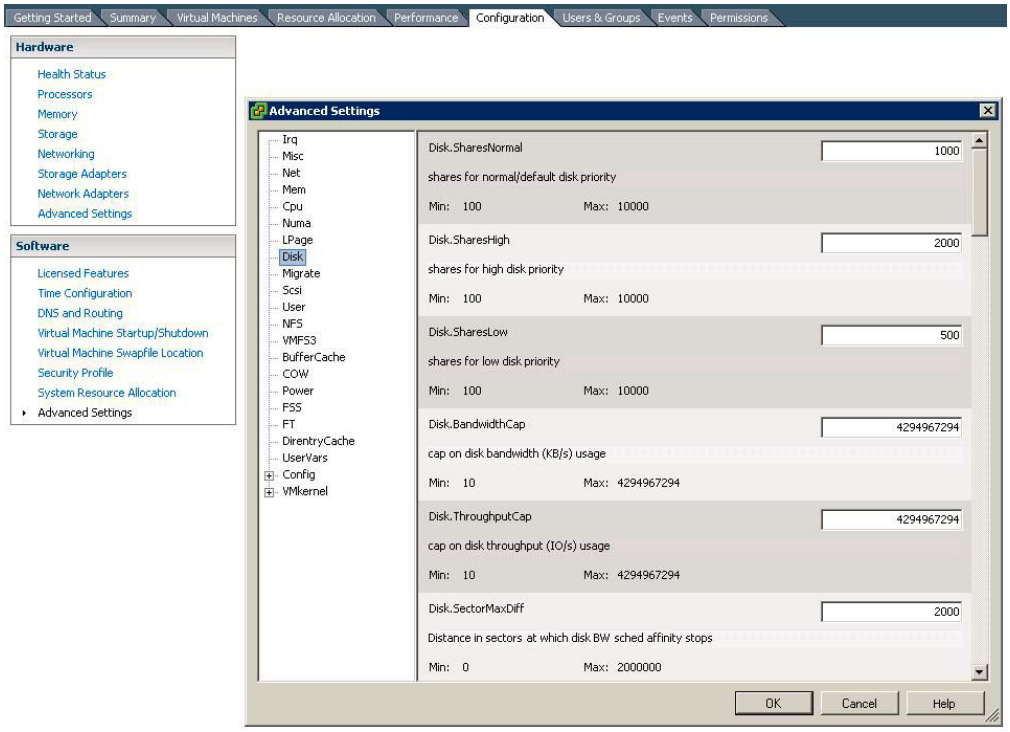


Figure 83. Dynamic queue setting in ESXi graphical user interface

ESX 3.5

Note:

For VMware, the queue depth setting is HBA, not LUN based, which differs from the other supported operating systems. Refer to the section, “Serial Attached SCSI host attachment” on page 12for further information.

1. Execute esxcfg-module –l to get module names module name (should be mptscsi_2xx)
2. Execute esxcfg-module –s “mpt_can_queue=63” mptscsi_2xx
3. Execute esxcfg-boot –b
4. Reboot the host blade
5. Execute esxcfg-module -g mptscsi_2xx to verify the change

   Note: If the queue depth is not set correctly or the system is overly busy due to the IO load, there may be a BUSY response returned for commands. This status will appear in the vmkernel log like the following:

   ```
   vmhba2:0:2:0 status = 8/0 0x0 0x0 0x0
   ```

Specific Instructions for VMware ESX/ESXi 5.1

About this task

For users running VMware ESX/ESXi 5.1 on their host blades, the following instructions are required.

Procedure

1. Execute `esxcli system settings advanced list`.
2. Verify that the current value of `/ UserVars/ CIMvmw_lsiproviderProviderEnabled` is 1

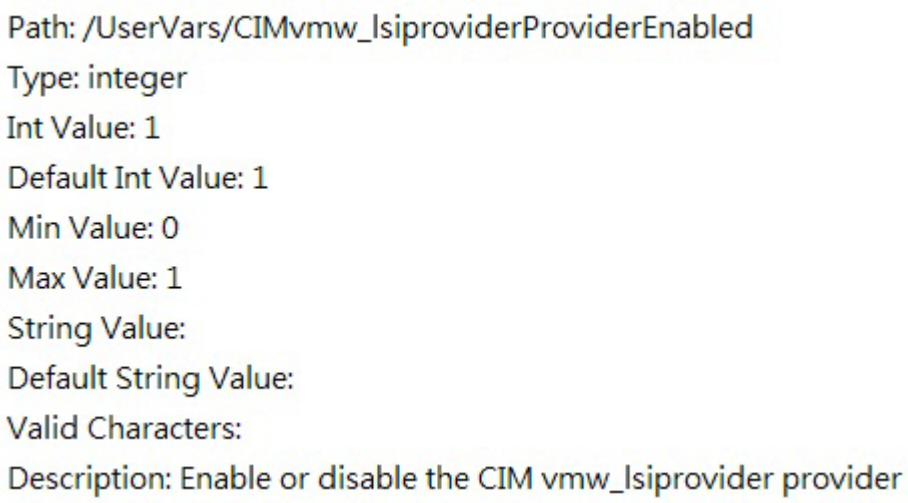


Figure 84. UserVars/CIMvmw_lsiproviderProviderEnabled is 1

3. Disable the CIM vmw_lsiprovider provider by executing:
   `esxcli system settings advanced set -o /UserVars/CIMvmw_lsiproviderProviderEnabled -i 0`
4. Use the following command to make the change taking effect:
   `/etc/init.d/sfcbd-watchdog restart`
5. Execute `esxcli system settings advanced list` again to verify the current value of `/UserVars/CIMvmw_lsiproviderProviderEnabled` is 0

```
Path: /UserVars/CIMvmw_IsiproviderProviderEnabled
Type: integer
Int Value: 0
Default Int Value: 1
Min Value: 0
Max Value: 1
String Value:
Default String Value:
Valid Characters:
Description: Enable or disable the CIM vmw_Isiprovider provider
```

Figure 85. /UserVars/CIMvmw_IsiproviderProviderEnabled is 0

Configuring Multipath on x86-64 (Intel or AMD) Host Running VMware

This section covers the setup and verification of the multipath configuration settings on x86-64 (Intel or AMD) host running VMware.

Verify the controller state and preferred path

- **Instructions for using CLI**
  1. Check the controllers are in bound state by issuing the following commands:

```
<CLI> list controller
Current Machine Local Time: 08/05/2013  01:59:13 PM
 ____________________________________________________________________
|   Ctlr#    |   Controller   |       Status       |  Ports  |  LUNs   |
|____________|________________|____________________|_________|_________|
|          0 |           Ctlr0|             PRIMARY|        1|        0|
|          1 |           Ctlr1|           SECONDARY|        1|        0|
|____________|________________|____________________|_________|_________|
```

Figure 86. Commands

  2. Check your preferred path by issuing the following commands:

```
<CLI> list pool
Current Machine Local Time: 08/05/2013  02:01:06 PM
 ____________________________________________________________________________________________________
|Pool#| ID |    Name     |RaidType|OwnerCtlr|TotalCap|AvailCap|       Status         |  State  | Degraded  |
|_____|____|_____________|________|_________|________|________|______________________|_________|___________|
|    0|   1|         p1r10|      10|   Slot 0|  1676GB|   716GB|  Viable-InTransition|      ONV|         No|
|    1|   2|          p2r5|       5|   Slot 1|  1460GB|   980GB|               Viable|      ONV|         No|
|    2|   3|          p3r0|       0|   Slot 0|  1116GB|   876GB|               Viable|      ONV|         No|
|    3|   4|          p4r1|       1|   Slot 1|   279GB|    39GB|               Viable|      ONV|         No|
|_____|____|_____________|________|_________|________|________|______________________|_________|___________|
```

Figure 87. Commands

In this example the pool “p1r10” has its preferred path set to controller 0 as indicated by “Slot 0”. All of the volumes (LUNs) belonging to this pool will have a preferred path to controller 0 (also known as bay 3 or I/O module 3). Similarly the “p2r5” pool has its preferred path set to controller 1 as indicated by “Slot 1”.

- **Instructions for using Storage Configuration Manager**
  1. Go to the controller tab and check to make sure both controllers are online.
  2. Go to the storage pool tab and identify the preferred path by displaying the properties of the storage pool as shown below. Please note that all of the volumes(LUNs) belonging to a given storage pool will have the same preferred path as the storage pool itself. In the example given below, preferred controller ownership is indicated by “Primary Controller” and is showing controller 2 (this is equivalent to “Slot 1” in the CLI display and is the same as bay 4 or I/O module 4)

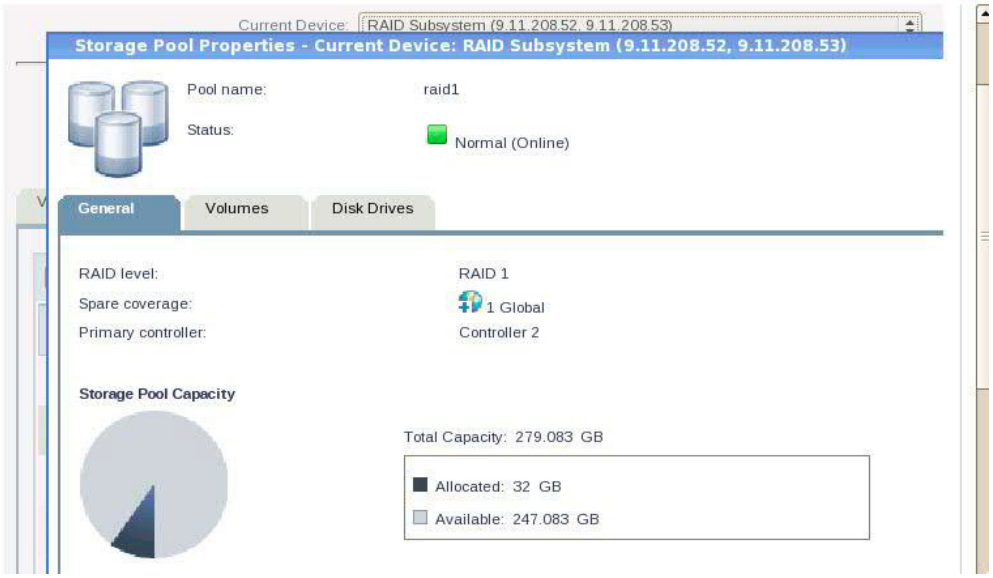


Figure 88. Example of SCM preferred path view

Identifying the WWN for certain SAS RAID Controller Module

1. Open a telnet connection to the SAS switch which belongs to the preferred SAS RAID Module.
2. Login to the SAS switch.

   Note: The default username and password is USERID/PASSW0RD
3. Execute the following command

   `phystat`

   The WWN for the SAS RAID Controller Module will be listed in the address of PHY 08 to PHY 0A. This WWN will be used in later steps to identify the connection to the specific module.

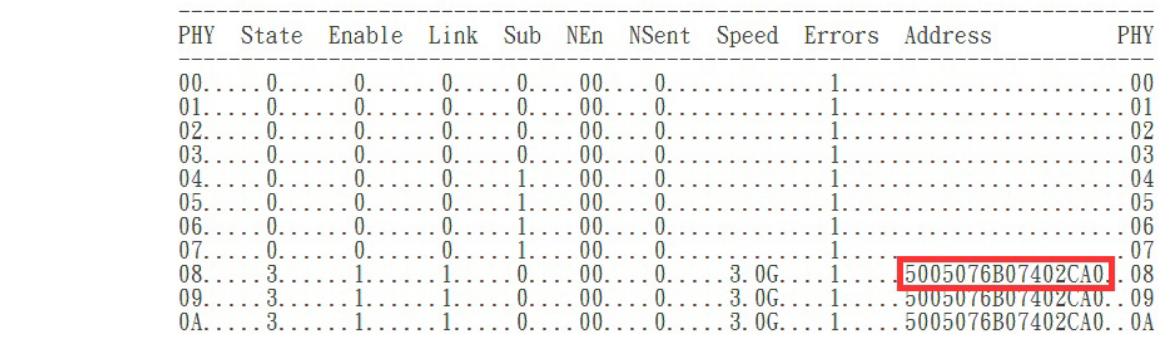


Figure 89. WWN

Updating the preferred path policy on VMware

- **VMware ESX and ESXi 3.5**
  1. Open the VMware Infrastructure Client.
  2. Select the host that you wish to change in the left pane.
  3. In the right pane, click on the Configuration tab.
  4. In the Configuration window, by the Details box is a "Properties" link.
  5. Click on "Properties" and it will open a Datastore properties window.
  6. Select the "Manage Paths" button in the bottom right corner of the window.
  7. In the "Manage Paths" window, click on the "Change" button at the top in the Policy box.
  8. In the "Manage Paths - Selection Policy" window, select the radio button next to "Fixed " and click OK. If “Fixed” policy is already selected, no action is required.
  9. Back out of the other windows and click OK and Close. These changes will need to be made for all ESX hosts that you wish to have this setting.
- **VMware ESX and ESXi 4.x / 5.x**
  1. Open the vSphere Client.
  2. Click the host you want to modify and click the Configuration tab.
  3. Click “Storage” and select a mapped LUN. And then click the “Properties” link.
  4. In the “Properties” dialog, select the desired extent, if necessary.
  5. Click **Extent Device** > **Manage Paths** and obtain the paths in the Manage Path dialog.
  6. Under the “Policy” section, select "Fixed" from the dropdown and click OK. If "Fixed" policy is already selected, no action is required.
  7. Click "Change" to confirm the change in path policy. These changes will need to be made for all LUNs mapped.

Updating the active path settings

- **VMware ESX and ESXi 3.5**
  1. Within the VMware Infrastructure client, highlight the host with access to the SAS RAID Controller Module.
  2. Under configuration, select "Storage" from the side panel/menu and highlight the storage LUN to be changed.
  3. Click "Properties" and then select "Manage paths."

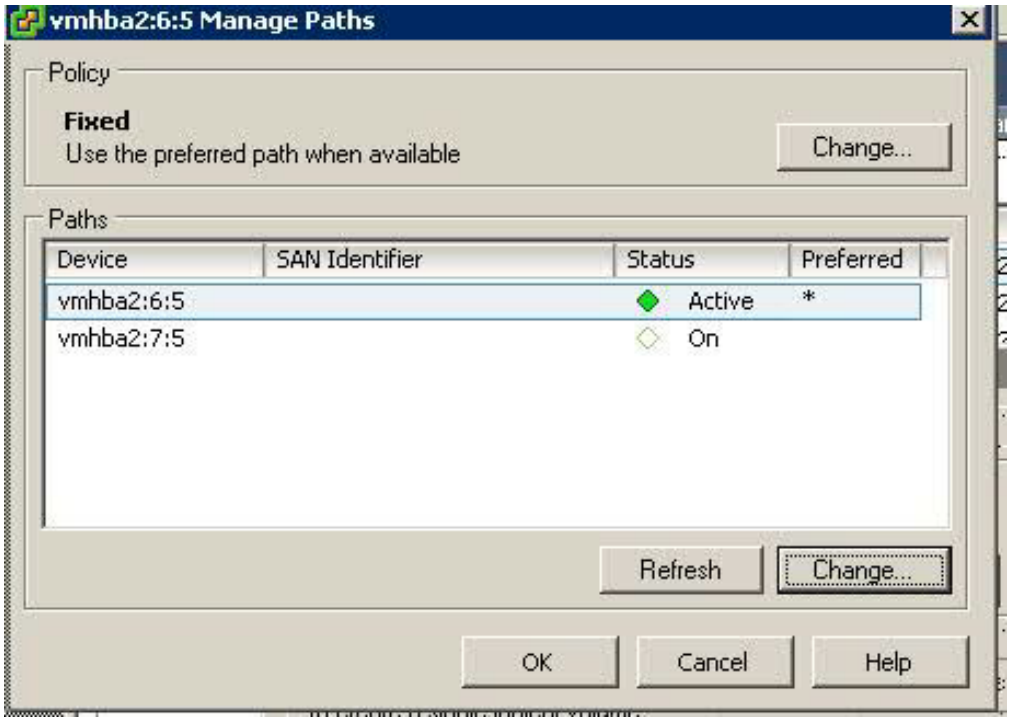


Figure 90. Example of VMware ESX and ESXi 3.5 manage paths Dialog

Note: The lower numbered path represents controller0 (vmhba2:6:5) and the higher numbered path represents controller 1 (vmhba2:7:5)

4. If the preferred path is same as indicated by the CLI or SCM display, no action is required. If the preferred path does not match what is indicated in the SAS RAID Controller Module CLI or SCM display, click the “Change” button to correct it. Repeat the process for each of the LUNs.

- **VMware ESX and ESXi 4.x / 5.x**
  1. Within the vSphere Client, highlight the host with access to the SAS RAID Controller Module.
  2. Under configuration, select "Storage" from the side panel/menu and highlight the storage LUN to be changed.
  3. Click "Properties" and then select "Manage paths."

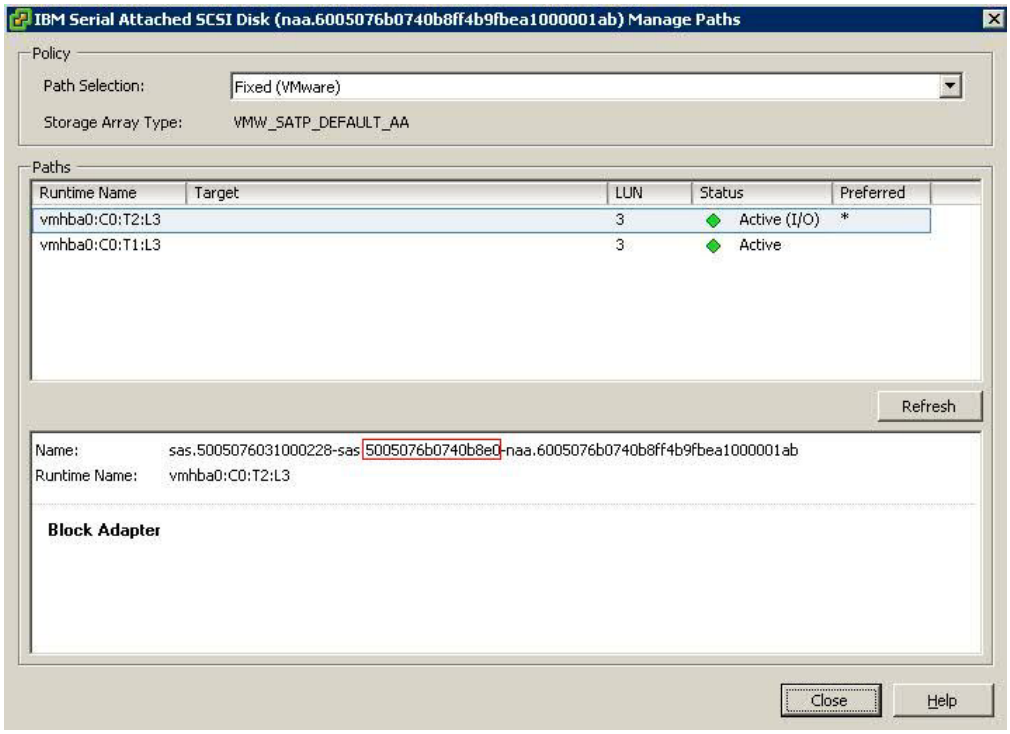


Figure 91. Example of VMware 4.x / 5.x manage paths Dialog

The red box in the figure highlights the WWN of the controller. Selecting a different volume in the dialog will update the lower sections associated information. One of the WWNs associated with the volume will match the WWN found when using the SAS switch CLI above. In this example the volume with the WWN that matches is for the controller in IO Bay 3.

4. If the preferred path is same as indicated by the CLI or SCM display, no action is required. Repeat the process for each of the LUNs. If the preferred path is different from what is indicated in the SAS RAID Controller Module CLI or SCM display, then this needs to be updated using the ESX CLI or GUI. Repeat the process for each of the LUNs.

Configuration for SAS Booting on x86-64 (Intel or AMD) Host Running VMware

The following section describes how to configure Remote SAS Booting on x86-64 (Intel or AMD) host running VMware.

Refer to Appendix B, “Appendix B: SAS Boot Pre-Operating System Installation Activities,” on page 157, to validate that the system is ready to install a SAS booted operating system.

Operating system installation

Use the applicable procedures and instructions that are provided with your operating system software to configure the operating system on the boot volume that is mapped to the blade server. It is not the intention of this document to show how to install the operating systems or to select which software packages will be installed or required for the initial installation of the operating system.

The ESX Server operating system should contain the latest SAS device drivers and multipath drivers. There is no need to go to the IBM Support web sites for these drivers. There may be patches that are required for your version of ESX server at the VMware Support web site.

Post-Operating system installation activities

Perform the following steps to complete the ESX Server operating system setup.

Procedure

1. Using the SCM program or the CLI interface the second path to the boot volume can now be mapped to the blade server. At this time additional volumes may also be created and mapped to both SAS ports.
2. In the VMware ESX server, rescan the SCSI bus to discover the boot volume on the second path and the newly mapped LUNs. An example of VMware Infrastructure Client screenshot showing the two paths to the ESX Server for the 50GB and 7GB volumes is shown below. Use the Rescan button on the upper right corner to scan for new devices.

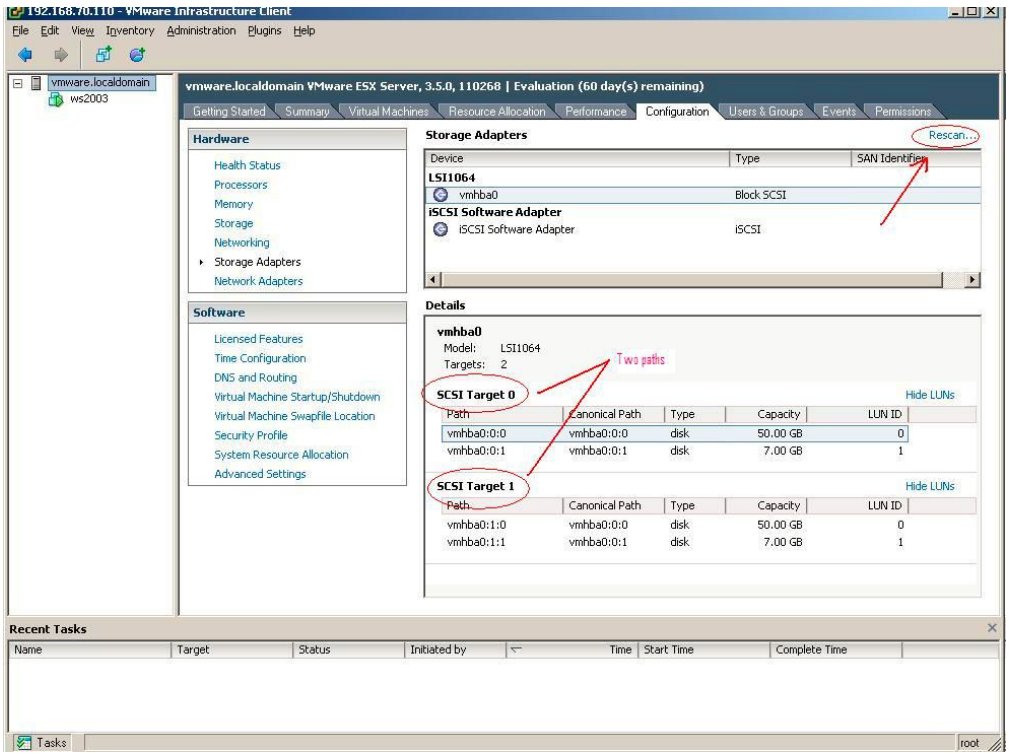


Figure 92. Example VMware Dialog showing rescan option

3. Right click on the path entry in the Storage Adapter screen under the Configuration tab of the ESX server VMware Infrastructure Client window to verify and set, if required, the preferred path for the mapped volumes. The ESX

Server multipath driver will always use the first known path to the SAS RAID Controller Module volumes as the preferred path by default. Because of the SAS adapter and the BC-S chassis architecture, the first known (scanned) path is normally through the SAS RAID Controller Module controller installed in IO bay 3 of the BC-S chassis. If the volume has the SAS RAID Controller Module in IO bay 4 as the preferred owner, the preferred path for this volume might need to be reset to the SAS RAID Controller Module in IO bay 4 instead of the SAS RAID Controller Module in IO bay 3. An example screenshot is shown below.

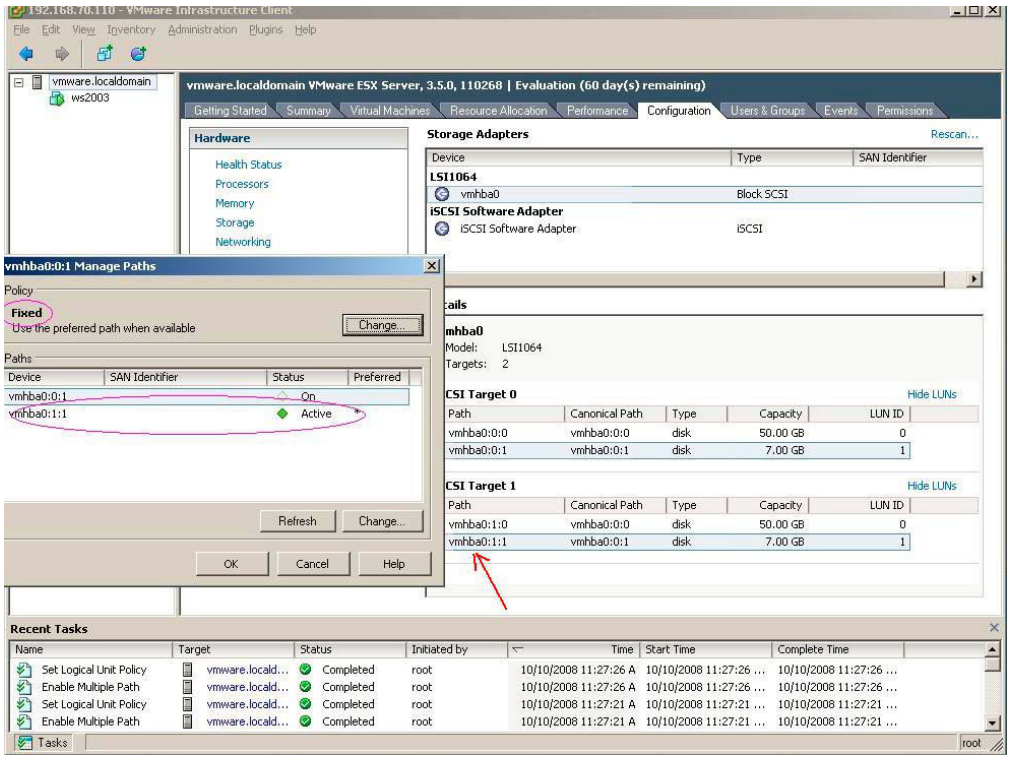


Figure 93. Example of VMware Dialog showing active preferred path

4. After installing the operating system in the VMware virtual machine, the "VMware tools" should be installed in the VMware virtual machine. The "VMware tools" is installed by right-clicking on the Guest OS entry and select Install/Update VMware tools from the pull-down menu. Please refer the VMware publications for more info about the "VMware tools" and how to install it.

Verifying & Setting LUN Parameters on VMWare Guest Operating Systems running Linux

The following procedures are used to verify and set the LUN configuration parameters on VMWare Guest Operating Systems running Linux.

To verify these setting, change the directory to /sys/block/sdXX/device, where sdXX is one of the SAS RAID Controller Module devices. View the contents of the files named queue_depth and timeout. For example,

```
[ ... … ] # cd /sys/block/sdb/device
[ ... … ] # cat queue_depth
32
[ ... … ] # cat timeout
30
```

Figure 94. VMWare Linux timeout and queue depth settings

Note: For running **RHEL 6.x** as VMWare Guest Operating Systems, the SCSI controller need to be set to "LSI logic SAS" in advance to ensure the queue depth setting work properly.

To change the queue_depth value to the recommended value of 4 use the following procedure:

1. Change to the uDev rules directory as follows:

   ```
   cd /etc/udev/rules.d
   ```

   For SLES 10.x edit the file named:

   ```
   50-udev-default.rules
   ```

   For SLES 11.x edit the file named:

   ```
   50-scsidisk.rules
   ```

   For RHEL5.x / RHEL 6.x edit the file named:

   ```
   50-udev.rules
   ```

2. Look for lines similar to:

   ```
   ACTION=="add", SUBSYSTEM=="scsi", SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo 60 > /sys$$DEVPATH/timeout'"
   ```

   If the value is not 60, then update the value to 60 as shown above.

   If the line cannot be found, insert the above line into the file.

3. Insert the below line into the file:

   ```
   ACTION=="add", SUBSYSTEM=="scsi", SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo 4 > /sys$$DEVPATH/queue_depth'"
   ```

4. Save the file and exit the editor.
5. Reboot the system and then verify the queue_depth value as shown in Figure 94

Verifying & Setting LUN Parameters on VMWare Guest Operating Systems running Microsoft Windows

The following procedures are used to verify and set the LUN configuration parameters on VMWare Guest Operating Systems running Microsoft Windows.

About this task

Note:

1. The actual value used depending on the number of LUNs mapping to the host. See Serial Attached SCSI host attachment for more information on how to calculate the correct settings, and then back to this section.
2. The SAS HBA driver level needs to be verified with different parameter and route settings for changing the queue depth. To verify the driver level, see Updating the Driver for a SAS HBA on x86-64 (Intel or AMD) Host Running Windows for more information. Check the Properties screen of "SCSI and RAID controllers" (or "Storage Controllers" in Windows Server 2008/2012) in Device manager. The driver level should be listed in the Driver tab.

Procedure

1. Start the registry editor command by entering the following command from the Windows command prompt.

   ```
   regedit
   ```

2. Save a backup copy of the current registry before making any changes. Select the highest level key and then select File → Export.
3. Navigate to the following key. Create the key if one is not available.

   ```
   For driver of LSI_SAS,
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSI_SAS\Parameters\Device
   For driver of LSI_SAS2,
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSI_SAS2\Parameters\Device
   ```

4. Right-click DriverParameter and select Modify from the menu. Create the DriverParameter if one is not available.
5. Add the parameter of the SAS registry entry.
   a. LSI_SAS with driver version 1.33.01 (or later); LSI_SAS2 with driver version 2.00.29 (or later).

      Add **MaxSASQueueDepth=4** (default 64) after the last entry. Update the value if the entry already exists.

      The number is decided by the number of LUNs assigned to the host. Ex: MaxSASQueueDepth = 4 while setting 16 LUNs to the host.

   b. LSI_SAS with driver version prior to version 1.33.01; LSI_SAS2 with driver version prior to version 2.00.29.

      Add **MaximumTargetQueueDepth=4** after the last entry. Update the value if the entry already exists.

      Important: Make sure to update the value in the registry entry above. See Serial Attached SCSI host attachment for more information on how to calculate the correct settings.

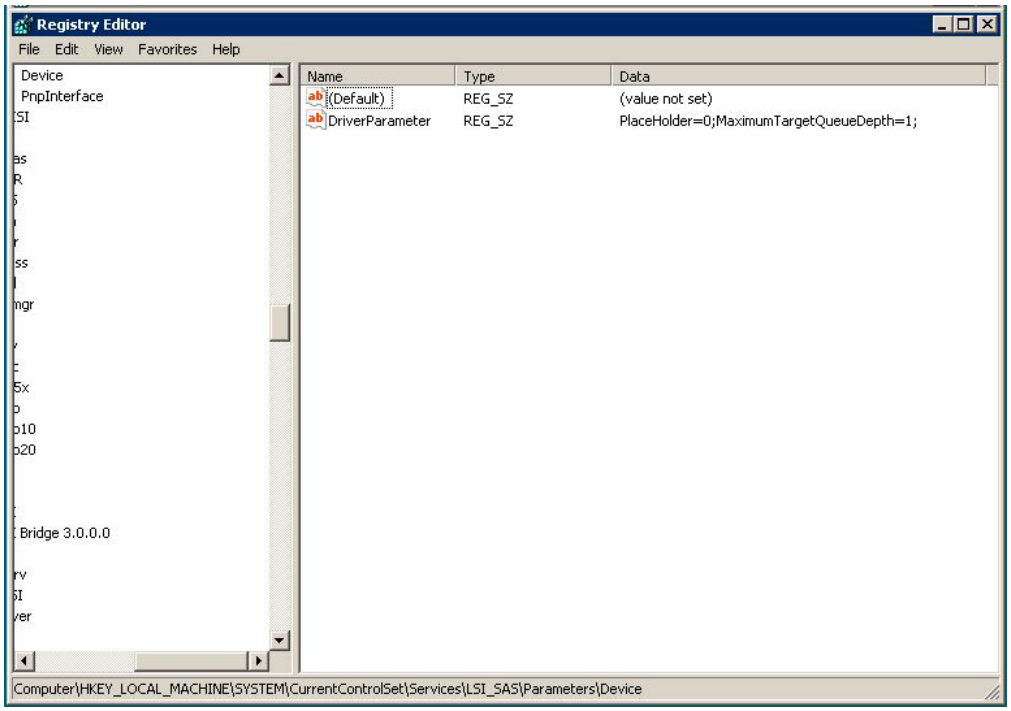


Figure 95. Example Registry Settings Screen for Windows

6. Save changes and exit the registry editor.
7. Reboot the host blade for the changes to be applied.

Troubleshooting

This section covers currently known issues with using the IBM BladeCenter S SAS RAID Controller Module with the host blades running the Linux operating system.

Concurrent Maintenance using the AMM

When performing maintenance on the SAS RAID Controller Module which requires the module to be powered off and then back on through the AMM, it is possible that all paths may not be restored after the SAS RAID Controller Module has powered back on and bound to the surviving controller.

About this task

After the maintenance operation is complete, verify that the host blade multipathing has restored all available paths to both SAS RAID Controller Modules. To perform this check on the host blade run the following command as root:

```
[root@localhost ~] esxcli nmp path list
```

The output of the command should be similar to the following, showing two paths to each LUN:

```
sas.5005076031000228-sas.5005076b0740b8a0-naa.6005076b0740b8ff4b21563f00000141
Runtime Name: vmhba0:C0:T1:L0
Device: naa.6005076b0740b8ff4b21563f00000141
Device Display Name: IBM Serial Attached SCSI Disk (naa.6005076b0740b8ff4b21563f00000141)
Group State: active
Storage Array Type Path Config:
```

```
Path Selection Policy Path Config: {current: yes; preferred: yes}

sas.5005076031000228-sas.5005076b0740b8e0-naa.6005076b0740b8ff4b21563f00000141
Runtime Name: vmhba0:C0:T2:L0
Device: naa.6005076b0740b8ff4b21563f00000141
Device Display Name: IBM Serial Attached SCSI Disk (naa.6005076b0740b8ff4b21563f00000141)
Group State: active
Storage Array Type Path Config:
Path Selection Policy Path Config: {current: no; preferred: no}
```

If the output shows only one path or a mix of paths to the SAS RAID Controller Modules, then run the one of the following ways to restore the redundant paths:

Procedure

1. Using the VMware vSphere or VI Client to perform a rescan:
   a. Log in to the client and select an ESX/ESXi host in your inventory.
   b. Click the Configuration tab.
   c. Click Storage Adapters.
   d. Click the Rescan link.
   e. Click OK to begin the rescan.

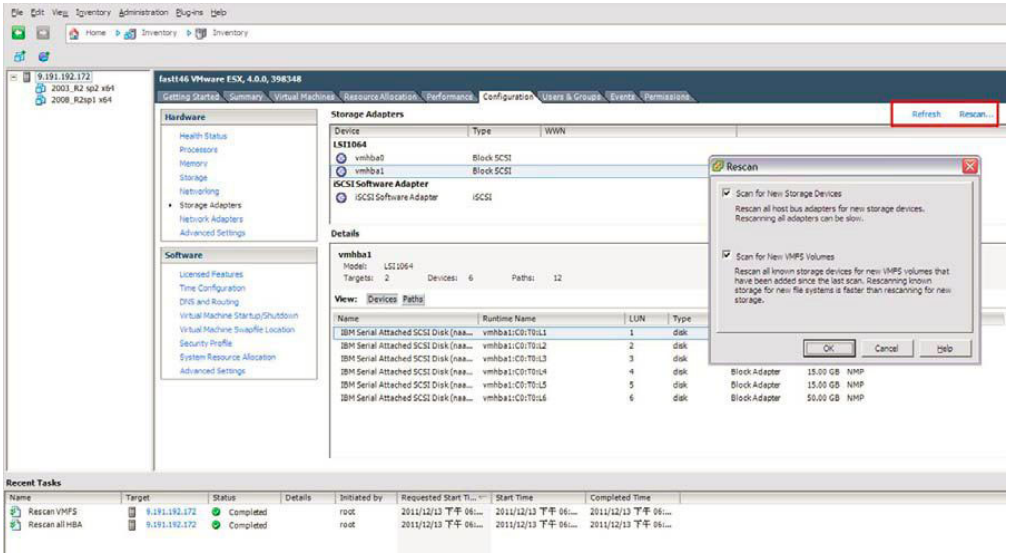


Figure 96. Perform a rescan usingVMware vSphere to restore the redundant paths

   Note: This performs a rescan of every installed Hardware Bus Adapter (HBA), regardless of the HBA that is selected in the Storage Adapters view.

2. Perform a rescan from the ESX/ESXi host command-line
   a. Log in to the ESX/ESXi host console.
   b. Run the command:

   For ESX/ESXi 4.x

   ```
   esxcfg-rescan <vmkernel SCSI adapter name>
   ```

   Where <vmkernel SCSI adapter name> is the vmhba# to be rescanned.

   Note: The rescan must be performed on each HBA that is attached to the storage that changed. In ESX 4.x there may not be any output if there are no changes.

For ESXi 5.x

- To rescan all HBAs:

```
esxcli storage core adapter rescan --all
```

- To rescan a specific HBA:

```
esxcli storage core adapter rescan --adapter<vmkernel SCSI adapter name>
```

Where <vmkernel SCSI adapter name> is the vmhba# to be rescanned.

Note: There may not be any output if there are no changes.

Verify that after running the above command all paths become available using the following command:

```
[root@localhost ~] esxcli nmp path list
```

Chapter 5. Chapter 5 IBM Power Systems Running AIX / VIOS Host Attachment

This section describes how to attach a System P host blade running the AIX or VIOS operating system to the SAS RAID Controller Module.

For the most current information on supported hosts and operating systems, fix packs, and i-fixes, review the *IBM SAS RAID Module Interoperability Guide* at:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5078491&brandind=5000020

The following sections are covered in this chapter:

Updating the Driver for a SAS Expansion Card on an IBM Power Blade Running AIX / VIOS

Drivers are update using AIX fix packs; please refer to the section regarding installation of fix packes for updating the SAS Expansion Card driver.

Configuring Host System Settings on an IBM Power Blade Running AIX / VIOS

The following section describes how to perform required changes to the host system settings on an IBM PS / JS (Power / pSeries) blade running AIX / VIOS.

Changing Queue Depth and Hot plug settings

To edit the queue depth settings for host blades running the AIX or VIOS operating system, perform the following steps.

Note: These actual value used will depend on the number of LUNs mapped to the host. Refer to the section, "Serial Attached SCSI host attachment" on page 12, to review how to calculate the correct settings, then return to this section.

To identify the current queue depth value, execute the following command on the AIX host blade:

```
blade1# lsattr -El hdisk5
PCM             PCM/friend/sasother                 Path Control Module             False
algorithm       fail_over                           Algorithm                       True
clr_q           no                                  Device CLEARS its Queue on error True
dist_err_pcnt   0                                   Distributed Error Percentage    True
dist_tw_width   50                                  Distributed Error Sample Time   True
hcheck_cmd      test_unit_rdy                       Health Check Command            True
hcheck_interval 60                                  Health Check Interval           True
hcheck_mode     nonactive                           Health Check Mode               True
max_transfer    0x40000                             Maximum TRANSFER Size           True
pvid            none                                Physical volume identifier      False
q_err           yes                                 Use QERR bit                    True
q_type          simple                              Queuing TYPE                    True
queue_depth     5                                   Queue DEPTH                     True
reassign_to     120                                 REASSIGN time out value         True
reserve_policy  no_reserve                          Reserve Policy                  True
rw_timeout      30                                  READ/WRITE time out value       True
size_in_mb      0                                   Size in Megabytes               False
start_timeout   60                                  START unit time out value       True
unique_id       362136005076B0741A17F4B71ECF000..   Unique device identifier        False
ww_id           6005076b0741a17f4b71ecf000000071    World Wide Identifier           False
```

Note: The queue depth value is identified by the variable queue_depth and it is 5 by default. Please refer to section "Serial Attached SCSI host attachment" on page 12 for information on how to determine the desired queue depth value.

Change it to a desired value by using the following example.

```
blade1# chdev -l hdisk5 -a queue_depth=3
hdisk5 changed
```

In the above case queue depth value is being changed to 3

Note: In the case of an active volume (a disk which is part of an active volume group), queue depth value should be changed using the following command. Please check the man pages of command chdev for detailed explanation on each option.

```
blade1# chdev -l hdisk5 -a –P queue_depth=3
hdisk5 changed
```

Verify that the queue depth value is changed to the desired value by using the following command;

```
lsattr -El hdisk
```

Reboot the server to have the values take effect.

Important: If you remove the disk device from the system, you will need to set the value once the device is reconfigured.

Configuring SDD PCM on an IBM Power Blade Running AIX / VIOS

This section shows how to configure SDD PCM on an IBM Power Blade Running AIX / VIOS.

For installation and configuration if the SDD PCM driver on AIX host systems, please refer to the *Multipath Subsystem Device Driver User's Guide*:

https://www.ibm.com/support/docview.wss?uid=ssg1S7000303

Configuration for SAS Booting on an IBM Power Blade Running AIX / VIOS

This section describes the configuration for SAS booting on an IBM PS / JS (Power / pSeries) blade running AIX / VIOS.

Creating a SAS RAID Module volume for the SAS boot installation

About this task

Before beginning:

- Ensure the SAS RAID Modules are powered ON.
- Ensure the SAS RAID Modules are in dual controller mode and in Primary/Secondary state.

Procedure

1. Use the IBM Storage Configuration Manager (SCM) or the SAS RAID Controller Module command line interface (CLI) to create at least one volume, a boot volume, for each blade server in the IBM BladeCenter S (BC S) chassis. It is recommended that you map this boot volume as LUN 0 for each blade server.

   The following are guidelines for creating the boot volume:

   a. Ensure that the volume that is used as the boot volume has enough free disk space to contain the operating system, its swap space, and any application code. The volume must also be large enough to accommodate future updates.

   b. For protection against disk failure, the boot volume should be part of RAID 1, 10 or 5 storage pools. You can use a RAID 0 pool for a boot volume, however there is no protection against disk failure.

c. Even though you can create the boot volumes for all the server blades in a BC S chassis as part of the same RAID storage pools, it is recommended to split the boot volumes into at least two RAID storage pools where one pool has the SAS RAID Module in bay 3 as the preferred owner and the other pool has the SAS RAID Module in bay 4 as the preferred owner.

d. Each blade server supports a maximum of sixteen volumes. At this time, only create the volume that is going to be used as the boot volume. You can use additional volumes later on to store operating system code, swap space, application program code, and application data. If you choose to create volumes other than the boot volume at this time, do not map the additional volumes to the blade server SAS ports. You can create the additional volumes and map them to the blade server as part of the post operating system installation activities.

   Important: Map this boot volume to only **one** of the blade server SAS ports. The system presents multiple disk device entries when it sees the same boot volume on multiple paths. For example, if the boot volume is mapped to two SAS ports, the system will present two available disks that can be used for the operating system installation. If you are not using SCM, you can obtain the WWPN of the blade server SAS port by using telnet to connect to the SAS switch component of the SAS RAID Module and running the **sasport status all** command. In the example SAS Switch phy output figure below, the output of the **sasport status all** command shows the WWPN of the SAS port in blade server 1 is **500062B0000D7A10**.

   Note: The blade servers must be turned on and should be at the Software Maintenance System (SMS) menu so that the SAS switch can discover the SAS card WWPN. Once you map the boot volume to the SAS port in the blade server, you should see the volume displayed as an hdisk in the AIX installation menu.

```
=== IBM BladeCenter(R) SAS RAID Controller Module ===
Login: USERID
Password: ********
USERID logged on
MAIN> sasport status all
ID SAS Port Name SAS Address Enable Flt Status
---+-------------------------+----------------+------
+---+--------
E1 External Port 1 True Off NoCable
PHY 1C 0000000000000000 True NoCable
PHY 1D 0000000000000000 True NoCable
PHY 1E 0000000000000000 True NoCable
PHY 1F 0000000000000000 True NoCable
E2 External Port 2 True Off NoCable
PHY 20 0000000000000000 True NoCable
PHY 21 0000000000000000 True NoCable
PHY 22 0000000000000000 True NoCable
PHY 23 0000000000000000 True NoCable
E3 External Port 3 True Off Normal
PHY 00 0000000000000000 True Normal
PHY 01 0000000000000000 True Normal
PHY 02 0000000000000000 True Normal
PHY 03 0000000000000000 True Normal
E4 External Port 4 True Off NoCable
PHY 04 0000000000000000 True NoCable
PHY 05 0000000000000000 True NoCable
PHY 06 0000000000000000 True NoCable
PHY 07 0000000000000000 True NoCable
B1 Blade Slot Connection 1 True Off Normal
PHY 1B 500062B0000D7A10 True Normal
B2 Blade Slot Connection 2 True Off Normal
PHY 1A 500062B00007CD84 True Normal
B3 Blade Slot Connection 3 True Off Normal
PHY 19 500062B0000D79F4 True Normal
B4 Blade Slot Connection 4 True Off Normal
PHY 18 500062B00007E6DC True Normal
B5 Blade Slot Connection 5 True Off NoCable
PHY 17 0000000000000000 True NoCable
B6 Blade Slot Connection 6 True Off Normal
PHY 16 500062B00007E6E0 True Normal
B7 RAID HA Connection True Off Normal
PHY 0A 5005076B07418C20 True Normal
PHY 09 5005076B07418C20 True Normal
PHY 08 5005076B07418C20 True Normal
PHY 0F 5005076B07418C20 True Normal
---+-----------------------+----------------+------+---
+--------
ID SAS Port Name SAS Address Enable Flt Status
```

Figure 97. Example SAS Switch phy output

Note: When the boot volume is created, you can specify that the storage pool with the SAS RAID Module in bay 3 (-port 0 option when creating the pool) be the preferred owner, or that the storage pool with the SAS RAID Module in bay 4 (-port 1 option when creating the pool) be the preferred owner. Regardless of this preferred owner setting always use the WWPN of

the SAS port that is shown in the **sasport status all** command of the SAS switch in bay 3 for the initial OS installation (this is the first SAS port of the SAS card adapter). The first SAS port of a two port SAS card adapter will always have a WWPN that is one less than the WWPN of the second adapter. For example, if the first SAS port WWPN is '500062B0000D7A10', the second SAS port WWPN will be '500062B0000D7A11'.

2. If there is an internal hard drive installed in the blade server, it must be removed before installing the operating system on the remote boot volume.

Installing AIX 6.1 on a remote volume

Complete the following steps to start the AIX installation from an installation DVD.

Procedure

1. Insert the DVD into the DVD-ROM drive in the Media Tray of the BladeCenter S chassis.
2. Connect to the Advanced Management Module (AMM) and select **Blade Tasks -> Remote Control** from the navigation menu.
3. Click **Start Remote Control** to open a Remote Console window.
4. In the Remote Control window, click the **Media Tray** list and select the blade where you will load the new AIX operating system.
5. In the Remote Control window, click the blade list and select the blade that will be loading the operating system.
6. To begin loading the new OS, you must reboot the blade and set it to boot from the DVD-ROM drive. From the Remote Control window, select the **Power Control -> Restart**.

   Monitor the reboot of the blade from the Remote Console window.
7. As the blade reboots, press 1 to enter the SMS Menu.

   Note:

   - The menu options display for a short period of time. If it is missed reboot the blade again.
   - Some blades may require you to enter options before displaying the SMS menu option. A screen may appear asking you to enter the number 1 to choose that screen as the display. It may then ask you to enter an option to continue with the boot process, after which the option to enter the SMS menu displays as shown in the figure below.

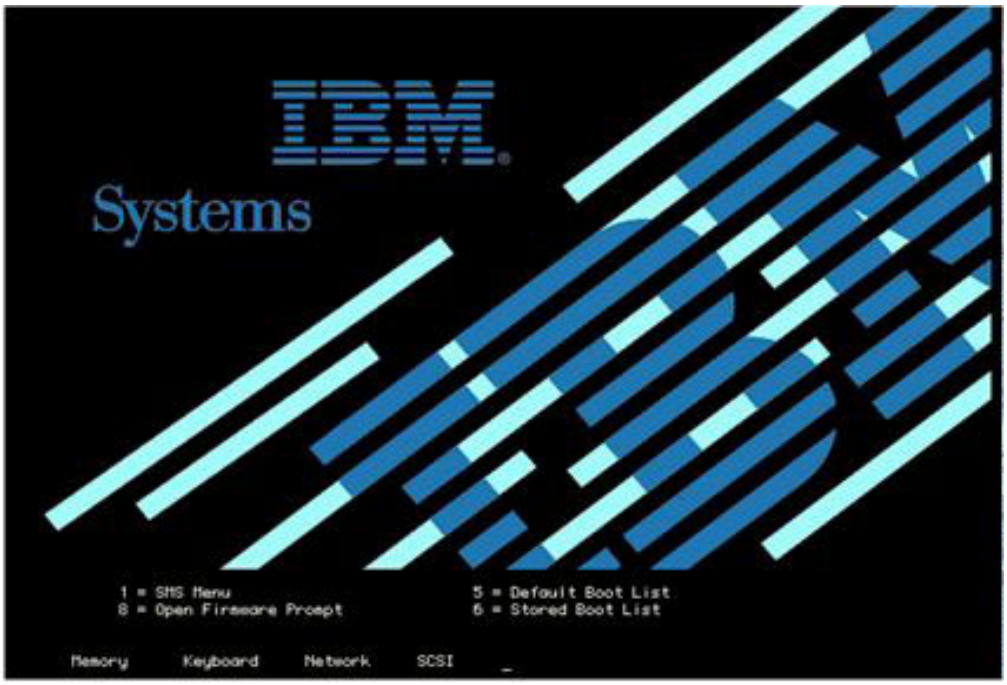


Figure 98. Reboot screen with option to enter SMS menu

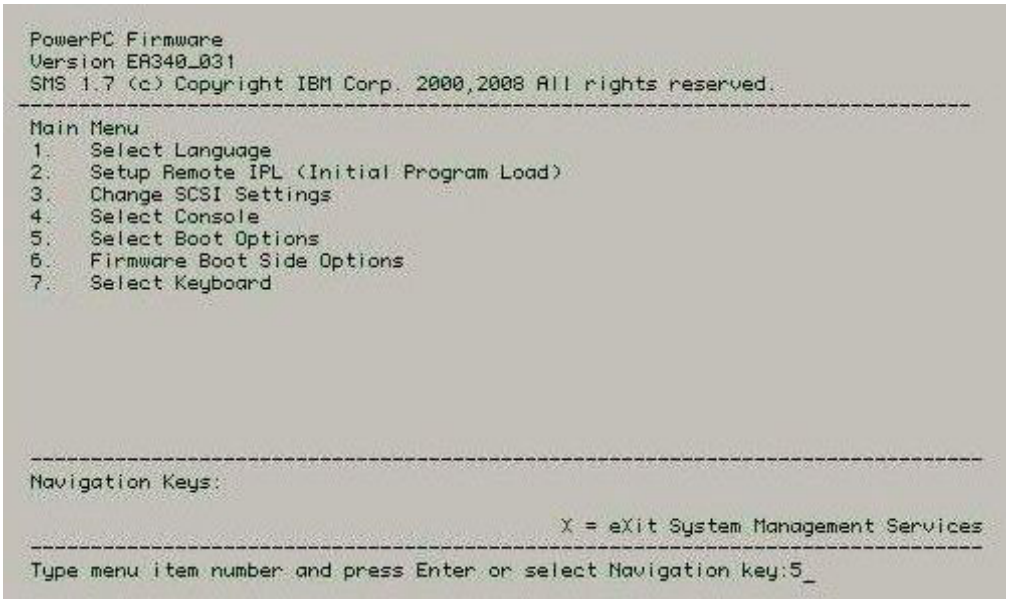


Figure 99. The SMS Main Menu

8. From the SMS Main Menu, enter the number for the **Select Boot Options** menu and press Enter.
9. Enter the number for the **Select Install / Boot Device** menu and press Enter.
10. Enter the number for the **CD/DVD** menu and press Enter.
11. Enter the number for the **List All Devices** and press Enter.
12. A list of all available devices now loads (note this may take a little time). Enter the number of the **USB CD-ROM** device and press Enter. For this

example, the USB CD-ROM is device 3.

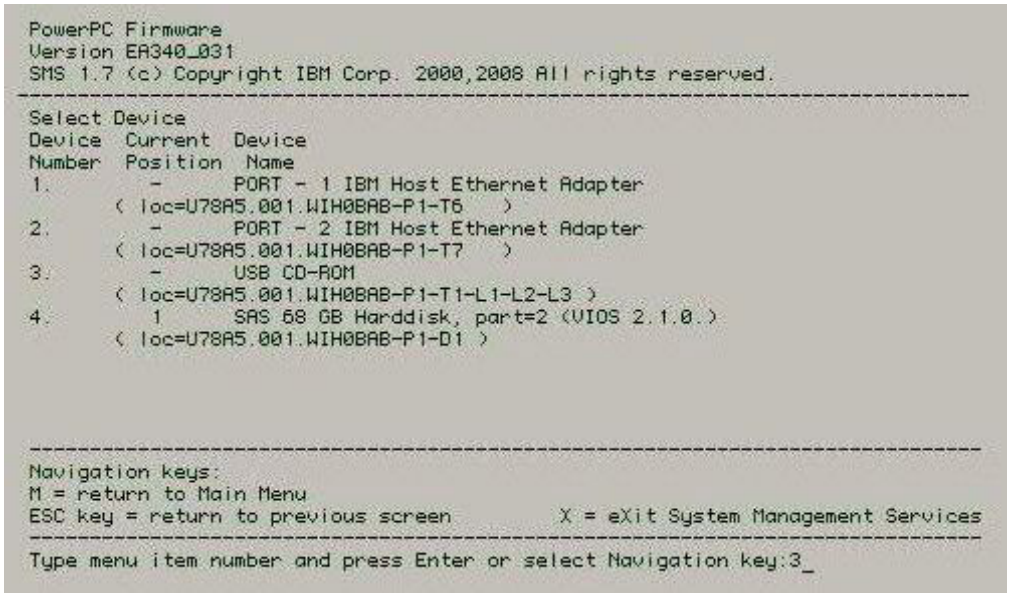


Figure 100. An SMS menu showing a list of CD and DVD devices

13. Enter **2** for **Normal Boot Mode** and press Enter.
14. Enter **1** for **Yes** and press Enter.

    Note: It may take up to 10 minutes before the installation begins.
15. When the installation screen appears, the system console will need to be defined. Follow the instructions on the screen to press F1 and then press Enter to use the current display as the system console.

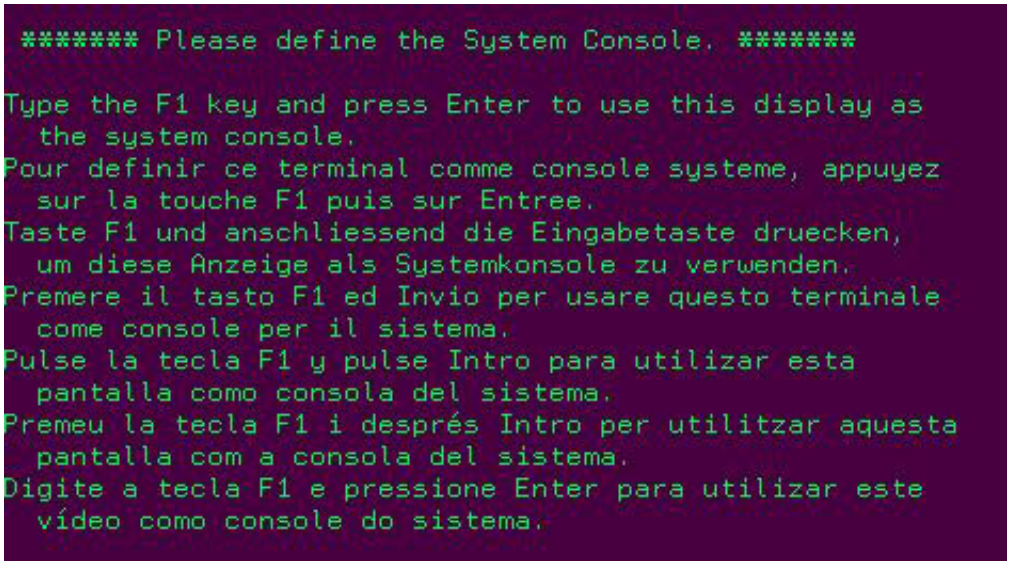


Figure 101. Define the system console for the AIX installation

16. Enter the number of the language you want to use during the installation and press Enter.
17. Enter **2** and press Enter to go to the Installation and Settings screen.

Note: In the below figure, there are two items listed under option 1, System Settings. The first option is **Method of Installation**. For a Blade that has never had an AIX installation this item will always be set to **New and Complete Overwrite**. However, if the blade has had a previous installation of AIX then there is the option to update the installation or to overwrite the previous installation. For either case, ensure **New and Complete Overwrite** is selected.

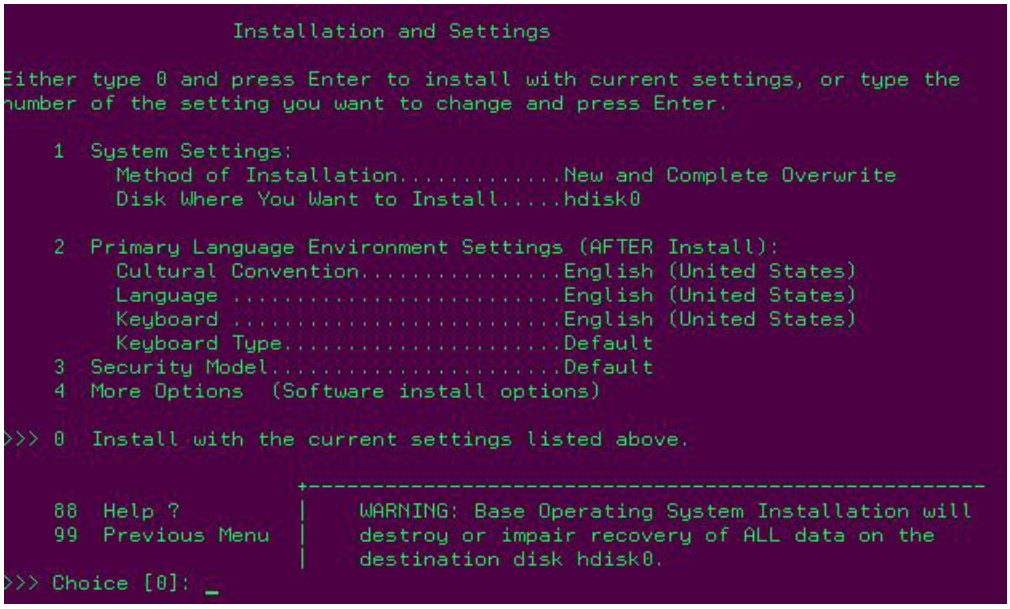


Figure 102. Installation and Setting screen of the AIX installation

18. Enter **1** and press Enter to go to System Settings.
19. If the blade had a previously AIX installation, Enter **1** for **New and Complete Overwrite**.
20. Enter the number of the hdisk to be used for the installation and press Enter.

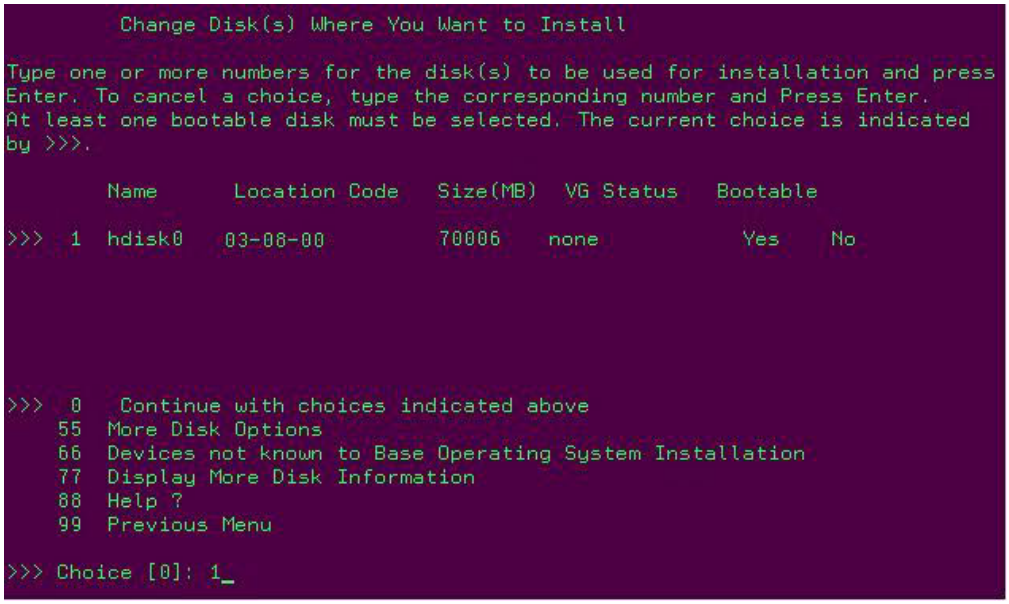


Figure 103. Example from a JS22 blade without an internal hard drive

21. Once the hdisk has been selected, enter **0** for **Continue with choices indicated above** and press Enter. The Installation and Settings menu will display with your choice.

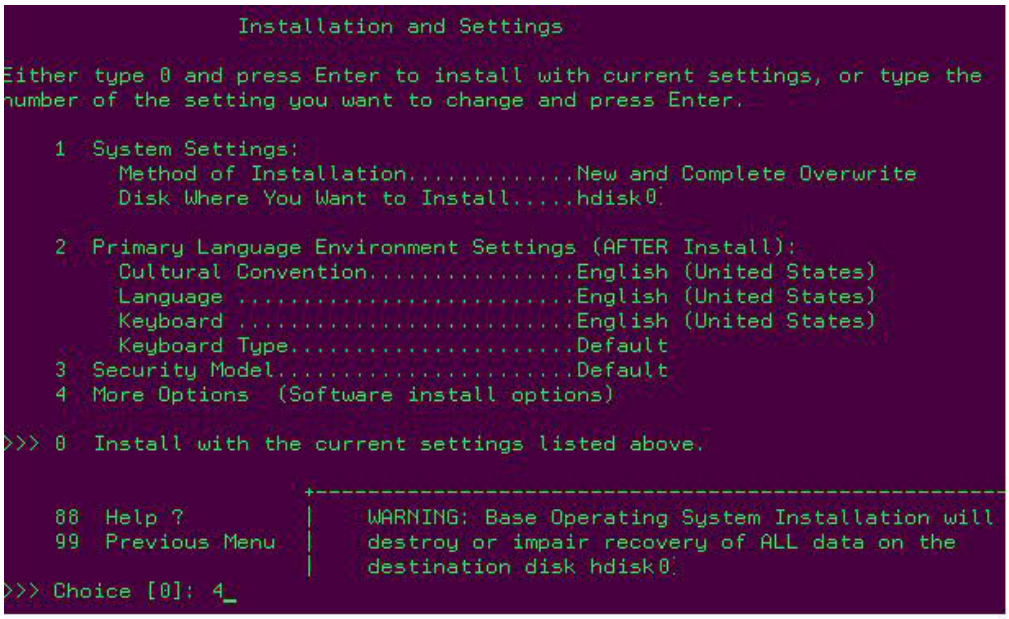


Figure 104. Updated Installation and Settings screen of the AIX installation

22. Proceed with normal installation.
23. Once installation is complete, use the SCM program or the CLI interface to map the boot volume to the second SAS port in the blade. Create additional volumes and map them to both SAS ports.
24. In order to see both paths and any additional LUNs reboot the blade now.
25. To check the the state of the paths and remote volumes, run the commands from section "Checking System hdisk (volume) Status on AIX" on page 119.

Obtaining AIX 6.1 Service Packs and Verifying the Installation

This section describes the steps required to obtain AIX Service Pack code.

About this task

For the most current information on supported operating systems, fix packs, and i-fixes, review the *IBM SAS RAID Module Interoperability Guide* at:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5078491&brandind=5000020

Procedure

1. Open a web browser to the following URL:

   http://www.ibm.com/support/fixcentral/

   This opens the IBM Support Fix Central website.
2. From the IBM Support Fix Central page, select the following options from the corresponding lists then click Continue:

Option	Description
Product Group:	**System p**
Product:	**AIX**
Version:	**6.1**
Fix Type:	**Fix packs**

3. In this example, select TL 6100-03-00-0920 from the Select a Technology Level list, then click Go.
4. Click the link for the 6100-03-01-0921 fix pack to open the 6100-03 Service Pack 1 page.

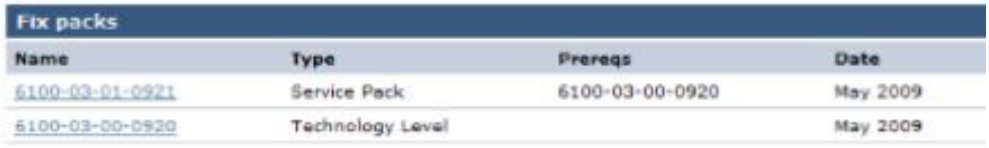


Figure 105. 6100-03-01-0921 fix pack

5. On the 6100-03 Service Pack 1 website, select **No, I am already at Technology Level 6100-03** and click **Continue**.

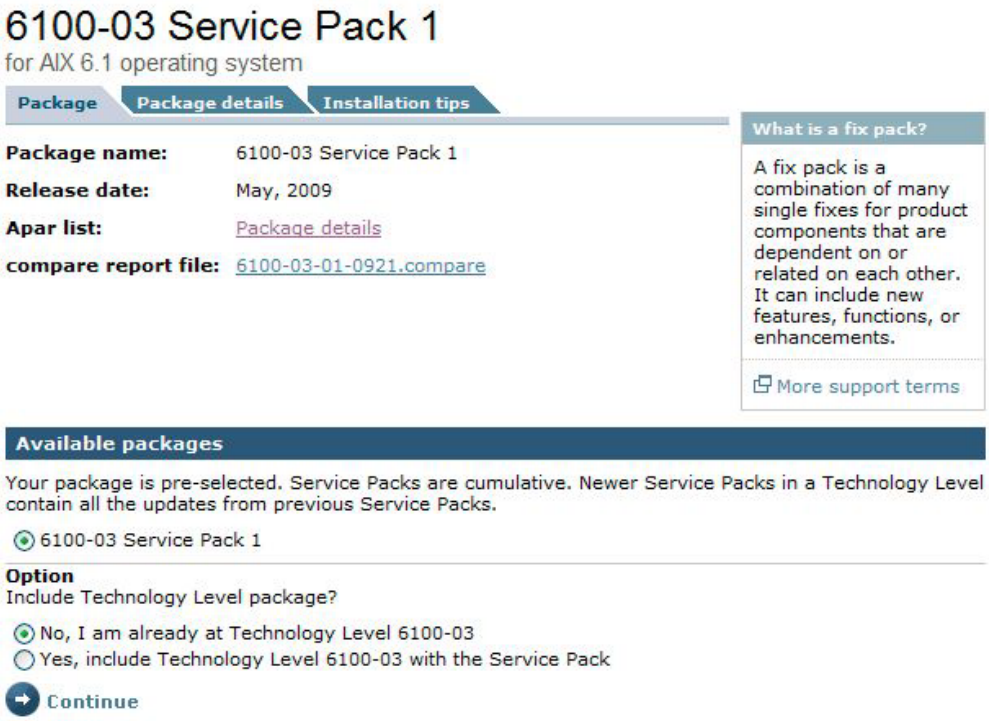


Figure 106. 6100-03 Service Pack 1

6. From the Package download page, select **Download using Bulk FTP** and click **Continue**.

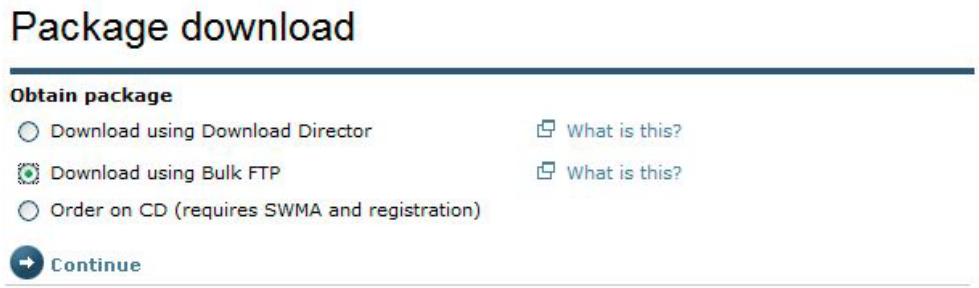


Figure 107. Package download page

7. Click **Continue** on the Download using Bulk FTP page. A notification will appear with the location of the file that you can download using FTP as seen in Figure 85: Select how to download the Service Pack.

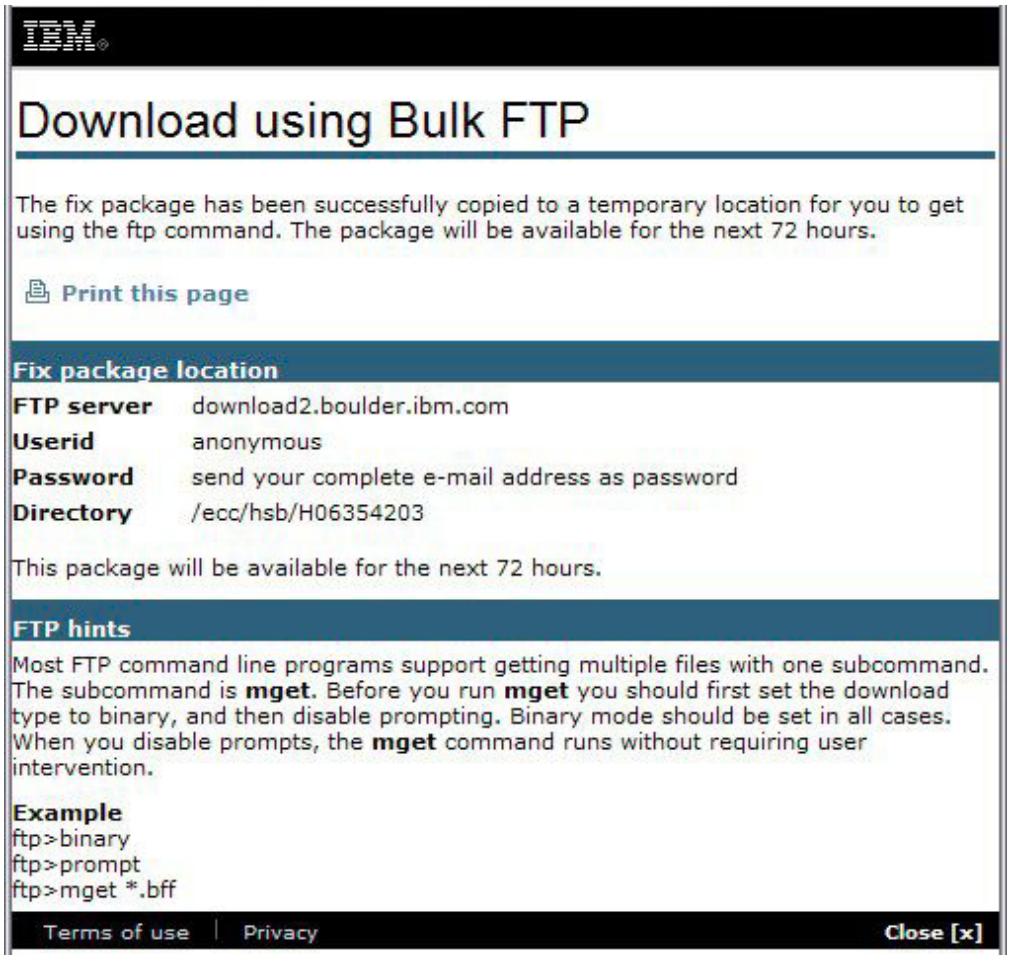


Figure 108. Select how to download the Service Pack

Note: The FTP Server, Userid, Password, and Directory information received in the notification will be needed in order to FTP the SP1 code to the AIX blade.

8. Install the Service Pack using normal installation procedures.
9. After the installation completes, reboot the blade.

10. When the blade is back up, open a new terminal window and enter **oslevel –s** to verify the existing code level.

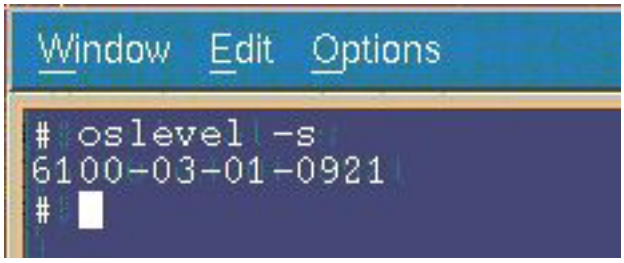


Figure 109. oslevel –s

Obtaining AIX APARs and Verifying the Installation

The following section describes how to obtain and install AIX APARs for the SAS RAID Controller Module.

About this task

For the most current information on required AIX APARs, review the *IBM SAS RAID Module Interoperability Guide* at:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5078491&brandind=5000020

Procedure

1. AIX APARs may be found in two location, BM FixCentral or the FTP APAR download site. The following describes how to access both locations.

   Location APARs on Fix Central

   a. Open a web browser to the following URL:

      http://www.ibm.com/support/fixcentral/

      The window will open the IBM Support Fix Central website.

   b. Select the following options from the corresponding lists on the Fix Central page, then click **Continue**:

Product Group:	**System p**
Product:	**AIX**
Version:	**6.1**
Fix Type:	**Fix search**

   c. Enter the desired APAR number on the Fix Search page. Select **Date: newest first**, then click **Search**.

   d. Follow the onscreen instructions to locate and download the APAR.

   Locating APARs on FTP APAR download site

   a. ftp to public.dhe.ibm.com: ftp public.dhe.ibm.com

      ```
      login: anonymous
      password: anything
      ```

   b. cd aix/efixes/izxxxxx where xxxxx = apar #

   c. type the following:

```
bin
prompt
mget *
bye
```

d. This will download 2 files: README.txt; izxxxxx.epkg.Z

2. Install the APARs using normal APAR installation procedures. Once all APAR installations are completed successfully, run the following command to verify the state of the APARs.

```
emgr –l
```

Note: All of the APARs should have a State of 'Q' for 'reboot required'. See the example in Figure 86: emgr –l command results.

```
# emgr -l

ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ============================
1   *Q*   iz52971    06/23/09 17:19:22            Fix SAS disk description
2   *Q*   iz53650    06/23/09 17:20:37            Allow more SCSI Busy status

STATE codes:
 S = STABLE
 M = MOUNTED
 U = UNMOUNTED
 Q = REBOOT REQUIRED
 B = BROKEN
 I = INSTALLING
 R = REMOVING
 T = TESTED
 P = PATCHED
 N = NOT PATCHED
 SP = STABLE + PATCHED
 SN = STABLE + NOT PATCHED
 QP = BOOT IMAGE MODIFIED + PATCHED
 QN = BOOT IMAGE MODIFIED + NOT PATCHED
 RQ = REMOVING + REBOOT REQUIRED
#
```

Figure 110. emgr –l command results

3. Reboot the blade.
4. Once the blade comes back up, run the following commands to change the working directory and check the status of the APARs again. All of the APARs should have a state of 'S' for 'Stable'.

```
cd /usr/update/apars
emgr –l
```

```
# emgr -l

ID   STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ============================
1    S     iz52971    06/23/09 17:19:22            Fix SAS disk description
2    S     iz53650    06/23/09 17:20:37            Allow more SCSI Busy status

STATE codes:
 S = STABLE
 M = MOUNTED
 U = UNMOUNTED
 Q = REBOOT REQUIRED
 B = BROKEN
 I = INSTALLING
 R = REMOVING
 T = TESTED
 P = PATCHED
 N = NOT PATCHED
 SP = STABLE + PATCHED
 SN = STABLE + NOT PATCHED
 QP = BOOT IMAGE MODIFIED + PATCHED
 QN = BOOT IMAGE MODIFIED + NOT PATCHED
 RQ = REMOVING + REBOOT REQUIRED
#
```

Figure 111. emgr –l command results after reboot

Checking System hdisk (volume) Status on AIX

This section describes how to verify the state of the AIX blade.

About this task

Once all of the necessary software updates are completed, you can assign volumes to the blade using SCM or CLI. Once the configuration completes, perform the following steps to verify the state of the AIX blade.

Procedure

1. Open a new terminal window on the AIX blade and run the following command.

   ```
   lspath
   ```

   The **lspath** command shows the available paths to the blade. If the system has an internal hard drive, for example hdisk0, will have only one path. All other hdisks will have two paths. On a JS12/JS22 blade, the hdisks will be assigned to SAS1. hdisks on JS23/JS43 blades will be assigned to SAS0. See the example below for a JS12/JS22 blade with two paths to each of 8 hdisks (LUNs).

   ```
   [root@localhost] / # lspath
   Enabled hdisk0 sas0
   Enabled hdisk1 sas1
   Enabled hdisk2 sas1
   Enabled hdisk3 sas1
   Enabled hdisk4 sas1
   Enabled hdisk5 sas1
   Enabled hdisk6 sas1
   Enabled hdisk7 sas1
   Enabled hdisk8 sas1
   Enabled hdisk1 sas1
   Enabled hdisk2 sas1
   Enabled hdisk3 sas1
   Enabled hdisk4 sas1
   Enabled hdisk5 sas1
   Enabled hdisk6 sas1
   Enabled hdisk7 sas1
   Enabled hdisk8 sas1
   ```

2. Run the following command in the terminal window:

   ```
   lsdev –Cc disk
   ```

The **lsdev –Cc** disk command shows all of the drives available to the blade. The internal hard drive on a JS12/JS22 blade is hdisk0 SAS Disk Drive. All other drives are virtual hard drives (LUNs). All of the virtual hard drives should be of type 'SAS IBM 1820 Disk'.

```
[root@localhost] / # lsdev -Cc disk
hdisk0 Available 00-08-00 SAS Disk Drive
hdisk1 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk2 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk3 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk4 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk5 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk6 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk7 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
hdisk8 Available 03-08-00 MPIO Other SAS IBM 1820 Disk
```

If the results of the **lspath** and **lsdev –Cc** disk commands match the configuration in SCM, then the blade is ready for use.

If the results of these two commands do **not** match the expected configuration, run the following commands to delete the drives and re-discover them.

a. Run the following command for each hdisk (not including the internal hard drive hdisk0 or the boot volume):

   ```
   rmdev –dl hdisk#
   ```

   Example: rmdev –dl hdisk1, rmdev –dl hdisk2, rmdev –dl hdisk3, etc.

b. When all of the hdisks are removed, run the following command to re-discover the hdisks.

   ```
   cfgmgr –v
   ```

c. When the **cfgmgr –v** command completes, run the **lspath** command from step #1 and the **lsdev –Cc** disk command from step #2 to verify that the drives reported match the expected configuration.

3. Run the following command to check the status of an hdisk.

   ```
   lsattr –El hdiskX (where X is the number of the hdisk)
   ```

```
jsblade9> lsattr -El hdisk5
PCM             PCM/friend/sasother                                 Path Control Module             Fals
e
algorithm       fail_over                                           Algorithm                       True
clr_q           no                                                  Device CLEARS its Queue on error True
dist_err_pcnt   0                                                   Distributed Error Percentage    True
dist_tw_width   50                                                  Distributed Error Sample Time   True
hcheck_cmd      test_unit_rdy                                       Health Check Command            True
hcheck_interval 60                                                  Health Check Interval           True
hcheck_mode     nonactive                                           Health Check Mode               True
max_transfer    0x40000                                             Maximum TRANSFER Size           True
pvid            0000c93aad1de1250000000000000000                    Physical volume identifier      Fals
e
q_err           yes                                                 Use QERR bit                    True
q_type          simple                                              Queuing TYPE                    True
queue_depth     5                                                   Queue DEPTH                     True
reassign_to     120                                                 REASSIGN time out value         True
reserve_policy  no_reserve                                          Reserve Policy                  True
rw_timeout      30                                                  READ/WRITE time out value       True
size_in_mb      0                                                   Size in Megabytes               Fals
e
start_timeout   60                                                  START unit time out value       True
unique_id       362136005076B0740D0FF4A27BB490000002E071820N0003IBMsas Unique device identifier     Fals
e
ww_id           6005076b0740d0ff4a27bb490000002e                    World Wide Identifier           Fals
e
jsblade9>
```

Figure 112. The status of an hdisk

Note: The lsattr –El hdiskX output above indicates that the size of the hdisk is 0 (size_in_mb 0). To see the actual size of the hdisk, run a **bootinfo –s hdiskX** command as shown below. The size displayed will be in Megabytes.

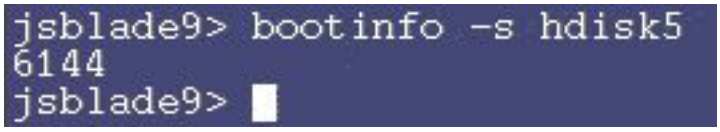


Figure 113. bootinfo –s hdiskX command

Installing VIOS on a PS / JS blade with Remote Volumes

The following section describes how to install VIOS 2.1.1 on a PS / JS blade with remote volumes.

For the most current information on supported operating systems review the *IBM SAS RAID Module Interoperability Guide*.

Creating a remote volume for the SAS boot installation

The section shows how to create a remote volume for the SAS boot installation.

About this task

Before Beginning

- Ensure the SAS RAID Modules are powered ON.
- Ensure the SAS RAID Modules are in dual controller mode and in Primary/Secondary state.

Procedure

Use the SCM or CLI create at least one volume, a boot volume, for each blade server in the BC S chassis. It is recommended that you map this boot volume as LUN 0 for each blade server. Follow the following guidelines when creating the boot volume.
The following are guidelines for creating the boot volume:

1. Ensure the volume that is used as the boot volume has enough free disk space to contain the operating system, its swap space, and any application code. The volume must also be large enough to accommodate future updates.
2. For protection against disk failure, the boot volume should be part of RAID 1, 10 or 5 storage pools. You can use a RAID 0 pool for a boot volume, however there is no protection against disk failure.
3. Even though you can create the boot volumes for all the server blades in a BC S chassis as part of the same RAID storage pools, it is recommended to split the boot volumes into at least two RAID storage pools where one pool has the SAS RAID Module in bay 3 as the preferred owner and the other pool has the SAS RAID Module in bay 4 as the preferred owner.
4. Each blade server supports a maximum of sixteen volumes. At this time, only create the volume that is going to be used as the boot volume. You can use additional volumes late on to store operating system code, swap space, application program code, and application data. If you choose to create volumes other than the boot volume at this time, do not map the additional volumes to the blade server SAS ports. You can create the additional volumes and map them to the blade server as part of the post operating system installation activities.

   Important: Map this boot volume to only **one** of the blade server SAS ports. The system presents multiple disk device entries when it sees the same boot

volume on multiple paths. For example, if the boot volume is mapped to two SAS ports, the system will present two available disks that can be used for the operating system installation. If you are not using SCM, you can obtain the WWPN of the blade server SAS port by using telnet to connect to the SAS switch component of the SAS RAID Module and running the **sasport status all** command. In Figure 88: sasport status all command output, the output of the **sasport status all** command shows the WWPN of the SAS port in blade server 1 is **500062B0000D7A10**.

Note: The blade servers must be turned on and should be at the SMS menu so that the SAS switch can discover the SAS card WWPN. Once you map the boot volume to the SAS port in the blade server, you should see the volume displayed as an hdisk in the AIX installation menu.

```
=== IBM BladeCenter(R) SAS RAID Controller Module ===
Login: USERID
Password: ********
USERID logged on
MAIN> sasport status all
ID SAS Port Name SAS Address Enable Flt Status
---+-------------------------+----------------+------
+---+--------
E1 External Port 1 True Off NoCable
PHY 1C 0000000000000000 True NoCable
PHY 1D 0000000000000000 True NoCable
PHY 1E 0000000000000000 True NoCable
PHY 1F 0000000000000000 True NoCable
E2 External Port 2 True Off NoCable
PHY 20 0000000000000000 True NoCable
PHY 21 0000000000000000 True NoCable
PHY 22 0000000000000000 True NoCable
PHY 23 0000000000000000 True NoCable
E3 External Port 3 True Off Normal
PHY 00 0000000000000000 True Normal
PHY 01 0000000000000000 True Normal
PHY 02 0000000000000000 True Normal
PHY 03 0000000000000000 True Normal
E4 External Port 4 True Off NoCable
PHY 04 0000000000000000 True NoCable
PHY 05 0000000000000000 True NoCable
PHY 06 0000000000000000 True NoCable
PHY 07 0000000000000000 True NoCable
B1 Blade Slot Connection 1 True Off Normal
PHY 1B 500062B0000D7A10 True Normal
B2 Blade Slot Connection 2 True Off Normal
PHY 1A 500062B00007CD84 True Normal
B3 Blade Slot Connection 3 True Off Normal
PHY 19 500062B0000D79F4 True Normal
B4 Blade Slot Connection 4 True Off Normal
PHY 18 500062B00007E6DC True Normal
B5 Blade Slot Connection 5 True Off NoCable
PHY 17 0000000000000000 True NoCable
B6 Blade Slot Connection 6 True Off Normal
PHY 16 500062B00007E6E0 True Normal
B7 RAID HA Connection True Off Normal
PHY 0A 5005076B07418C20 True Normal
PHY 09 5005076B07418C20 True Normal
PHY 08 5005076B07418C20 True Normal
PHY 0F 5005076B07418C20 True Normal
---+-------------------------+----------------+------+---
+--------
ID SAS Port Name SAS Address Enable Flt Status
```

Figure 114. sasport status all command output

Note: When the boot volume is created, you can specify that the storage pool with the SAS RAID Module in bay 3 (-port 0 option when creating the pool) be the preferred owner, or that the storage pool with the SAS RAID Module in bay 4 (-port 1 option when creating the pool) be the preferred owner. Regardless of this preferred owner setting, always use the WWPN of the SAS

port that is shown in the **sasport status all** command of the SAS switch in bay 3 for the initial OS installation (this is the first SAS port of the SAS card adapter). The first SAS port of a two port SAS card adapter will always have a WWPN that is one less than the WWPN of the second adapter. For example, if the first SAS port WWPN is '500062B0000D7A10', the second SAS port WWPN will be '500062B0000D7A11'.

If there is an internal hard drive installed in the blade server, you should disable it before installing the operating system on the remote boot volume.

Installing VIOS to a Volume

Complete the following steps to start the installation from an installation DVD.

Procedure

1. Insert the Installation DVD into the DVD-ROM drive in the Media Tray of the BladeCenter S chassis.
2. Connect to the Advanced Management Module (AMM) and select **Blade Tasks -> Remote Control** from the navigation menu.
3. Click **Start Remote Control** to open a Remote Control window.
4. In the Remote Control window, click the **Media Tray** list and select the Blade where you will load the new AIX operating system.
5. In the Remote Control window, click the blade list and select the blade that will be loading the operating system.
6. To begin loading the new OS, you must reboot the blade and set it to boot from the DVD-ROM drive. From the Remote Control window, select the **Power Control -> Restart**.

   Monitor the reboot of the blade from the Remote Console window.
7. As the blade reboots, press 1 to enter the SMS Menu.

   Note:

   - The menu options display for a short period of time. If it is missed reboot the blade again.
   - Some blades may require you to enter options before displaying the SMS menu option. A screen may appear asking you to enter the number 1 to choose that screen as the display. It may then ask you to enter an option to continue with the boot process, after which the option to enter the SMS menu displays as shown in Example of the SMS Main Menu figure.

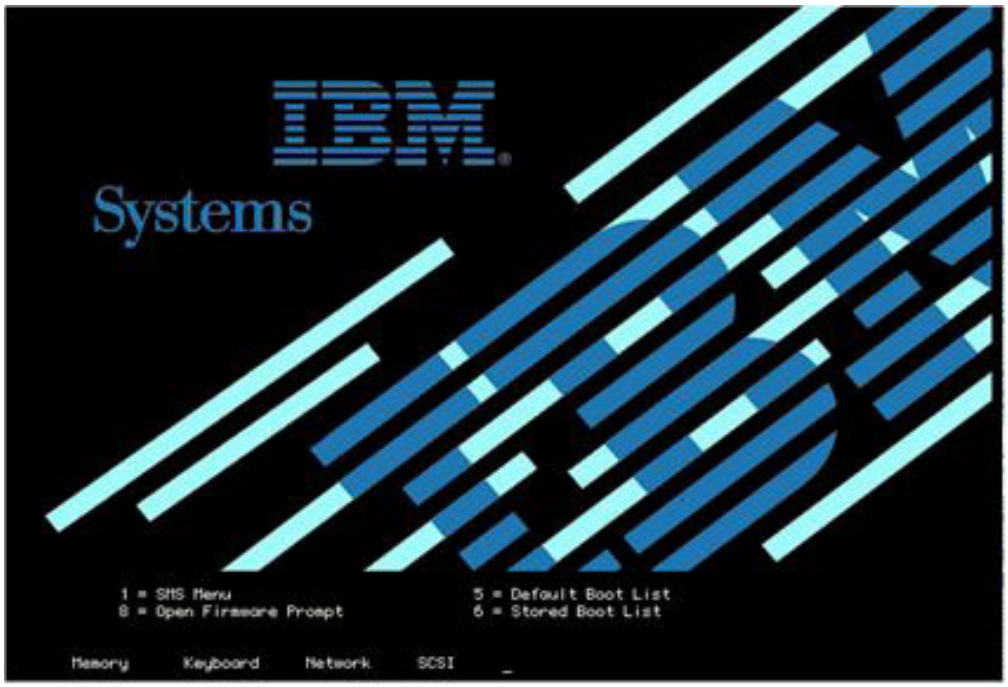


Figure 115. Reboot screen with option to enter SMS menu

```
PowerPC Firmware
Version EA340_031
SMS 1.7 (c) Copyright IBM Corp. 2000,2008 All rights reserved.
-------------------------------------------------------------------------------
Main Menu
1.   Select Language
2.   Setup Remote IPL (Initial Program Load)
3.   Change SCSI Settings
4.   Select Console
5.   Select Boot Options
6.   Firmware Boot Side Options
7.   Select Keyboard




-------------------------------------------------------------------------------
Navigation Keys:
                                                X = eXit System Management Services
-------------------------------------------------------------------------------
Type menu item number and press Enter or select Navigation key:5_
```

Figure 116. Example of the SMS Main Menu

8. From the SMS Main Menu, enter the number for the **Select Boot Options** menu and press Enter.
9. Enter the number for the **Select Install / Boot Device** menu and press Enter.
10. Enter the number for the **CD/DVD** menu and press Enter.
11. Enter the number for the **List All Devices** and press Enter.
12. A list of all available devices now loads (note this may take a little time). Enter the number of the **USB CD-ROM** device and press Enter. For this

example, the USB CD-ROM is device 3.

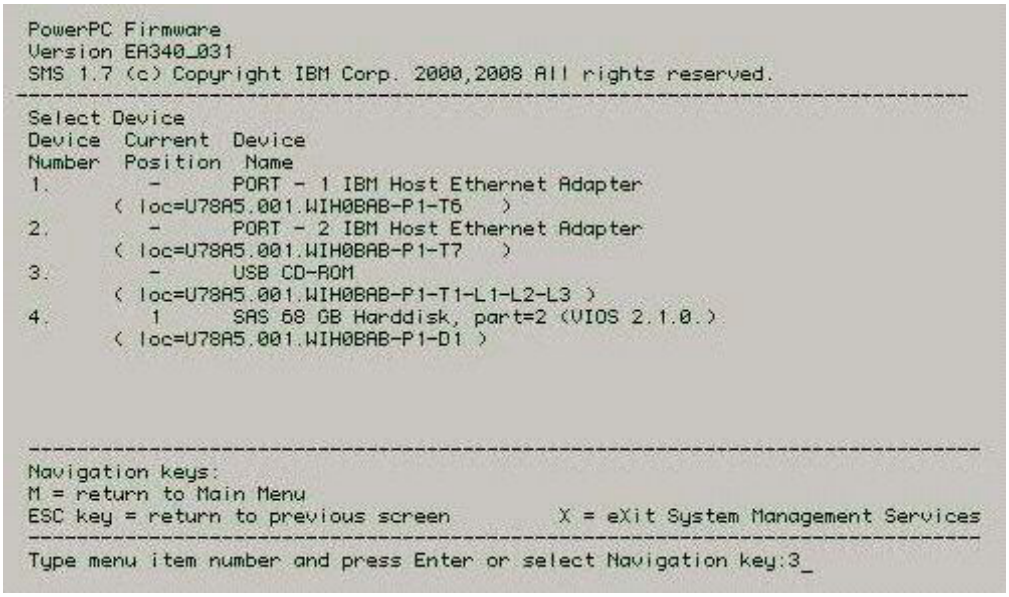


Figure 117. USB CD-ROM - device 3

13. Enter **2** for **Normal Boot Mode** and press Enter.
14. Enter **1** for **Yes** and press Enter.

    Note: It may take up to 10 minutes before the installation begins.
15. When the installation screen appears, you need to define the system console. Follow the instructions on the screen, press F1, then press Enter to use the current display as the system console.

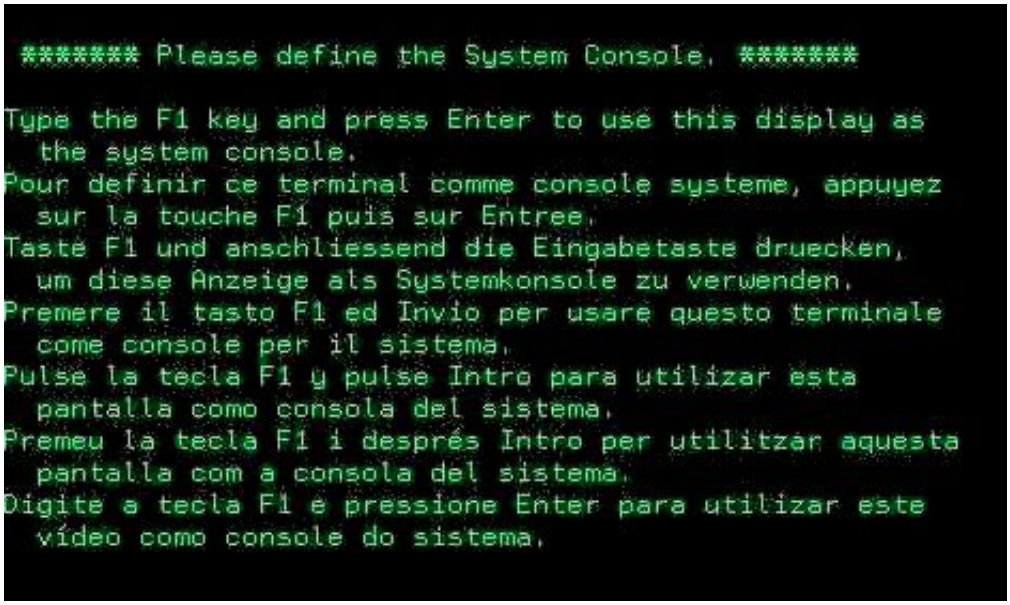


Figure 118. System console

16. To use English type the number **1** then press Enter.

17. Type the number **1** for **Install with Default Settings (recommended)** and press Enter.
18. Type the number **1** to **Continue with Install** and press Enter. Note that installation will be applied to hdisk0.

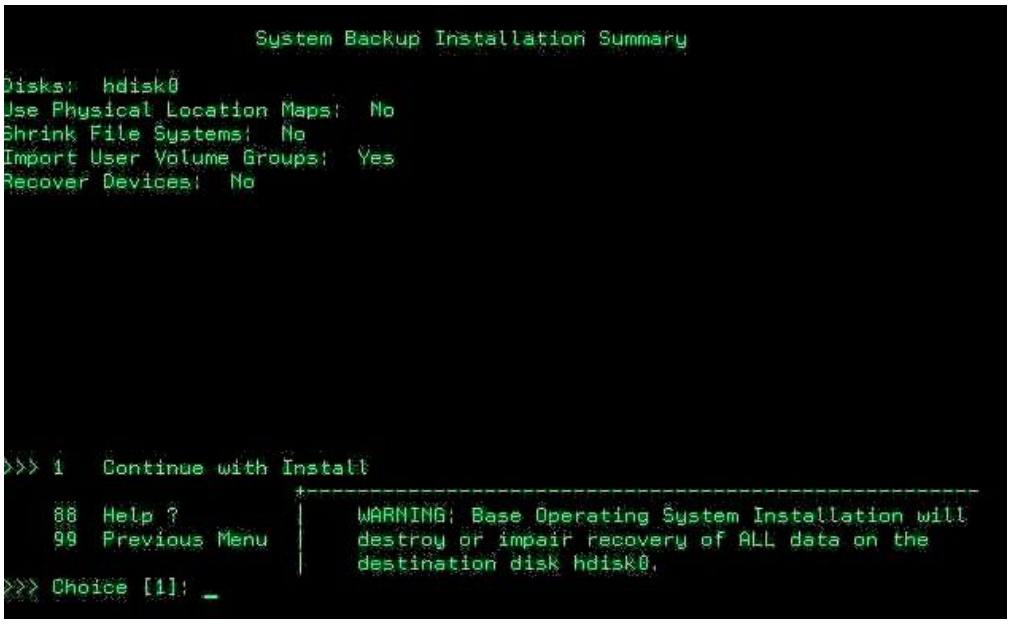


Figure 119. System backup Installation Summary

Figure 120. Installing base dperating system

19. You can monitor the installation from the screen in Figure 5.2.6. The installation takes approximately 45-60 minutes to complete. Once the installation is completed, the blade will reboot automatically.

    Note: Login will now be **padmin**.
20. Once installation is complete, use SCM or CLI to map the boot volume to the second SAS port in the blade. Create additional volumes and map them to both SAS ports.
21. To see both paths and any additional LUNs reboot the blade now.
22. To check the state of the paths and the remote volumes, run the commands from "Checking System hdisk (volume) Status on AIX" on page 119. To use the commands in that section on the VIOS OS, you must enter the AIX kernel by running the **oem_setup_env** command first.

Obtaining VIOS Fix Packs and Verifying the Installation

The following shows an example version for the VIOS Fix pack level.

About this task

For the most current information on VIOS fix packs review the *IBM SAS RAID Module Interoperability Guide*.

Open a web browser to the following URL:

http://www.ibm.com/support/fixcentral/

This opens the IBM Support Fix Central website.

Procedure

1. From the IBM Support Fix Central page, select the following options from the corresponding lists then click **Continue**:

Product Group:	**System p**
Product:	**Virtualization software**

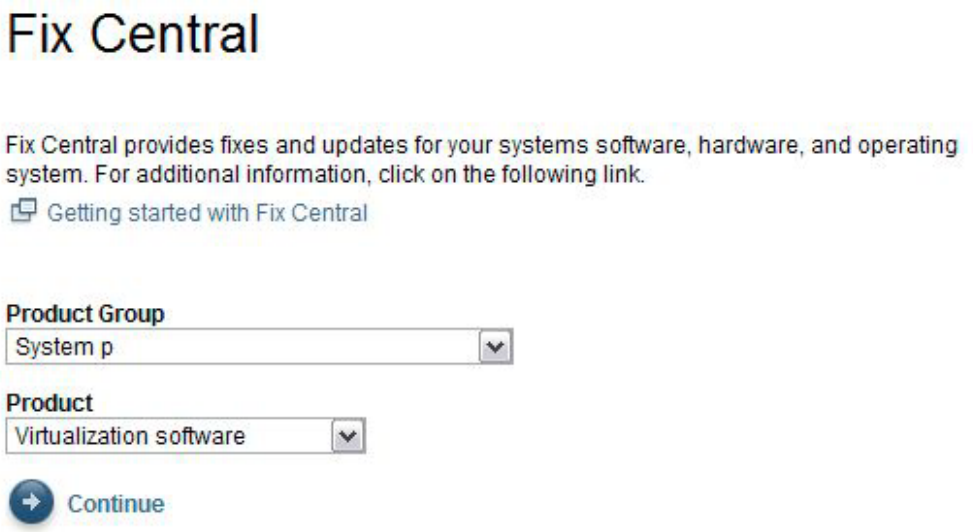


Figure 121. Fix Central search page

2. Click the link for **Virtual I/O Server**.

Figure 122. Example of VIOS code link

3. Click the link for **Download the latest VIOS V2.1 Fix Pack**.

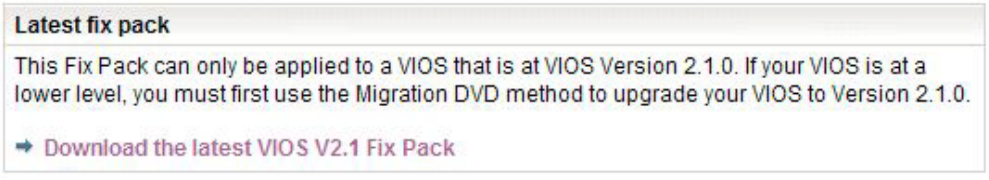
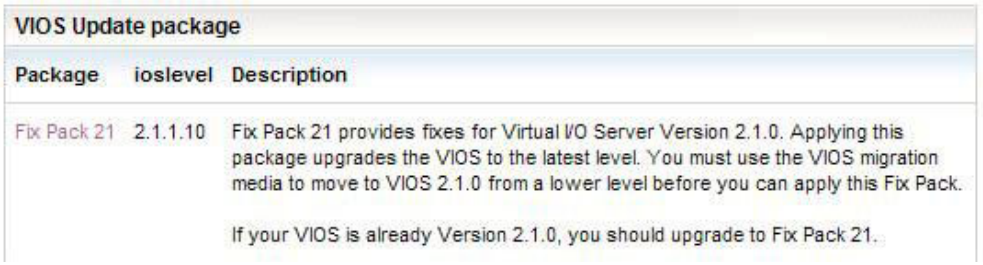


Figure 123. VIOS V2.1 Fix Pack

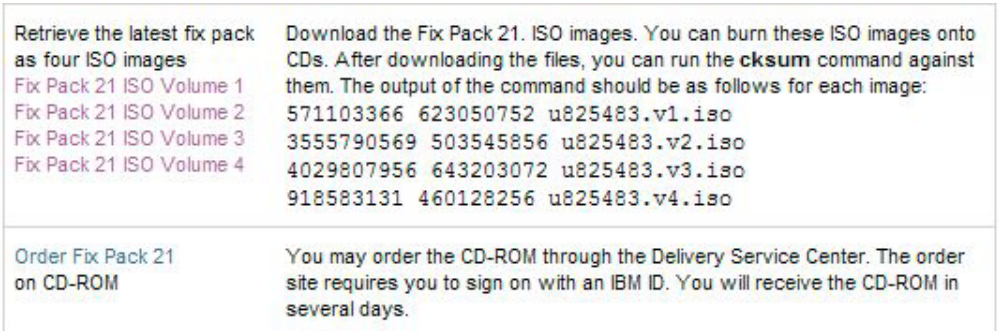
4. Click the link for **Fix Pack 21**.



VIOS Update package		
Package	**ioslevel**	**Description**
Fix Pack 21	2.1.1.10	Fix Pack 21 provides fixes for Virtual I/O Server Version 2.1.0. Applying this package upgrades the VIOS to the latest level. You must use the VIOS migration media to move to VIOS 2.1.0 from a lower level before you can apply this Fix Pack. If your VIOS is already Version 2.1.0, you should upgrade to Fix Pack 21.

Figure 124. Fix Pack 21

5. Links for the ISO images to create installation disks are located towards the end of the page.



Retrieve the latest fix pack as four ISO images Fix Pack 21 ISO Volume 1 Fix Pack 21 ISO Volume 2 Fix Pack 21 ISO Volume 3 Fix Pack 21 ISO Volume 4	Download the Fix Pack 21. ISO images. You can burn these ISO images onto CDs. After downloading the files, you can run the **cksum** command against them. The output of the command should be as follows for each image: 571103366 623050752 u825483.v1.iso 3555790569 503545856 u825483.v2.iso 4029807956 643203072 u825483.v3.iso 918583131 460128256 u825483.v4.iso
Order Fix Pack 21 on CD-ROM	You may order the CD-ROM through the Delivery Service Center. The order site requires you to sign on with an IBM ID. You will receive the CD-ROM in several days.

Figure 125. Example list of fix packs

6. Download the ISO images to a Windows based laptop or PC. Use the images to create four installation CDs.
7. Run the following command from the VIOS $ prompt to verify the level of code currently existing on the blade.

```
ioslevel
```

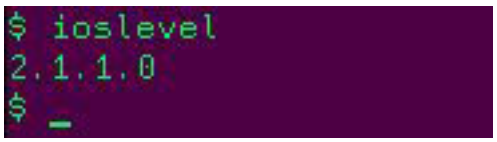


Figure 126. ioslevel

Note: The VIOS level must be at 2.1.0.0 or higher to load Fix Pack 21.

8. Install the Fix Pack using normal installation procedures. Once the Fix Pack installation completes, reboot the blade.
9. After Fix Pack 21 has been loaded and the blade has been rebooted, run the **ioslevel** command again from the VIOS $ prompt to verify the code level.

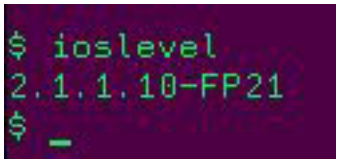


Figure 127. ioslevle - FP21

Obtaining VIOS i-fixes and Verifying the Installation

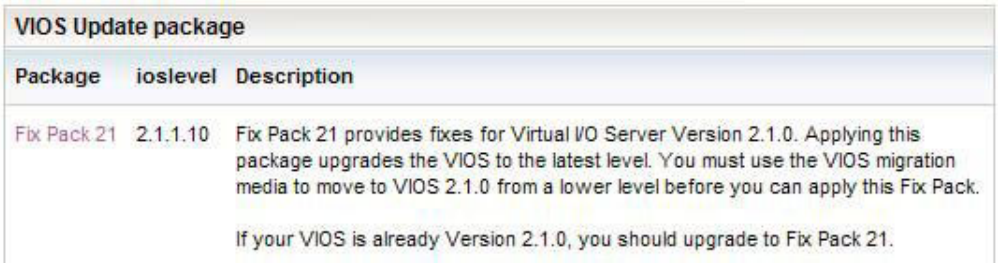
The following section shows how to obtain and install VIOS i-fix levels.

About this task

For the most current information on supported VIOS i-fix, review the *IBM SAS RAID Module Interoperability Guide* .

Procedure

1. Open a web browser to the following URL:
   http://www14.software.ibm.com/webapp/set2/sas/f/vios/home.html
   This opens the Virtual I/O Server Support for Power Systems.
2. The host blade should be at the minimum levels documented in the *IBM SAS RAID Module Interoperability Guide*.
3. Follow the links to " Download the latest VIOS V2.1 Fix Pack "
4. Click on the link for the **VIOS Update package**.



VIOS Update package

Package	ioslevel	Description
Fix Pack 21	2.1.1.10	Fix Pack 21 provides fixes for Virtual I/O Server Version 2.1.0. Applying this package upgrades the VIOS to the latest level. You must use the VIOS migration media to move to VIOS 2.1.0 from a lower level before you can apply this Fix Pack. If your VIOS is already Version 2.1.0, you should upgrade to Fix Pack 21.

Figure 128. VIOS update package

5. Search on this page for the latest i-fix. Download and install the i-fix using normal installation instructions.
6. Once all i-fix installations are completed, run the following command to verify the state of the i-fixes:
   ```
   emgr -l
   ```

   Note: All of the I-fixes should have a state of 'Q' for 'reboot required'. See the below figure.

```
# emgr -l

ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ==============================
========
1   *Q*   vios_rssm  07/01/09 23:53:17           Fixes for RSSM storage on VIOS


STATE codes:
 S = STABLE
 M = MOUNTED
 U = UNMOUNTED
 Q = REBOOT REQUIRED
 B = BROKEN
 I = INSTALLING
 R = REMOVING
 T = TESTED
 P = PATCHED
 N = NOT PATCHED
 SP = STABLE + PATCHED
 SN = STABLE + NOT PATCHED
 QP = BOOT IMAGE MODIFIED + PATCHED
 QN = BOOT IMAGE MODIFIED + NOT PATCHED
 RQ = REMOVING + REBOOT REQUIRED
# _
```

Figure 129. emgr –l command results

7. Reboot the blade.
8. Once the blade comes back up, run the following commands to change the working directory and check the status of the i-fixes again. All of the i-fixes should have a state of 'S' for 'Stable'. See the example in the figure below.

   ```
   cd /usr/update/apars
   emgr –l
   ```

```
# emgr -l

ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ==============================
========
1    S    vios_rssm  07/01/09 23:53:17           Fixes for RSSM storage on VIOS


STATE codes:
 S = STABLE
 M = MOUNTED
 U = UNMOUNTED
 Q = REBOOT REQUIRED
 B = BROKEN
 I = INSTALLING
 R = REMOVING
 T = TESTED
 P = PATCHED
 N = NOT PATCHED
 SP = STABLE + PATCHED
 SN = STABLE + NOT PATCHED
 QP = BOOT IMAGE MODIFIED + PATCHED
 QN = BOOT IMAGE MODIFIED + NOT PATCHED
 RQ = REMOVING + REBOOT REQUIRED
# _
```

Figure 130. emgr –l command results after reboot

Obtaining the PS / JS (Power / System P) Host Blade BIOS and Verifying the Installation

The following shows an example version for the PS / JS (Power / System P) host blade BIOS.

About this task

For the most current information on supported BIOS for PS / JS (Power / System P) host blades, review the *IBM SAS RAID Module Interoperability Guide*.

Procedure

1. Verify the existing level of firmware on the AIX blade. Open a terminal window on the AIX blade and enter lsmcode to display the current level. Press Enter to exit the screen.

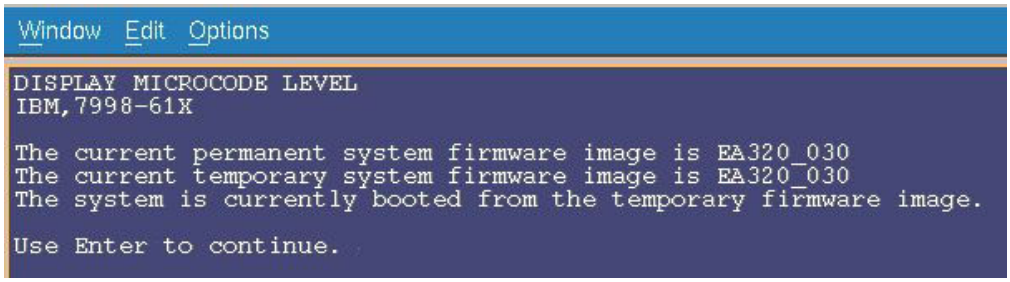


Figure 131. Display the current firmware level on the AIX blade

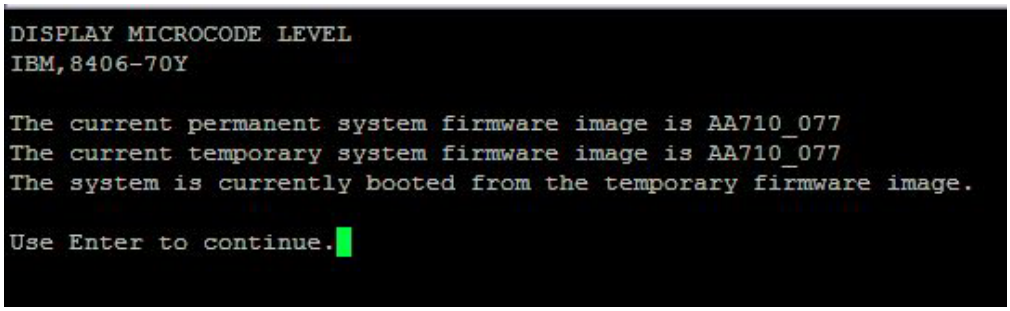


Figure 132. Display the current firmware level on the AIX PS70x blade

2. Open a web browse to the following URL:
   http://www.ibm.com/support/entry/portal/
   Under #1. Select: Search for a product and Sort by relevance.
   Type in BladeCenter to search on
   Under #2. Select: Downloads
   Under #3. Select: View your page

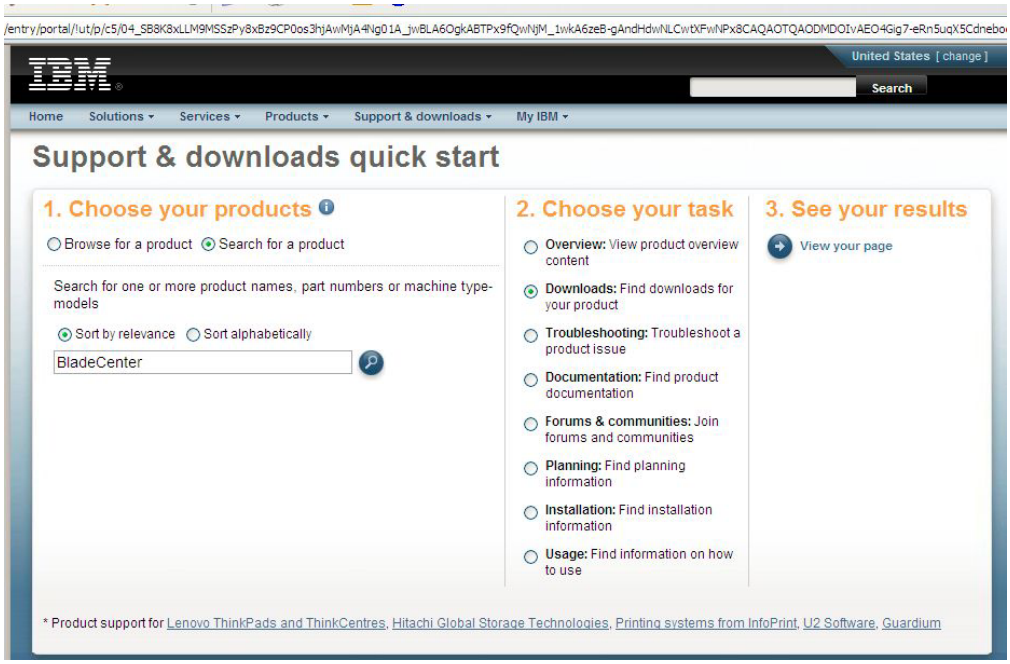


Figure 133. Support Portal View

3. Select Fix Central on the next page.

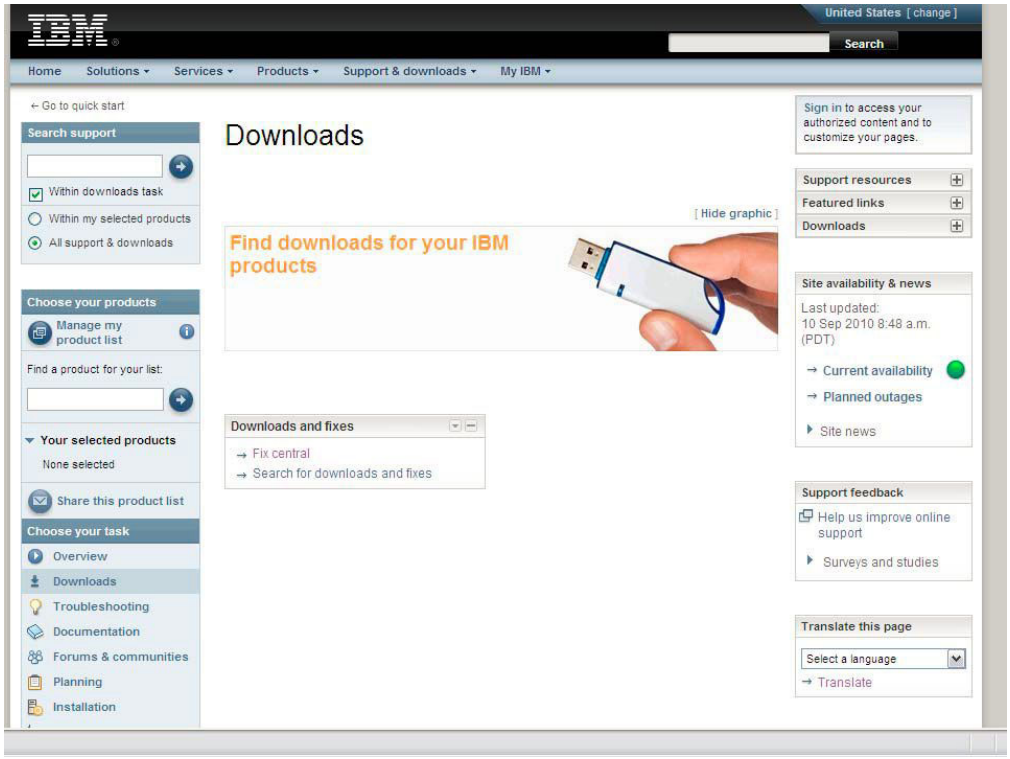


Figure 134. Fix Central View

4. Select the following options from the corresponding lists that appear:

Note: When refining the search criteria, after Operating System selection, select “Ccontinue” to get to the next screen where additional search refinements can be selected.

For PS70x blades use the following search criteria

Product Family:	**BladeCenter**
Type:	**BladeCenter PS700**
Model:	**8406**
Operating System:	**All**
Refine results:	**BIOS**

Note: The BIOS level of code will be the same for all PS700 / PS701 /PS702 blades.

For all previous JS blades use the following search criteria

Product Family:	**BladeCenter JS12**
Type:	**7998**
Model:	**All models**
Operating System:	**All**
Refine results:	**BIOS**

Note: The BIOS level of code will be the same for all JS12/JS22/JS23/JS43 blades.

5. Click Go next to the BIOS list to display a list of the most recently released code for this blade type.

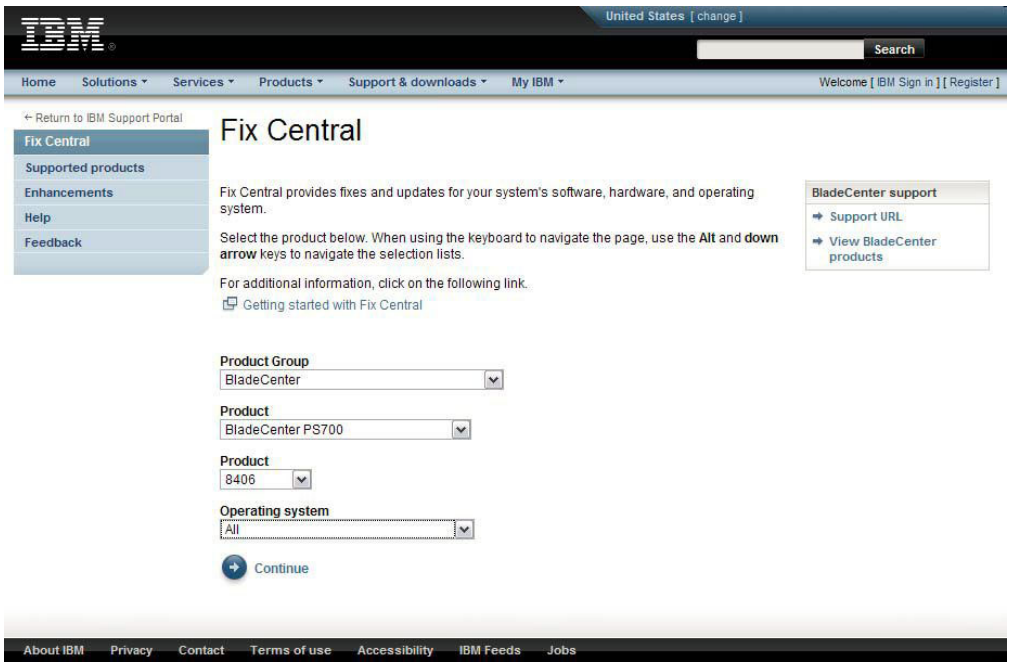


Figure 135. Fix Central Search Criteria Example

6. Select Continue.

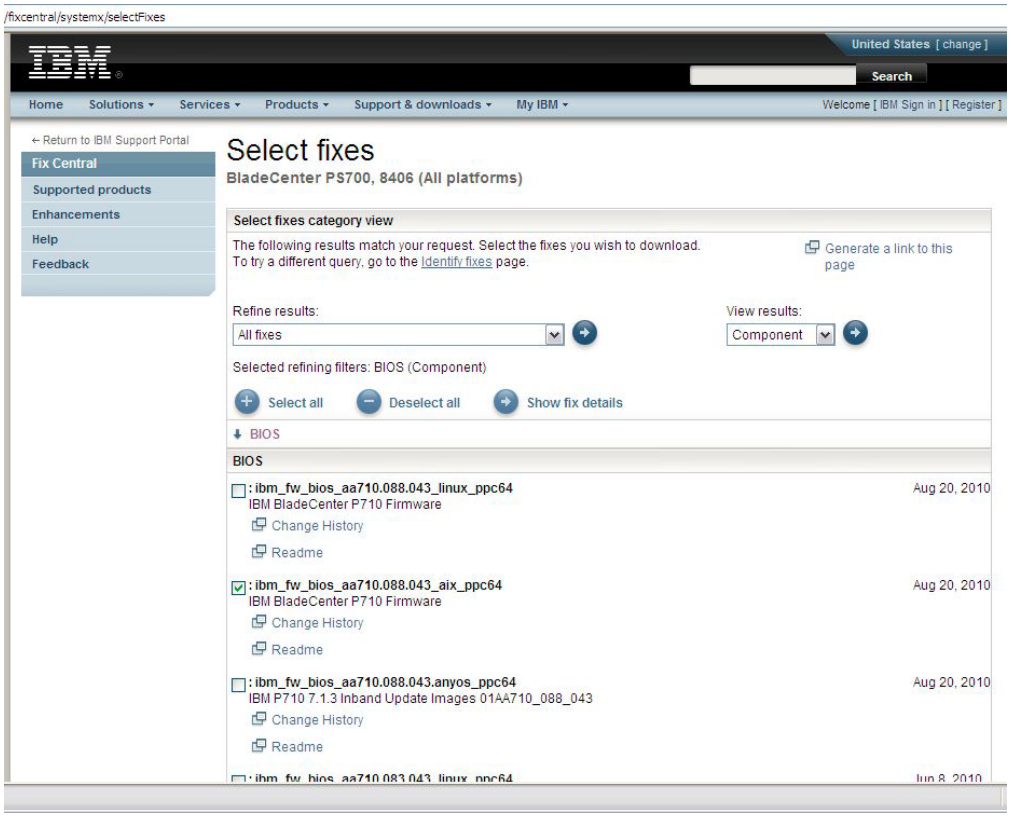


Figure 136. Selected fixes example

7. Select the aix_ppc64 installation version:
8. Select Continue to open a download window.

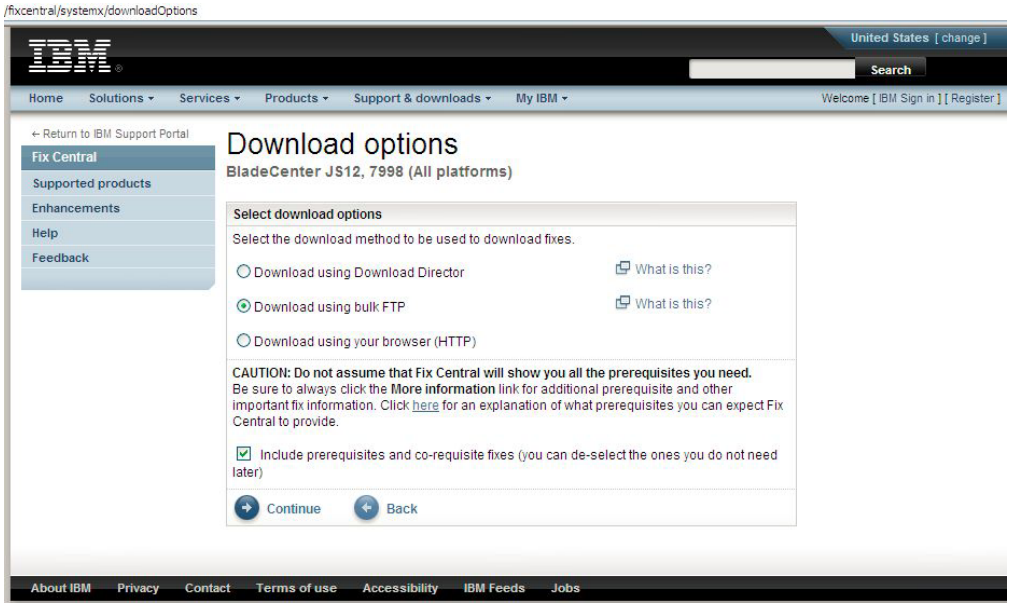


Figure 137. Download options example

9. Select continue and agree to the terms and conditions.
10. Download the image and install script.

11. Save the file to the AIX host blade.
12. Install the BIOS by running the downloaded script.

    Example for a JS blade

    ```
    chmod +x ibm_fw_bios_ea340_075_039_aix_ppc64.sh
    ./ibm_fw_bios_ea340_075_039_aix_ppc64.sh
    ```

    Example for a PS70x blade

    ```
    chmod +x ibm_fw_bios_aa710.088.043.aix_ppc64.sh
    ./ibm_fw_bios_aa710.088.043.aix_ppc64.sh
    ```

    Note: It may take a few minutes for the microcode to complete its up-grade. To view status of the Up-grade, open the AMM and navigate to the Blade Tasks -> Power/Restart menu:
13. Once installation completes and the blade reboots, run the lsmcode command again to verify the new level of BIOS.

    Note: AIX boots from the temporary image. Therefore, only the temporary image has been updated.

Figure 138. AIX terminal window showing results of lsmcod command

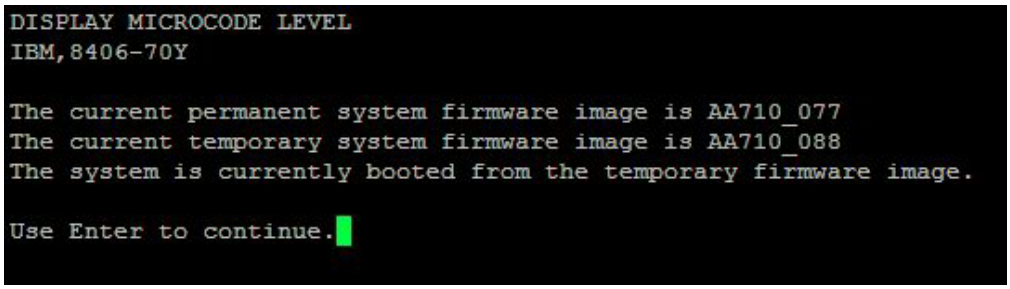


Figure 139. PS70x AIX terminal window showing results of lsmcod command

Installing SAS Integrated Controller Firmware for JS23/JS43 and PS700/PS701/PS702 Blades

This section describes how to install the SAS Integrated Controller firmware for JS23/JS43 and PS700/PS701/PS702 blades.

Obtaining SAS Integrated Controller firmware for JS23/JS43 and PS700/PS701/PS702 blades

About this task

For the most current information on supported firmware levels review the *IBM SAS RAID Module Interoperability Guide* at:

http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5078491&brandind=5000020

Procedure

1. Open a web browse to the following URL
   http://www.ibm.com/support/entry/portal/
   Under #1. Select: Search for a product and Sort by relevance.
   Type in BladeCenter to search on
   Under #2. Select: Downloads
   Under #3. Select: View your page

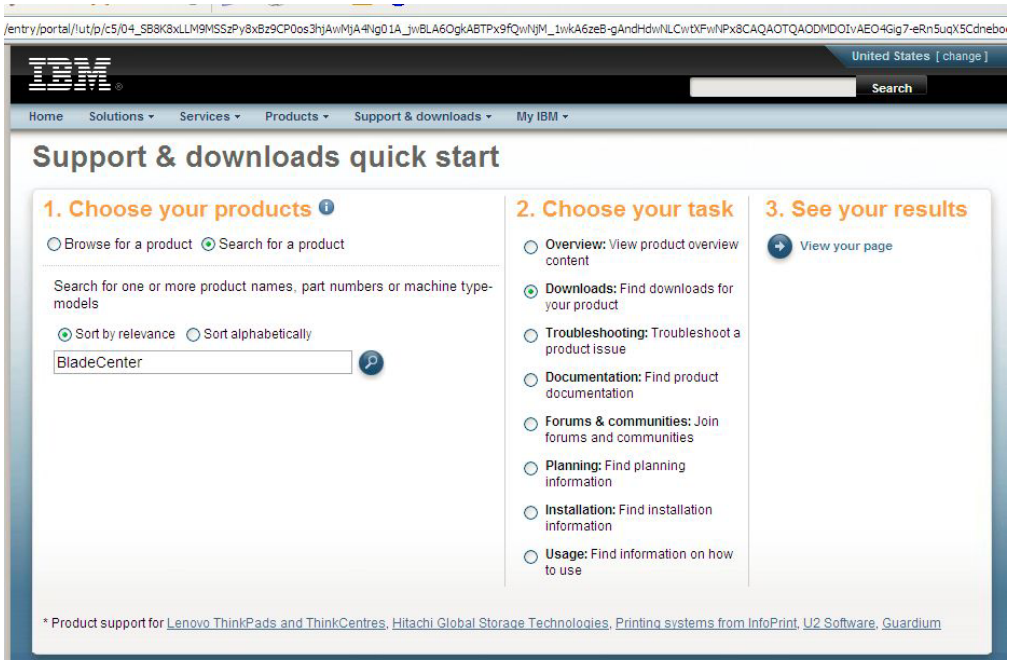


Figure 140. Support and Downlaod example

2. Select Fix Central on the next page.

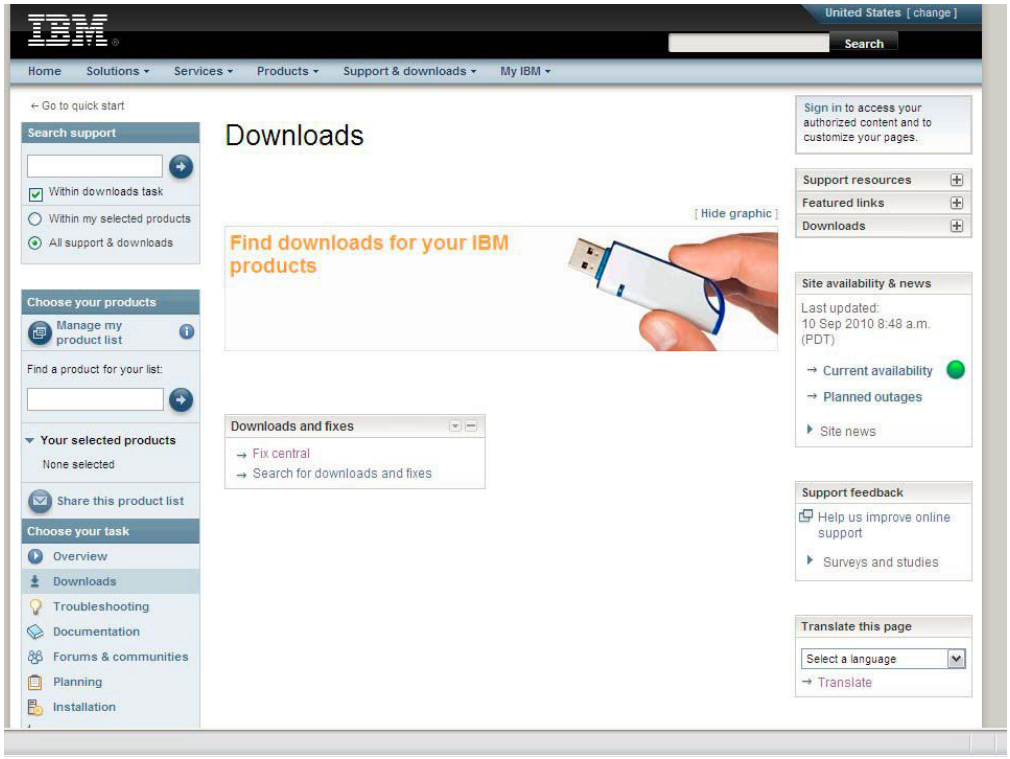


Figure 141. Fix central download example

3. Select the following options from the corresponding lists that appear:

Product Family:	**BladeCenter (JS23/JS43 PS700/PS701/PS702)**
Type:	**7778 / 8406**
Operating System:	**All**
Refine results:	**Component: SAS (Serial Attached SCSI)**

Note: The Integrated SAS Controller firmware level of code will be the same for JS23, JS43, PS700, PS701, and PS702 blades.

4. Click Go next to the Refine results list. This provides a list of recently released code for this blade type as shown in the following figure.

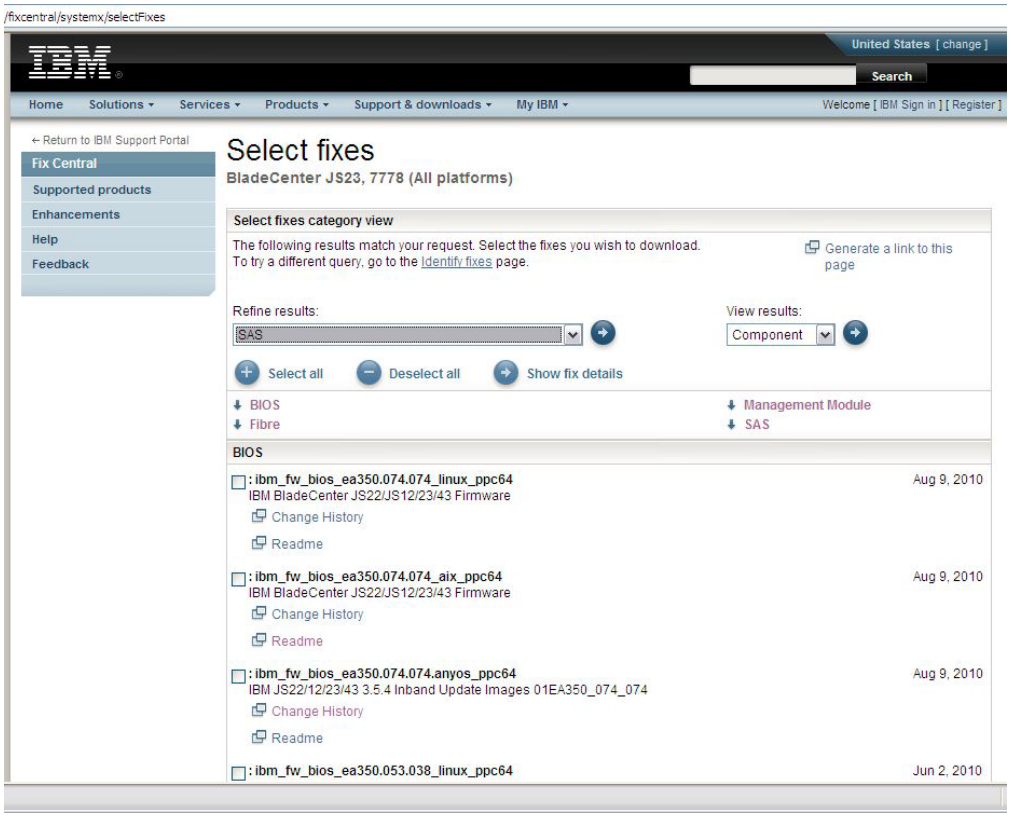


Figure 142. Example showing recent code updates for the selected blade type

5. Click on the link provided for SAS Integrated Controller. A download screen will open as seen in the example below. Download the appropriate file to /usr/lib/microcode on the AIX host blade.

Figure 143. Example SAS Integrated Controller firmware download screen

6. From the /usr/lib/microcode directory on the AIX blade, enter ls –l pci* to verify that the file was transferred.
7. Unpack the .rpm file using the following command.

```
rpm –ihv –ignoreos –force <file name>
```

Activating the SAS Integrated Controller firmware

The following section shows how to activate the SAS Integrated Controller firmware

Procedure

1. From the AIX terminal window, enter diag and press Enter to open the Diagnostics Operations application.
2. Press Enter.
3. Navigate to Task Selection and press Enter.
4. Navigate to Microcode Tasks and press Enter.
5. Navigate to Download Microcode and press Enter.
6. Navigate to /etc/microcode and press Enter.

   Note: /etc/microcode is linked to /usr/lib/microcode.
7. Navigate to sissas0 and press Enter. A plus sign (+) appears next to the selection as shown below.

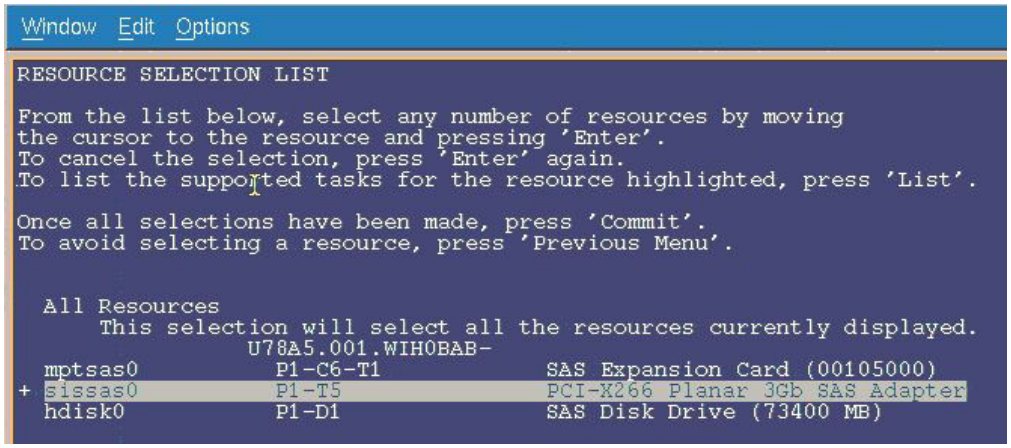


Figure 144. Select the resource to apply the firmware

8. Press F7 to Commit.
9. Press Enter.
10. Select the level to install and press Enter.

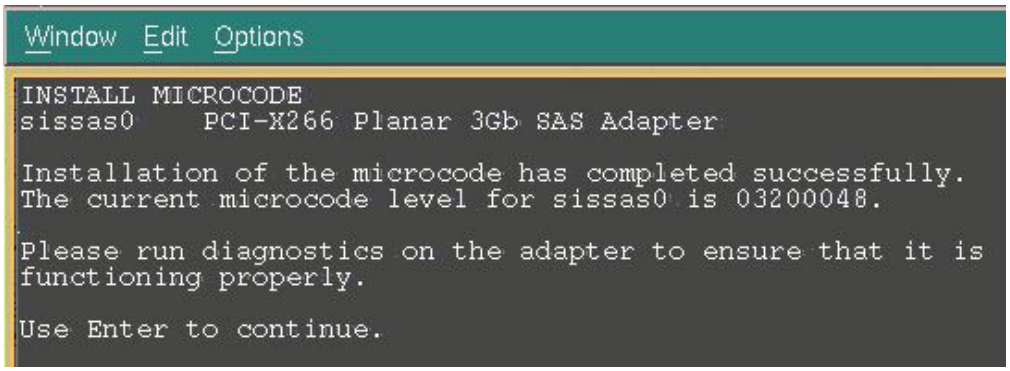


Figure 145. A message appears indicating the firmware installed successfully

11. When the download completes, press Enter to continue.
12. Press F10 to exit the Diagnostics Operations application. No reboot is required.

Verifying the installed firmware version

The following section shows how to verify the installed firmware version.

To verify the level of firmware installed, run the following command

```
# lscfg -vpl sissas0
  sissas0          U78A5.001.WIH2A24-P1-T5  PCI-X266 Planar 3Gb SAS Adapter

        ROM Level.(alterable).......03200065
        Customer Card ID Number.....57D0
        Hardware Location Code......U78A5.001.WIH2A24-P1-T5


  PLATFORM SPECIFIC

  Name:  pci1014,02BD
    Node:  pci1014,02BD@1
    Physical Location: U78A5.001.WIH2A24-P1-T5
```

Installing the SAS Expansion Card Firmware for JS12 and JS22 blades

Obtaining SAS integrated controller microcode firmware for JS12 and JS22 blades

About this task

For the most current information on supported firmware levels, review the *IBM SAS RAID Module Interoperability Guide*.

Procedure

1. Browse to the following URL

   http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020
2. Select the following options from the corresponding lists that appear:

Product Family:	**BladeCenter JS22**
Type:	**7998**
Model:	**All models**

Operating System:	**All listed operating systems**
Refine results	**Serial attached SCSI (SAS)**

Note: The SAS level of code will be the same for JS12 and JS22 blades.

3. Click **Go** next to the **Refine results** list. This provides a list of recently released code for this blade type as shown in the following figure.

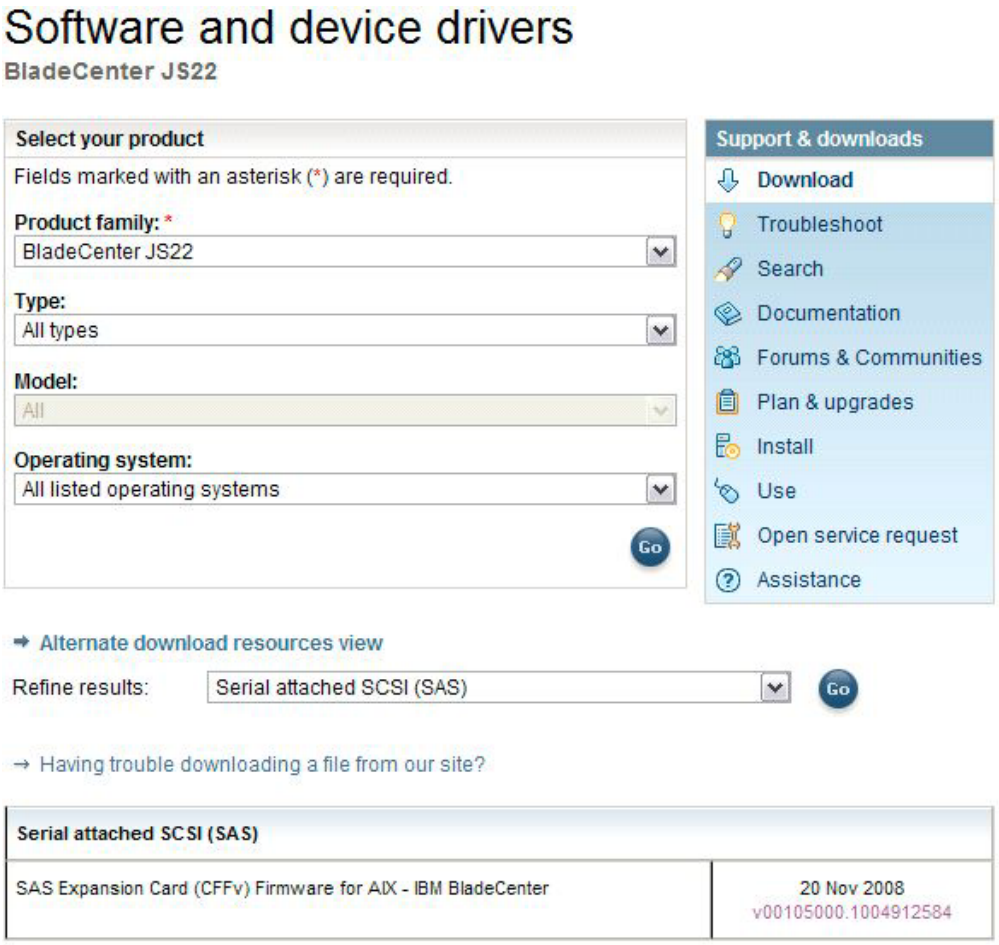


Figure 146. Example showing recent code updates for the selected blade type

4. Click the link for the latest code update to display a download page. Figure 10.1.2 shows the download page for code update v00105000.1004912584.

SAS Expansion Card (CFFv) Firmware for AIX - IBM BladeCenter

Applicable countries and regions

Systems supported:

- IBM BladeCenter JS12 (7998)
- IBM BladeCenter JS21 (7988, 8844)
- IBM BladeCenter JS22 (7998)

File details

Version: 00105000.1004912584
Release Date: 2008-11-20

File link	File size	File description
00105000.1004912584	307200	SAS Expansion Card (CFFv) Firmware for AIX
ibm_fw_mptsas_bc-sasexp-00105000.1004912584_aix.chg	624	CHANGE HISTORY for SAS Expansion Card (CFFv) Firmware for AIX
ibm_fw_mptsas_bc-sasexp-00105000.1004912584_aix.txt	3707	README for SAS Expansion Card (CFFv) Firmware for AIX

Figure 147. Download page for code update v00105000.1004912584

5. Click the link for the SAS Expansion Card (CFFv) Firmware for AIX and download the file to /usr/lib/microcode.
6. From the AIX blade desktop, open a terminal window and run the following command to change directory:

   ```
   cd /usr/lib/microcode
   ```

7. Enter ls –l and press Enter. You should see the file in the results that display.

```
Window  Edit  Options
-r--r--r--    1 root     system       888368 Jun 30 2007  ibmsis570B.img
-r--r--r--    1 root     system        41472 Jun 30 2007  sxbios
-r--r--r--    1 root     system        31232 Jun 30 2007  sxfep
# ls -l
total 13648
-rw-r-----    1 root     system       307200 Jun 07 01:06 00105000.1004912584
-r--r--r--    1 root     system        20176 Jun 30 2007  cx_conc
-r--r--r--    1 root     system        20768 Jun 30 2007  cx_e_conc
-r--r--r--    1 root     system        28672 Oct 03 2007  cxpabios
-r--r--r--    1 root     system        36864 Oct 03 2007  cxpafep
-r-xr-xr-x    1 bin      bin           99995 Jun 30 2007  dgr0871014d.00.00
-r-xr-xr-x    1 bin      bin          197089 Aug 23 2007  dgr0b91014d.00.00
-r-xr-xr-x    1 bin      bin          267973 Aug 23 2007  dgr0c91014d.00.00
-r-xr-xr-x    1 bin      bin          316207 Jun 30 2007  dgr0d31014d.00.00
-r-xr-xr-x    1 bin      bin           99095 Jun 30 2007  dgr0f81014d.00.00
-r--r--r--    1 bin      bin           74920 Aug 23 2007  ec8fd.00.03
-r--r--r--    1 root     system      1296532 Oct 03 2007  ibmsis2780.img
-r--r--r--    1 root     system       894684 Jun 30 2007  ibmsis5702.img
-r--r--r--    1 root     system      1254980 Jun 30 2007  ibmsis5703.img
-r--r--r--    1 root     system      1254980 Jun 30 2007  ibmsis5709.img
-r--r--r--    1 root     system       888368 Jun 30 2007  ibmsis570B.img
-r--r--r--    1 root     system        41472 Jun 30 2007  sxbios
-r--r--r--    1 root     system        31232 Jun 30 2007  sxfep
#
```

Figure 148. AIX terminal window showing results of ls -l command, including firmware file

Activating the SAS Expansion Card firmware

The following section shows how to activate the SAS Expansion Card firmware.

Procedure

1. From the AIX terminal window, enter **diag** and press Enter to go to the Diagnostics Operations application.
2. Press Enter.
3. Navigate to **Task Selection** and press Enter.
4. Navigate to **Microcode Tasks** and press Enter.
5. Navigate to **Download Latest Available Microcode** and press Enter.
6. Navigate to /etc/microcode and press Enter.
7. **Note**: /etc/microcode is linked to /usr/lib/microcode.
8. Navigate to **mptsas0** and press Enter. A plus (+) sign appears next to **mptsas0** as shown in the following figure.

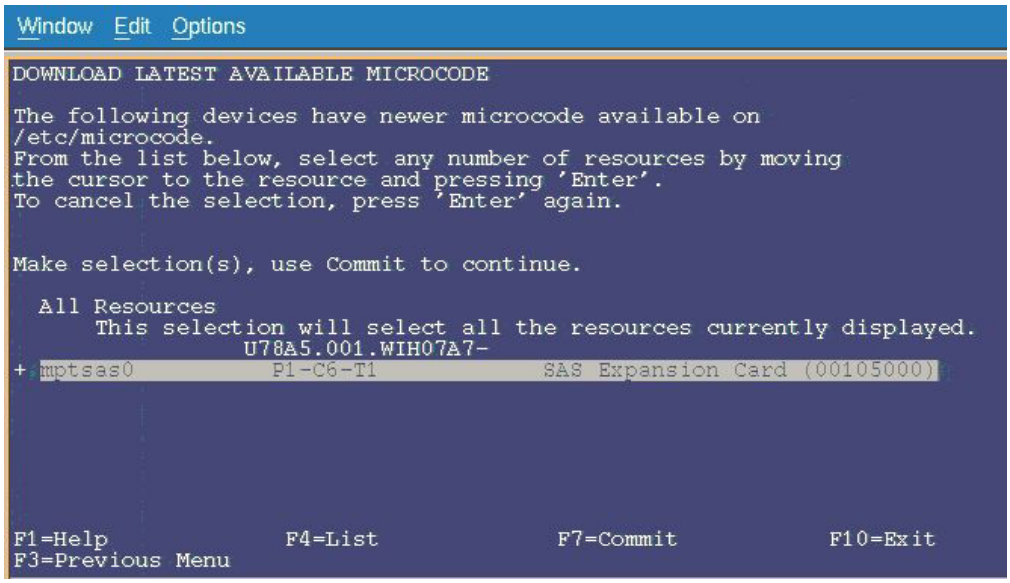


Figure 149. Select the resource to apply the firmware

9. Press F7 to begin the update. When the installation completes, a message similar to the following figure.

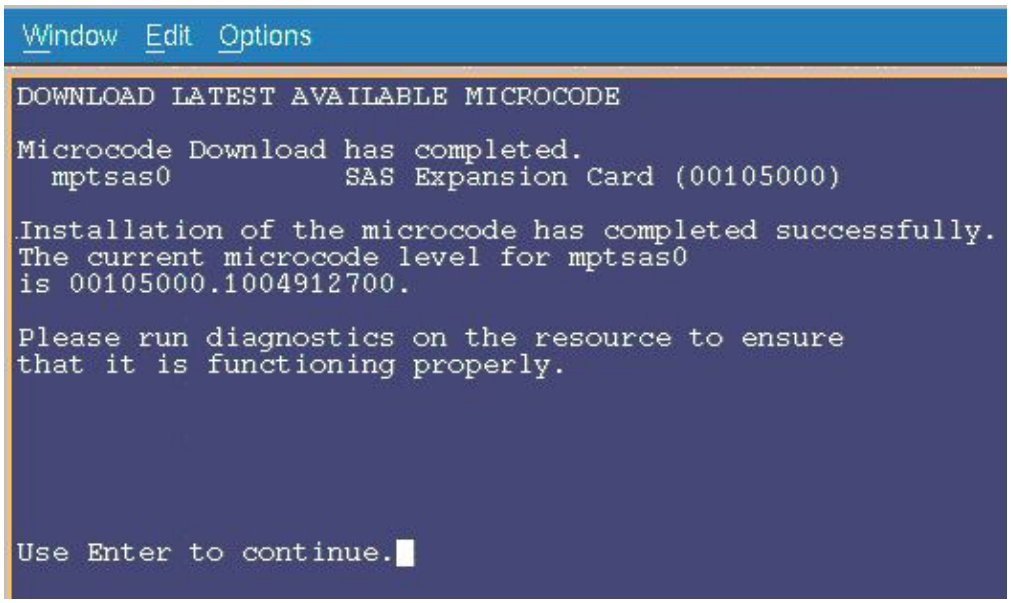


Figure 150. Message indicating that the firmware installed successful

10. Press Enter to see a summary screen.
11. Press F10 to exit the Diagnostics Operations application. No reboot is required.

Verifying the installed firmware version

To verify the level of firmware installed, run the following command.

```
# lscfg -vpl mptsas0
mptsas0 U78A5.001.WIH1970-P1-C10-T1 SAS Expansion Card (00105000)

ROM Level.(alterable).......1004912782
Device Specific.(Z0)........2701
Hardware Location Code......U78A5.001.WIH1970-P1-C10-T1


PLATFORM SPECIFIC

Name: pci1000,50
Model: LSI,1064
Node: pci1000,50@1
Physical Location: U78A5.001.WIH1970-P1-C10-T1
```

Appendix A. Appendix A: Configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host

The following section describes how to configure a SAS HBA BIOS on x86-64 (Intel or AMD) host.

This configuration is to allow for each host to perform error handing correctly when one of the SAS RAID Controller Modules has to be shutdown. This shutdown can occur during a failure condition, during concurrent code updates, or during user initiated service actions. It is required for proper operation that the following settings be applied to any System X host blade connected to an IBM BladeCenter S SAS RAID Controller Module.

Note:

- These configuration procedures are not required for PS/JS (Power/System p) host blades running AIX or VIOS.
- The following firmware versions shown in the figures are only for example, the current firmware may be at a later version.

For HS23/HS23E, you have to add the Legacy Only flag before configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host.

To add the Legacy Only flag to the boot order list, complete the following steps:

1. Restart the server and press F1 to start the Setup utility.
2. Select **Boot Manager**.
3. Select **Add Boot Option** or **Add WOL Boot Option**.

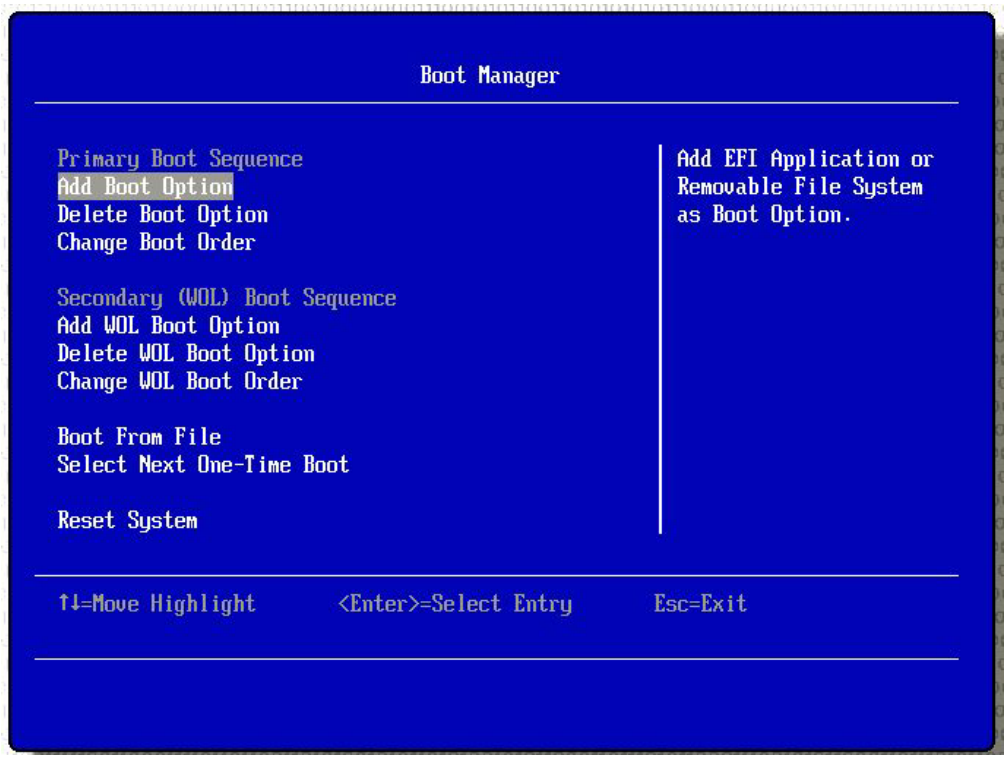


Figure 151. Add boot option

4. Select **Legacy Only** and press Enter. The Legacy Only flag is added to the end of the boot order list.

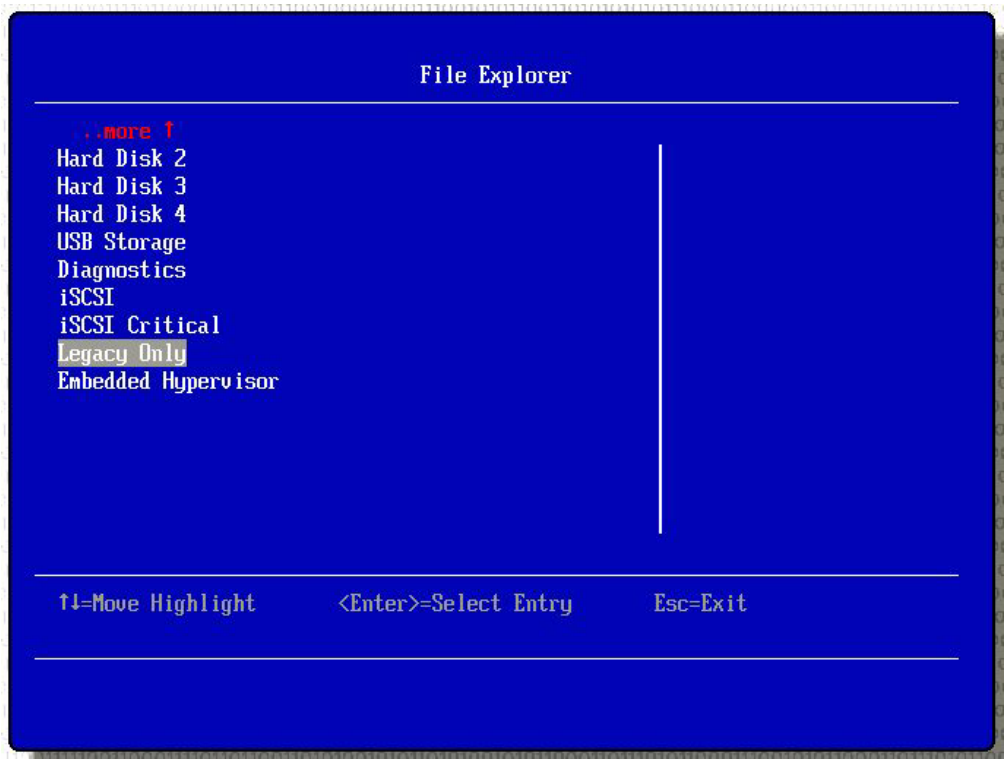


Figure 152. Legacy only

5. Select **Change Boot Order** or **Change WOL Boot Order** and press **Enter**.

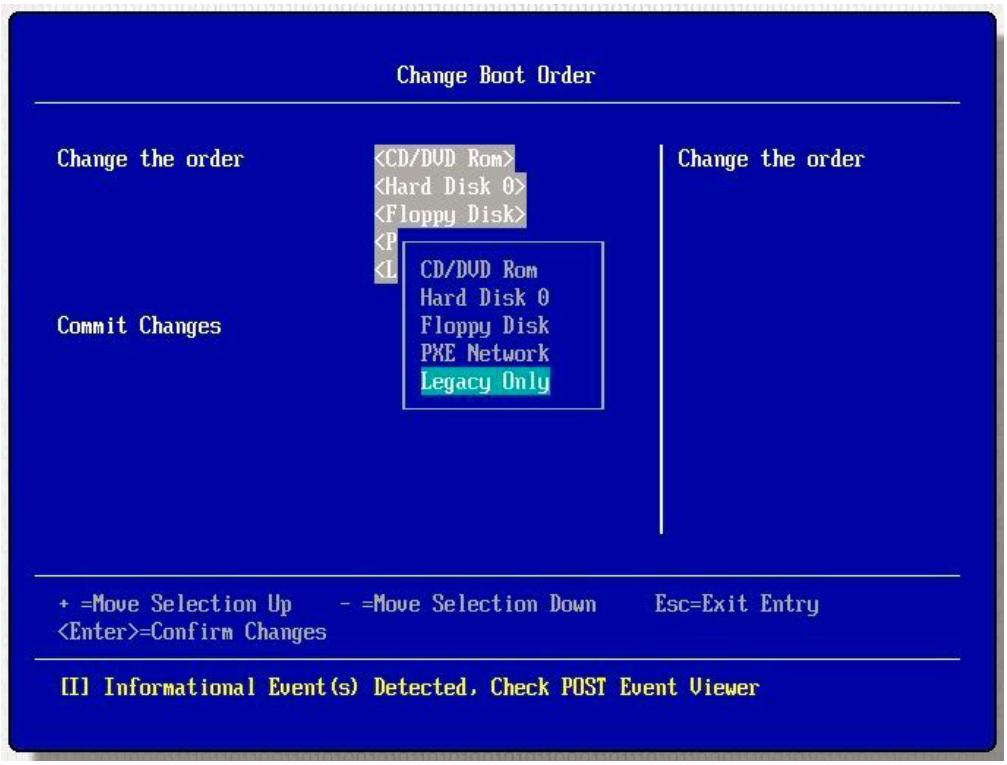


Figure 153. Legacy only

6. Highlight **Legacy Only** and press + until the Legacy Only flag is above the first boot target to which the Legacy Only flag applies. Press **Enter**.
7. Select **Commit Changes** and press **Enter**.
8. Exit from the Setup utility.

Configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host, complete the following steps:

1. Reboot the blade server.

   The following two figures must be pressed to enter SAS configuration menu, are examples of the boot sequence. Ctlr-C must be pressed to enter the SAS 1064 configuration screen.

   Note: Some blades will show only one “Searching for devices” line

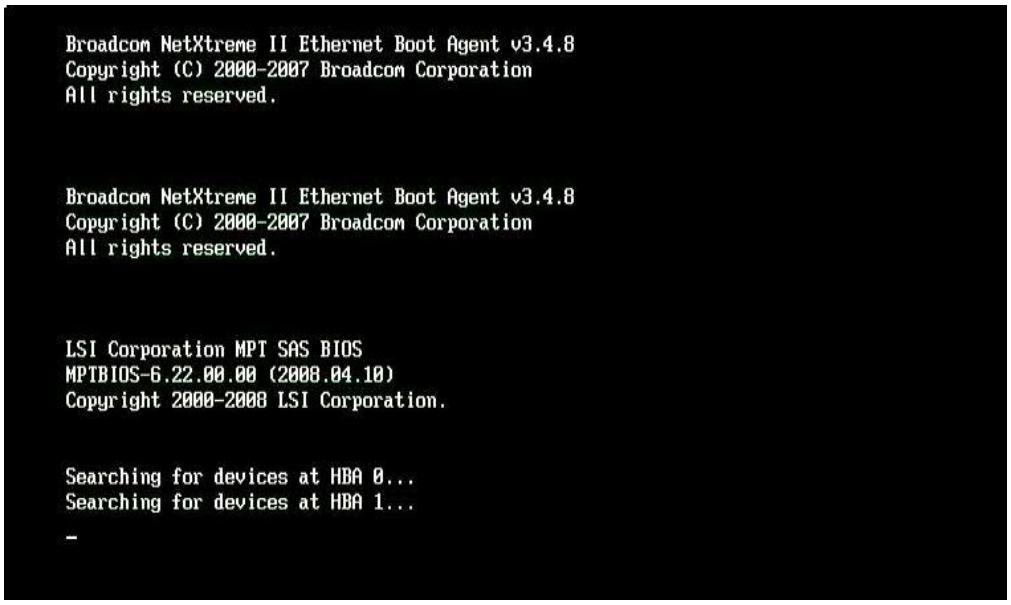


Figure 154. Example Boot Screen

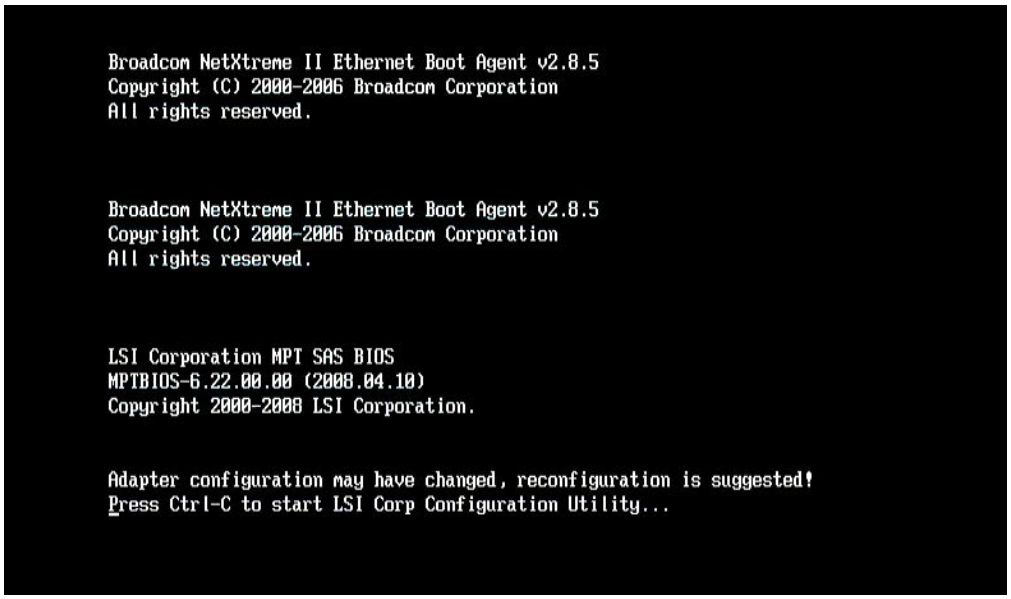


Figure 155. Screen where Ctrl-C must be pressed to enter SAS configuration menu

2. Enter the LSI Adapter BIOS configuration menu, by pressing the CTRL-C at the SAS configuration prompt during system boot. For blades with an enabled internal SAS planer and a SAS daughter card the screen will be similar to Screen where Ctrl-C must be pressed to enter SAS configuration menu figure. In Blade with Internal SAS Planer enabled and SAS Daughter card figure below, the external SAS daughter card is the top line, 'SAS3020XD'. The adapter name may vary depending on the particular blade model and daughter card version. To determine which line is for the external SAS daughter card the internal SAS planar can be temporarily disabled in by pressing F1 during boot. This will remove the internal SAS planer from the SAS configuration page, so that the remaining line will be for the SAS daughter card. HS20 and LS20 blade types will only have a single SAS entry by default because the internal hard

drive is connected with SCSI and therefore there is no internal SAS planar.

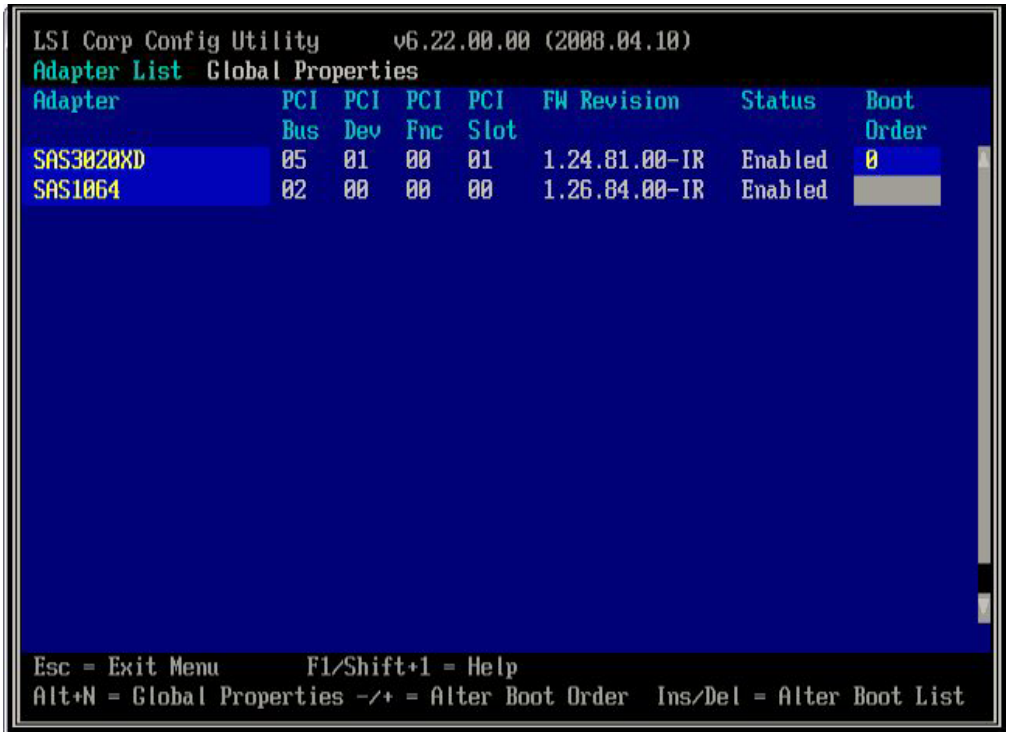


Figure 156. Blade with Internal SAS Planer enabled and SAS Daughter card

3. Select the appropriate SAS adapter and press the Enter key to enter the card configuration page.

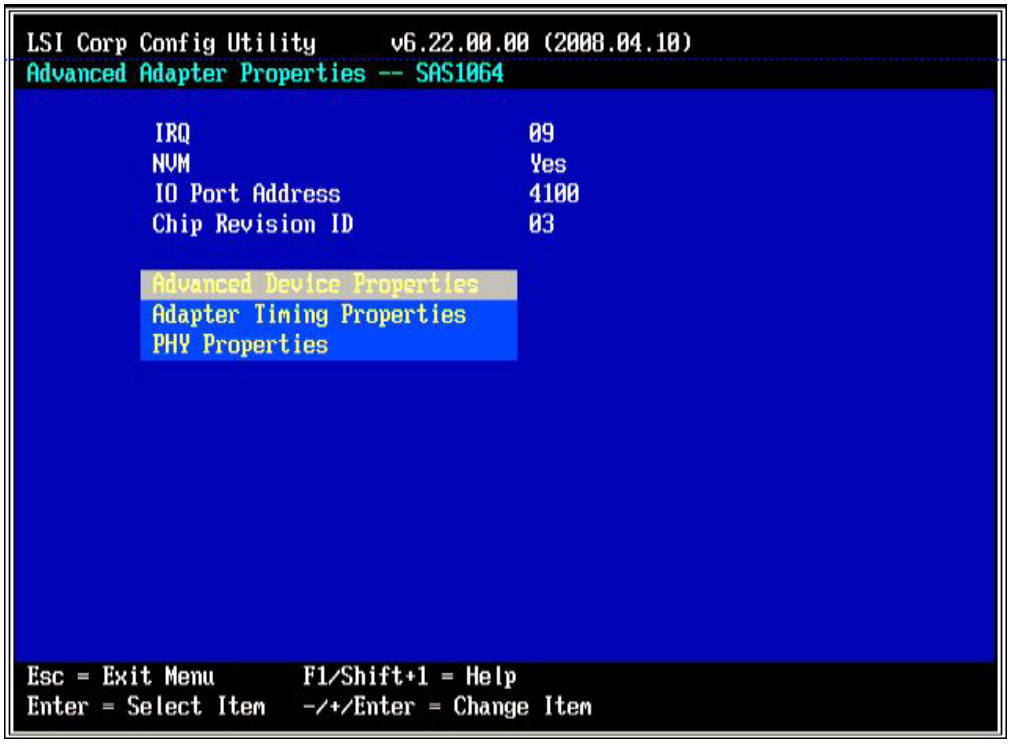


Figure 157. Setting Advanced Adapter Properties

4. Select 'Advanced Adapter Properties' and press enter to set the Block Device Timeout values. The following figure shows the setting values. The Timeout for Block Devices should be 30, all other timeout values on this page should be 10.

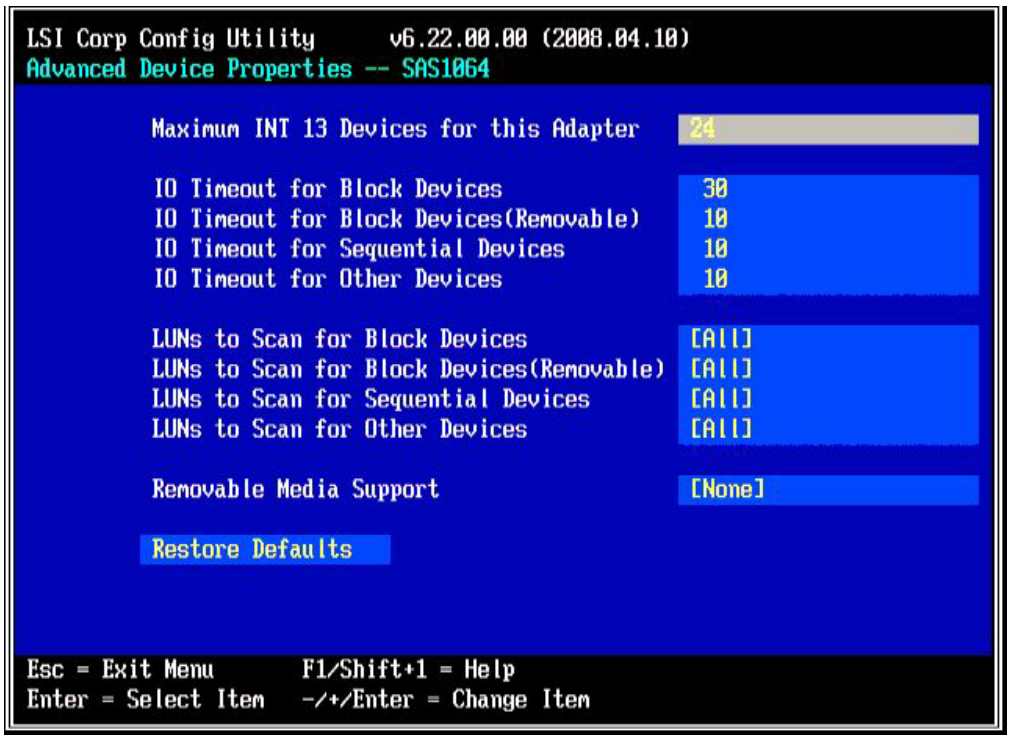


Figure 158. Setting for Block Device Timeouts

5. Back out to the previous menu and select the 'Adapter Timing Properties' option.

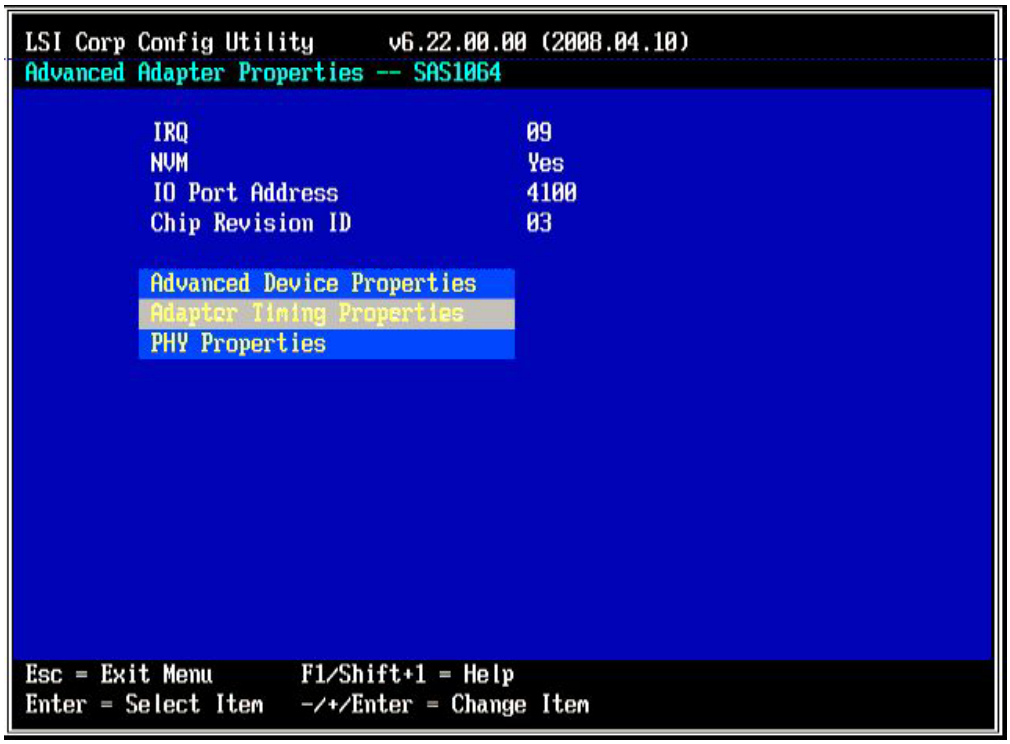


Figure 159. Selecting the Adpater Timing Properties menu option

6. Edit the 'Adapter Timing Properties' for the specific operating system being configured.
   a. For Linux, set the 'Report Device Missing Delay' to 30 and the 'I/O Device Missing Delay' to 30 in the 'Adapter Timing Properties' page as shown below.

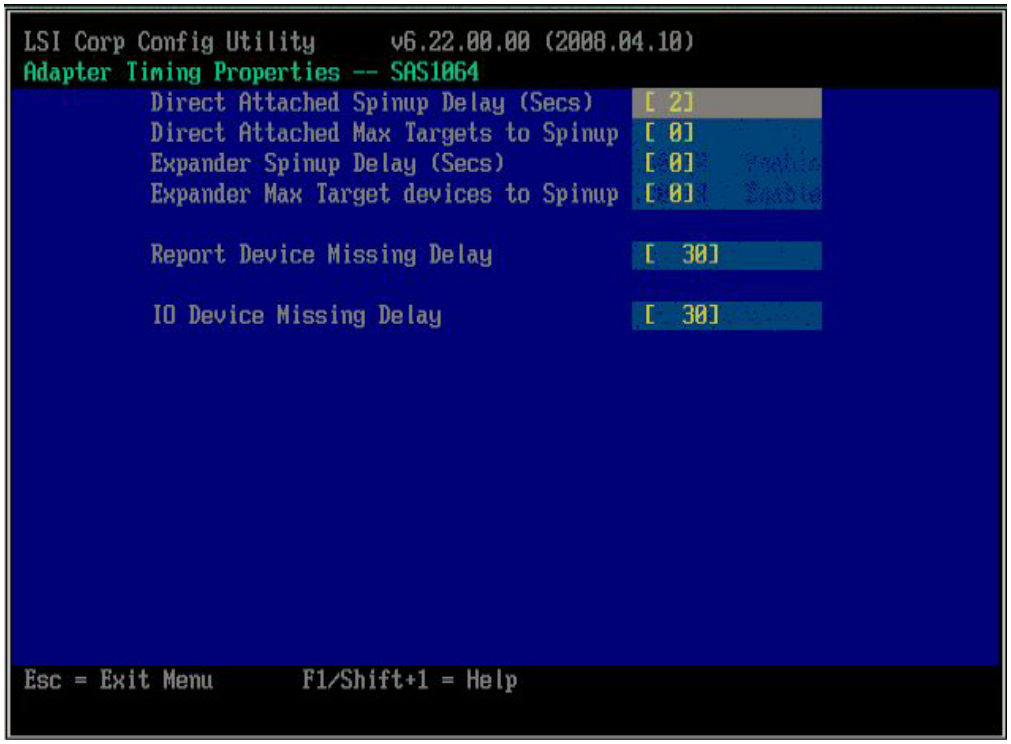


Figure 160. SAS 1064 adapter timing properties for Linux

Note: For Blades using LSI SAS 2004 HBA (e.g. HS23 and HS23E), set the "Report Device Missing Delay" to 30 and the "IO Device Missing Delay" to 8 in the Adapter Timing Properties.

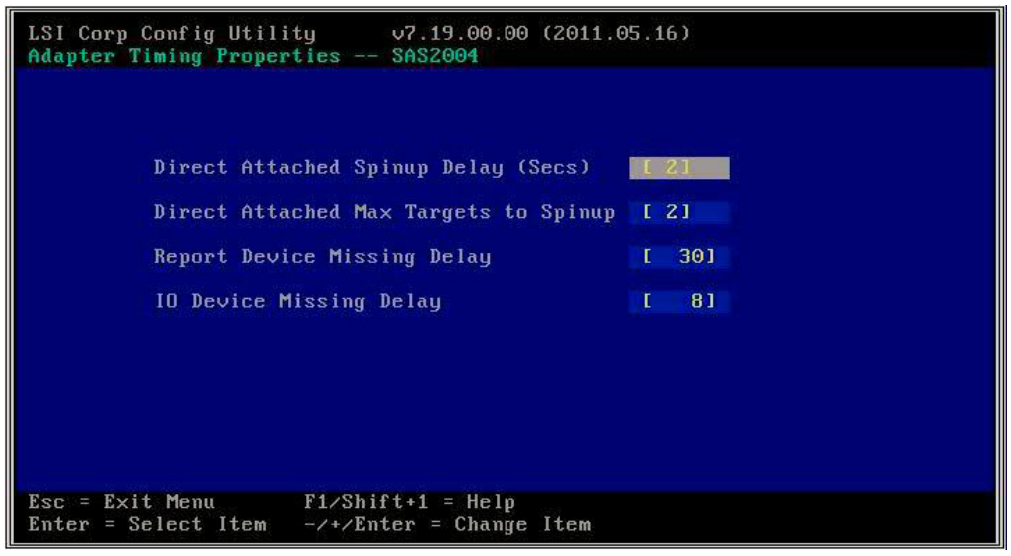


Figure 161. SAS 2004 adapter timing properties for Linux

b. For Windows, set the 'Report Device Missing Delay' to 144 and the 'I/O Device Missing Delay' to 8 in the 'Adapter Timing Properties' page as shown below.

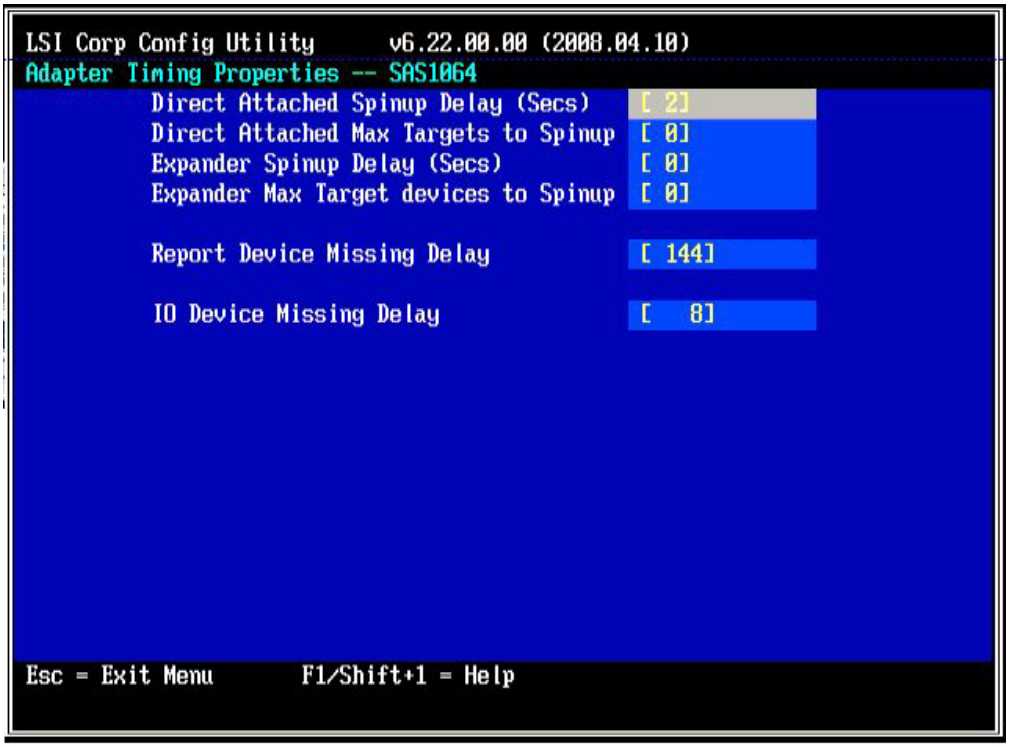


Figure 162. SAS 1064 Adapter timing properties for Windows

Note: For Blades using LSI SAS 2004 HBA (e.g. HS23 and HS23E), set the "Report Device Missing Delay" to 30 and the "IO Device Missing Delay" to 8 in the Adapter Timing Properties.

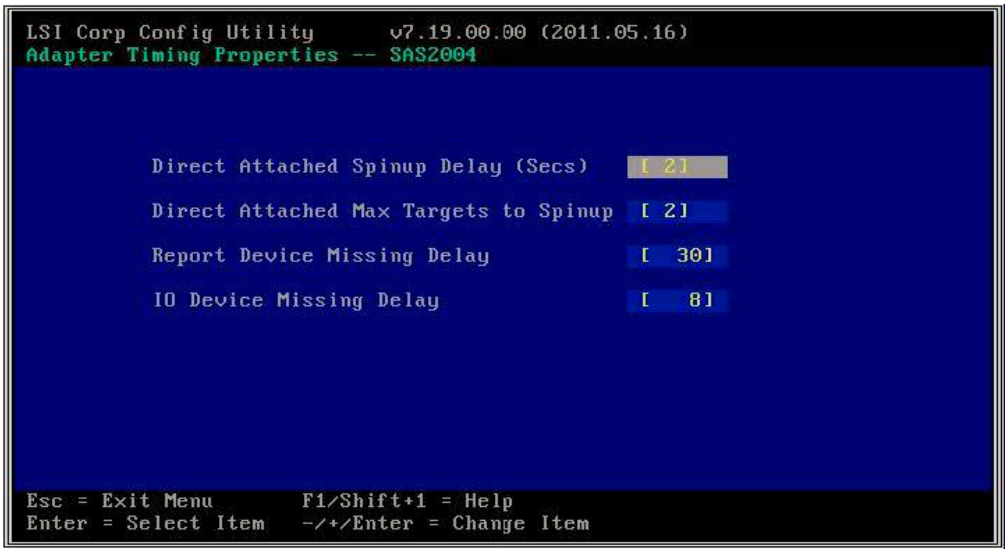


Figure 163. SAS 2004 Adapter timing properties for Windows

c. For VMware, set the 'Report Device Missing Delay' to 0 and the 'I/O Device Missing Delay' to 0 in the 'Adapter Timing Properties' page as shown below.

Figure 164. SAS Adapter timing properties for VMware

7. Use the ESC key to back out of the menus until asked to save the values, save them and then use the arrow keys to select the Exit the Configuration Utility and Reboot option, and press the enter key.

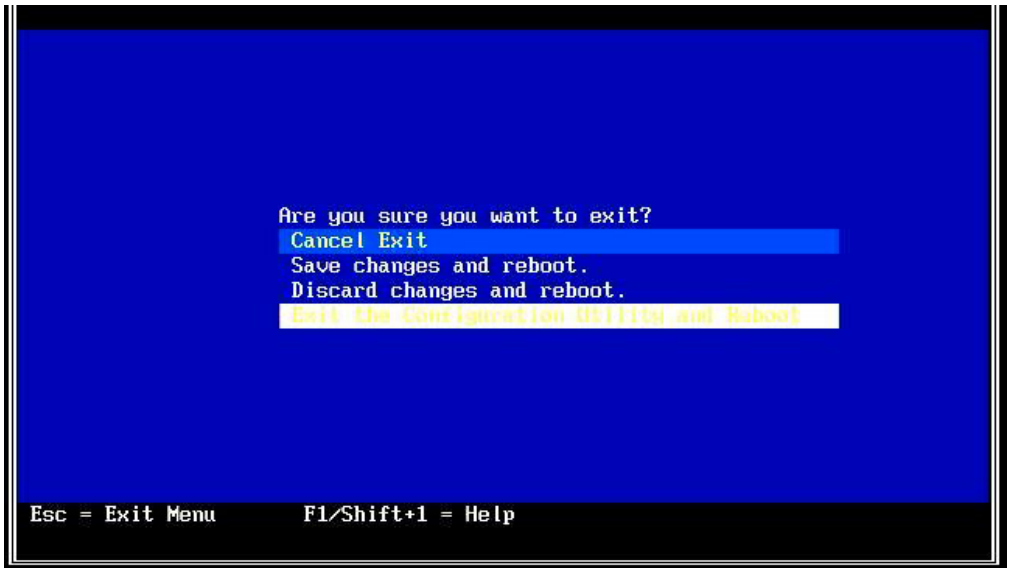


Figure 165. Saving the BIOS setting and rebooting

Appendix B. Appendix B: SAS Boot Pre-Operating System Installation Activities

Complete the following steps to configure the IBM BladeCenter S SAS RAID Controller Module, the BC-S chassis and blade servers for installing a SAS booted operating system.

Procedure

1. Before proceeding with any of the steps in this section, make sure that the SAS RAID Controller Module has been updated to the latest firmware levels. Review the *IBM BladeCenter S SAS RAID Controller Module Installation and Users Guide* for information on how to update the firmware on the module. Review and perform, if required, the steps in the section titled "Prerequisites" on page 15.
2. If using a SAS Expansion Card, it is recommended to disable the onboard SAS controller. press F1 when prompted in the System X splash screen to get in the BIOS setup window to:
   a. Disable the integrated/onboard SAS controller if you have SAS Expansion Card (CFFv) (39Y9190) installed.

      Note: Do not disable the integrated/onboard SAS controller if you have IBM SAS Connectivity Card (CFFv) (43W3974) installed instead.
   b. If this blade server has a mapped boot volume (LUN) that was create from a pool with the SAS RAID Controller Module in bay 4 (option -port 1 when creating the pool in the CLI) as the preferred owner, do not change the hard drive boot order. **If the boot volume was mapped as LUN 0, use hd0 as the boot drive in the blade server boot sequence no matter which SAS RAID Controller Module is the preferred owner**.
   c. Save the new BIOS settings before exiting the Configuration/Setup utility. Repeat this step for each blade server that has boot logical drives/LUNs defined in the boot disk system.
3. Modify the SAS Adapter Timing Properties. To change these settings, refer to Appendix A, "Appendix A: Configuring a SAS HBA BIOS on x86-64 (Intel or AMD) host," on page 147.
4. Use the IBM Storage Configuration Manager (SCM) program or the SAS RAID Controller Module Command Line Interface (CLI), create at least one volume (boot volume) for each blade server in the BC-S chassis. Observe the following guidelines when creating the boot volume:
   a. Ensure that the volume that is used as the boot volume is big enough to contain the operating system and its swap space and any application code.
   b. For Linux, it is assumed that the root volume and the swap partition are located in the same boot volume.
   c. For Linux, it is recommended that the swap device be at least the size of the physical memory that is configured in the blade server.
   d. The boot volume must be mapped to the blade server as LUN 0.
   e. For protection against disk failure, the boot volume should be part of RAID 1, 10 or 5 storage pools. Note: It is possible to use a RAID 0 pool for a boot volume however this is not recommended due to the potential risk of single disk failure without redundancy.

f. Though it is possible to create the boot and data volumes for all the server blades in a BladeCenter S Chassis as part of the same RAID storage pool, it is recommended to split the boot and data volumes using separate RAID storage pools where one pool has the SAS RAID Controller Module in bay 3 as the preferred owner and the other pool has the SAS RAID Module in bay 4 as the preferred owner.

g. At this time in the remote SAS boot configuration process you should create only the boot volume to which the host will be mapped in order to ensure that the operating system, swap space, applications, and application data are stored in the same volume. After completing this process you can create and map additional volumes to this host. Refer to section "Host attachment path considerations" on page 12 for total number of volumes that can be mapped to a host. If volumes other than the boot volume are created, do not map the additional volumes to the blade server SAS ports at this time. You can create the additional volumes and map them to the blade server as part of the post operating system installation activities.

5. Map this boot volume to only one of the blade server SAS ports as LUN 0. If the BIOS sees the same boot volume on multiple paths, it will present two available disks that can be used for OS installation. Because the BIOS will present the volumes in the order that it scans, if the volumes are not scanned in the same order every time the blade server reboots, one might get a "boot device not found" error when rebooting the blade server.

6. If not using SCM, the WWPN of the blade server SAS port can be obtained by making a telnet connection into the SAS switch component of the SAS RAID Controller Module and performing a "sasport status all" command. For example, in the command output below, the WWPN of the SAS port in blade server 1 is **"500062B0000D7A10"**.

   Note: The blade servers must be powered on and reach the MPT SAS BIOS and firmware loading point before the SAS switch can discover the SAS card WWPN. It is recommended that the Ctrl+C keys be pressed during the MPT SAS BIOS loading to enter the LSI Corp Config Utility and to stop the blade server from booting further. Once the SAS WWNs are recorded and the boot volume is configured and mapped to the appropriate SAS WWNs, one can restart the blade server to start the operating system installation.

```
=== IBM BladeCenter(R) SAS RAID Controller Module ===
Login: USERID
Password: ********
USERID logged on
MAIN> sasport status all
ID  SAS Port Name               SAS Address      Enable Flt Status
---+--------------------------+----------------+------+---+--------
E1  External Port 1                              True   Off NoCable
    PHY 1C                     0000000000000000 True       NoCable
    PHY 1D                     0000000000000000 True       NoCable
    PHY 1E                     0000000000000000 True       NoCable
    PHY 1F                     0000000000000000 True       NoCable
E2  External Port 2                              True   Off NoCable
    PHY 20                     0000000000000000 True       NoCable
    PHY 21                     0000000000000000 True       NoCable
    PHY 22                     0000000000000000 True       NoCable
    PHY 23                     0000000000000000 True       NoCable
E3  External Port 3                              True   Off Normal
    PHY 00                     0000000000000000 True       Normal
    PHY 01                     0000000000000000 True       Normal
    PHY 02                     0000000000000000 True       Normal
    PHY 03                     0000000000000000 True       Normal
E4  External Port 4                              True   Off NoCable
    PHY 04                     0000000000000000 True       NoCable
    PHY 05                     0000000000000000 True       NoCable
    PHY 06                     0000000000000000 True       NoCable
    PHY 07                     0000000000000000 True       NoCable
B1  Blade Slot Connection 1                      True   Off Normal
    PHY 1B                     500062B0000D7A10 True       Normal
B2  Blade Slot Connection 2                      True   Off Normal
    PHY 1A                     500062B00007CD84 True       Normal
B3  Blade Slot Connection 3                      True   Off Normal
    PHY 19                     500062B0000D79F4 True       Normal
B4  Blade Slot Connection 4                      True   Off Normal
    PHY 18                     500062B00007E6DC True       Normal
B5  Blade Slot Connection 5                      True   Off NoCable
    PHY 17                     0000000000000000 True       NoCable
B6  Blade Slot Connection 6                      True   Off Normal
    PHY 16                     500062B00007E6E0 True       Normal
B7  RAID HA Connection                           True   Off Normal
    PHY 0A                     5005076B07418C20 True       Normal
    PHY 09                     5005076B07418C20 True       Normal
    PHY 08                     5005076B07418C20 True       Normal
    PHY 0F                     5005076B07418C20 True       Normal
---+-------------------------+----------------+------+---+--------
ID  SAS Port Name            SAS Address      Enable Flt Status
```

Figure 166. sasport status all command output

Note: When the boot volume is created, it can be created in the pool that is preferentially owned by the SAS RAID Controller Module in bay 3 (-port 0 option when creating the pool) or in the pool that is preferentially owned by the SAS RAID Controller Module in bay 4 (-port 1 option when creating the pool. Regardless of the preferred owner setting, it is recommended to always use the WWPN of the SAS port that is shown in the "sasport status all" of the SAS switch in bay 3 (the first SAS port of the SAS card adapter) for the initial OS installation. The first SAS port of a two port SAS card adapter will always have the WWPN be one less than the WWPN of the second adapter. For example, if the first SAS port WWPN is "500062B0000D7A10", the second SAS port WWPN will be "500062B0000D7A11".

7. Once the boot volume is mapped to the SAS port in the blade server, one should see the volume displayed when the MPT SAS BIOS completes the scan for devices as shown below.

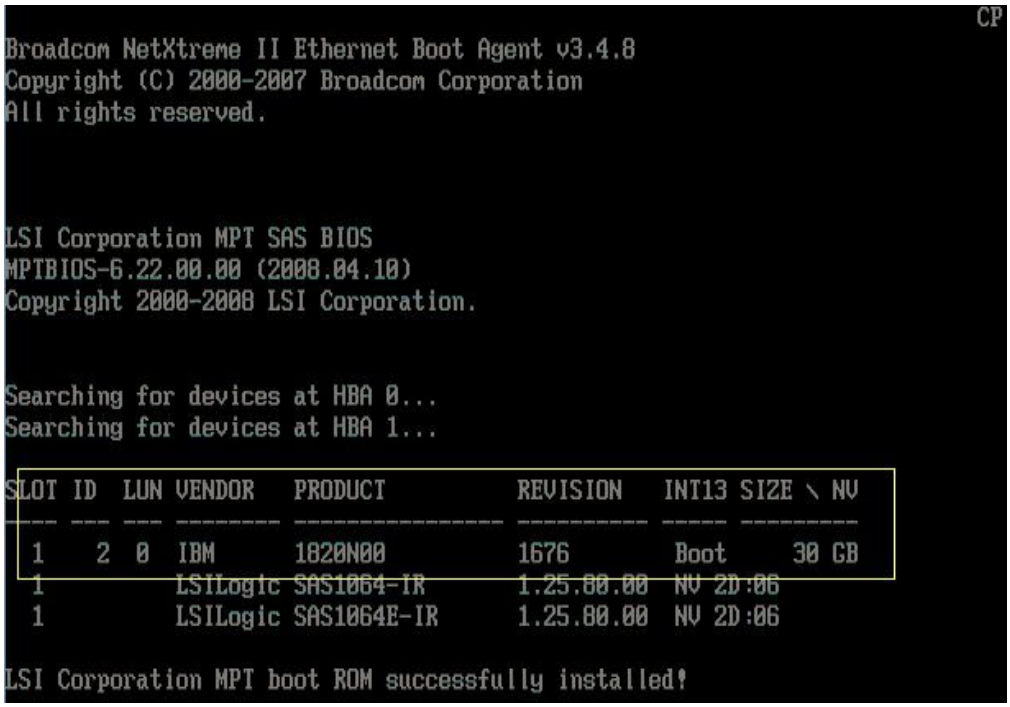


Figure 167. MPT SAS BIOS device scan result

8. If there is an internal hard drive installed in the blade server, it is recommended to remove it before installing the operating system on the SAS RAID Controller Module boot volume.

Appendix C. Appendix C: Procedure for MPTSAS FW upgrade of HS12, HS21-XM, HS21, HS22, HS22V, HX5 and LS20 blades

About this task

The installation of LSI SAS firmware 2.71 or later, when coming from a firmware level less than 2.71 requires modification of the host LUN mappings on the SAS RAID Controller Module prior to installing the firmware on the blade. This new version of firmware will change the World Wide Names (WWNs) that are presented to the SAS switch of the SAS RAID Controller Module. On a local booted blade (OS installed on internal drive) the new firmware will add 0x01 to the WWNs. On a SAS booted blade, with no internal drive present, the new firmware will add 0x02 to the current WWNs. Therefore prior to the installation of the new LSI SAS firmware on a HS12, HS21-XM, HS21, HS22, HS22V, HX5 and LS20 blades the system administrator needs create new host LUN mappings with the new WWN.

Example of WWN changes with SAS boot:

Prior to installation the WWNs are 5005076B08801D6E & 5005076B08801D6F. After installation of the 2.71 firmware the WWNs will become 5005076B08801D70 & 5005076B08801D71.

Example of WWN changes with local boot:

Prior to installation the WWNs are 5005076B08801D6F & 5005076B08801D70. After installation of the 2.71 firmware the WWNs will become 5005076B08801D70 & 5005076B08801D71.

Before installing the 2.71 firmware the system administrator must add new mappings of the current LUNs to the future WWNs that will be presented to the SAS switch. This can be done using either the CLI or the SCM. The following example uses the CLI commands.

CLI Procedure: Using SAS boot HS22(type 7870)

Procedure

1. Determine what the new WWNs will be. SAS booted – add 0x02 to the current WWNs.

   Current WWN: 5005076B08801D6E & 5005076B08801D6F

   New WWN: 5005076B08801D70 & 5005076B08801D71
2. Get current host LUN mappings.

   <CLI> hostlun -get -wwn 5005076B08801D6E

   HostWWN 5005076b08801d6e, HostName:

   LUNs Mapped :

LUN	Permission	Volume
0	ACCESS_READWRITE	raid0:sasbootvol01
11	ACCESS_READWRITE	raid0:vol04
12	ACCESS_READWRITE	raid0:vol10
13	ACCESS_READWRITE	raid0:vol16
14	ACCESS_READWRITE	raid0:vol22
6	ACCESS_READWRITE	raid1:vol04
7	ACCESS_READWRITE	raid1:vol10
8	ACCESS_READWRITE	raid1:vol16
9	ACCESS_READWRITE	raid1:vol22
10	ACCESS_READWRITE	raid1:vol28
15	ACCESS_READWRITE	raid5:vol31
1	ACCESS_READWRITE	raid5:vol04
2	ACCESS_READWRITE	raid5:vol10
3	ACCESS_READWRITE	raid5:vol16
4	ACCESS_READWRITE	raid5:vol22
5	ACCESS_READWRITE	raid5:vol28

Figure 168. LUNs Mapped

3. Map existing LUNs to new WWN.

   <CLI> hostlun -map -volume raid0:sasbootvol01 -wwn 5005076B08801D70 -lun 0

   <CLI> hostlun -map -volume raid0:sasbootvol01 -wwn 5005076B08801D71 -lun 0

4. Repeat for each LUN mapped to the blade which will receive the firmware update.

   <CLI>hostlun -map -volume raid5:vol31 -wwn 5005076B08801D70 -lun 15

   <CLI>hostlun -map -volume raid5:vol31 -wwn 5005076B08801D71 -lun 15

5. Verify Mapping to new WWNs.

   <CLI>hostlun -get -wwn 5005076B08801D70

   HostWWN 5005076b08801d70, HostName :

   LUNs Mapped :

LUN	Permission	Volume
0	ACCESS_READWRITE	raid0:sasbootvol01
11	ACCESS_READWRITE	raid0:vol04
12	ACCESS_READWRITE	raid0:vol10
13	ACCESS_READWRITE	raid0:vol16
14	ACCESS_READWRITE	raid0:vol22
6	ACCESS_READWRITE	raid1:vol04
7	ACCESS_READWRITE	raid1:vol10
8	ACCESS_READWRITE	raid1:vol16
9	ACCESS_READWRITE	raid1:vol22
10	ACCESS_READWRITE	raid1:vol28
15	ACCESS_READWRITE	raid5:vol31
1	ACCESS_READWRITE	raid5:vol04
2	ACCESS_READWRITE	raid5:vol10
3	ACCESS_READWRITE	raid5:vol16
4	ACCESS_READWRITE	raid5:vol22
5	ACCESS_READWRITE	raid5:vol28

Figure 169. LUNs Mapped

<CLI>hostlun -get -wwn 5005076B08801D71
HostWWN 5005076b08801d71, HostName :
LUNs Mapped :

LUN	Permission	Volume
0	ACCESS_READWRITE	raid0:sasbootvol01
11	ACCESS_READWRITE	raid0:vol04
12	ACCESS_READWRITE	raid0:vol10
13	ACCESS_READWRITE	raid0:vol16
14	ACCESS_READWRITE	raid0:vol22
6	ACCESS_READWRITE	raid1:vol04
7	ACCESS_READWRITE	raid1:vol10
8	ACCESS_READWRITE	raid1:vol16
9	ACCESS_READWRITE	raid1:vol22
10	ACCESS_READWRITE	raid1:vol28
15	ACCESS_READWRITE	raid5:vol31
1	ACCESS_READWRITE	raid5:vol04
2	ACCESS_READWRITE	raid5:vol10
3	ACCESS_READWRITE	raid5:vol16
4	ACCESS_READWRITE	raid5:vol22
5	ACCESS_READWRITE	raid5:vol28

Figure 170. LUNs Mapped

6. Install new mptsas firmware ibm_fw_mptsas_hs22-2.71_linux_32-64.
   After install the new WWNs will be in use.

   Note: Appendix B, "Appendix B: SAS Boot Pre-Operating System Installation Activities," on page 157 describes how to obtain the WWNs for a blade in the BC-S chassis.

Appendix D. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/systems/info/x86servers/serverproven/compat/us to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/supportportal to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/supportportal.

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at http://www.ibm.com/supportportal. IBM System x information is at http://www.ibm.com/systems/x. IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter/. IBM IntelliStation information is at http://www.ibm.com/systems/intellistation.

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw

Creating a personalized support web page

You can create a personalized support web page by identifying IBM products that are of interest to you.

To create a personalized support web page, go to http://www.ibm.com/support/mynotifications. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services or see http://www.ibm.com/planetwide for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services.

To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide . In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1,048,576 bytes, and GB stands for 1,073,741,824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1,000,000 bytes, and GB stands for 1,000,000,000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as "total bytes written" (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. IBM is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 5. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

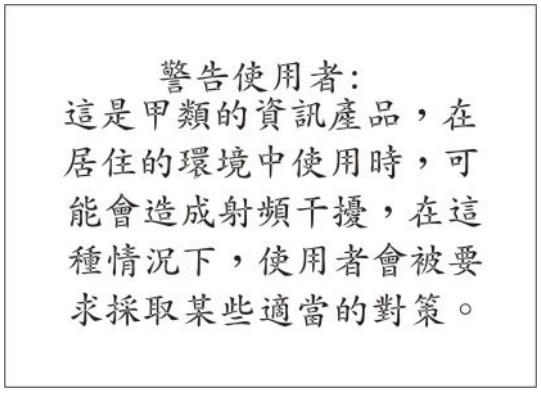
People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement



Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Part Number: 00AK732

Printed in USA

(1P) P/N: 00AK732