

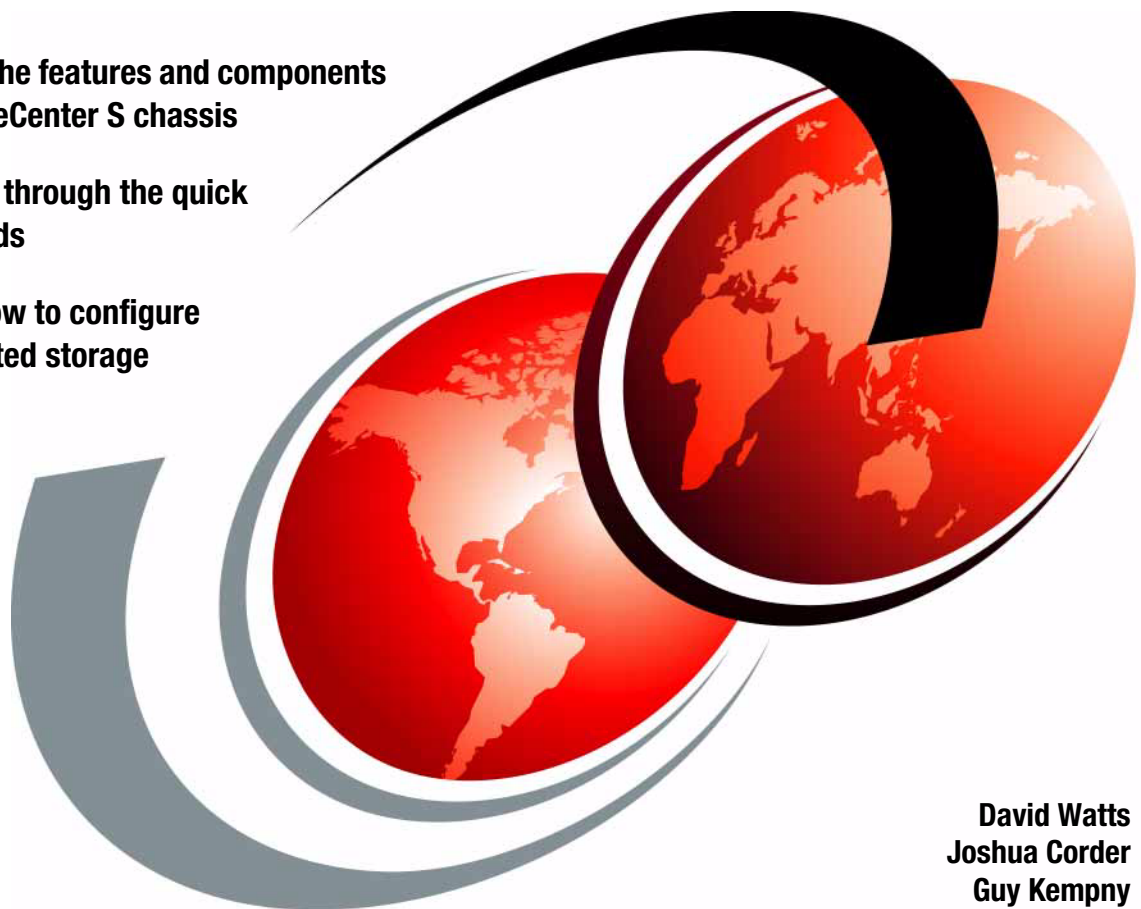


Implementing the IBM BladeCenter S Chassis

Describes the features and components of the BladeCenter S chassis

Guides you through the quick start wizards

Explains how to configure the integrated storage



David Watts
Joshua Corder
Guy Kempny

ibm.com/redbooks

Redbooks



International Technical Support Organization

Implementing the IBM BladeCenter S Chassis

July 2013

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

Second Edition (July 2013)

This edition applies to IBM BladeCenter S (machine type 8886).

© Copyright International Business Machines Corporation 2009, 2013. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	ix
Trademarks	x
 Preface	xi
Authors	xi
Now you can become a published author, too!	xiii
Comments welcome	xiv
Stay connected to IBM Redbooks	xiv
 Chapter 1. Introduction to the IBM BladeCenter S chassis	1
1.1 IBM BladeCenter	2
1.2 Why BladeCenter S	4
1.3 BladeCenter concepts and terminology	5
1.4 Disk Storage Module and Storage concepts	8
1.4.1 Serial Advanced Technology Attachment (SATA)	9
1.4.2 Serial-Attached SCSI (SAS)	9
1.4.3 Near line disk drives (NL disks)	10
1.5 Blade servers	11
1.5.1 BladeCenter HS23 server	12
1.5.2 BladeCenter HS23E server	14
1.5.3 BladeCenter HX5 server	16
1.5.4 BladeCenter PS700, PS701, PS702 servers	18
1.5.5 BladeCenter PS703 server	24
1.6 BladeCenter S server support matrix	26
 Chapter 2. BladeCenter S technical overview	29
2.1 BladeCenter S chassis	31
2.2 Storage modules	34
2.3 Drives	37
2.4 SAS Connectivity Module	39
2.4.1 Features and specifications	41
2.4.2 SAS Connectivity Module administration tools	42
2.5 SAS RAID Controller Module	44
2.5.1 Features and specifications	46
2.5.2 SAS RAID Controller Module administration tools	47
2.5.3 Comparison table of the two SAS module types	48
2.5.4 Battery Backup Units	49
2.6 SAS adapters	51
2.6.1 SAS Connectivity Card (CIOv)	51

2.6.2	ServerRAID H1135 (CLOv) Controller	53
2.7	External SAS connectivity: Storage	54
2.8	Media tray	55
2.9	System LED panels with light path diagnostics	58
2.9.1	Module LEDs	61
2.10	Advanced management module	62
2.10.1	AMM connections and indicators	64
2.11	Serial Pass-thru Module	66
2.12	I/O module bays	68
2.12.1	I/O expansion module options	71
2.12.2	Using I/O bay 2	73
2.12.3	Supported adapters	75
2.13	SAS tape storage for IBM BladeCenter	75
2.13.1	Tape drive guidelines	75
2.13.2	Supported tape drives	76
2.13.3	IBM RDX USB.3.0 Disk Backup Solution	78
2.14	BladeCenter S Office Enablement Kit	78
2.15	Extra rack options	80
2.16	Power supply modules and redundancy	82
2.16.1	Power supply modules	83
2.16.2	Power redundancy and throttling	85
2.17	Power management policies	86
2.17.1	Redundant AC power source policies	87
2.17.2	Redundant power module policies	88
2.17.3	No redundancy	89
2.17.4	Power redundancy examples	89
2.18	IBM uninterruptible power supply offerings	95
Chapter 3.	Getting started using the BladeCenter S chassis	99
3.1	AMM configuration	100
3.1.1	Setting up the advanced management module	100
3.1.2	Connecting to the AMM for the first time	101
3.2	AMM Configuration Wizard	103
3.2.1	Using the AMM Wizard Express path	107
3.2.2	Using the AMM Wizard Custom path	126
3.3	ServerGuide Scripting Toolkit	148
3.3.1	Key features	148
3.3.2	Operating system support	149
3.4	Using the command-line interfaces	150
3.5	IBM Fabric Manager	151
3.5.1	Overview	151
3.5.2	Licensing	152
3.5.3	Enabling Fabric Manager	154

3.5.4	Opening Fabric Manager components	155
3.5.5	Creating a BOFM configuration file	156
3.6	BladeCenter S tips and guidelines	161
3.6.1	Before you buy	162
3.6.2	Deploying the BladeCenter S chassis	162
Chapter 4.	Configuring storage	165
4.1	Features of each storage management interface	166
4.2	Understanding storage zones	168
4.2.1	User-defined zones	170
4.2.2	Predefined zones	171
4.3	Predefined configuration summary	172
4.4	Predefined storage configuration schematics	176
4.4.1	Predefined Storage Configuration 6	176
4.4.2	Predefined Storage Configuration 7	177
4.4.3	Predefined Storage Configuration 8	178
4.4.4	Predefined Storage Configuration 9	179
4.4.5	Predefined Storage Configuration 10a	180
4.4.6	Predefined Storage Configuration 10b	181
4.4.7	Predefined Storage Configuration 11	183
4.4.8	Predefined Storage Configuration 12	184
4.4.9	Predefined Storage Configuration 13	185
4.5	Storage Configuration Manager	187
4.5.1	Installing SCM with the BladeCenter S component	187
4.5.2	Starting Storage Configuration Manager	194
4.5.3	Initial Setup Wizard for the SAS RAID Controller Module	197
4.5.4	Initial Configuration Wizard for the SAS Connectivity Module	213
4.5.5	User-defined and zone configurations	219
4.5.6	All Resources window	229
4.5.7	Physical View window	230
4.5.8	Battery backup unit status and management	231
4.5.9	Active Alerts window	233
4.5.10	Long Running Tasks window	234
4.5.11	Storage window	235
4.5.12	SAS Zoning task	236
4.5.13	Ports and SAS ports	237
4.5.14	Audit log	242
4.5.15	Update firmware for the SAS Connectivity Module	243
4.5.16	Updating firmware for the SAS RAID Controller Module	243
4.5.17	Device log	244
4.5.18	Error counters	246
4.5.19	Collecting support data	248
4.5.20	User management	249

4.6	Using the AMM Storage Configuration task	250
4.7	Using the SAS module web browser interface	253
4.7.1	Logging in	254
4.7.2	Monitoring SAS subsystem health	255
4.7.3	Updating firmware: SAS Connectivity Module	256
4.7.4	Updating firmware: SAS RAID Controller module	257
4.7.5	View logs	258
4.7.6	View error counters	259
4.7.7	View alarms	260
4.7.8	View RAID	260
4.7.9	User administration	261
4.7.10	Zoning	262
4.8	Configuring the SAS RAID Controller Module using the CLI	265
4.9	Configuring the SAS Connectivity Module using CLI	269
4.9.1	Understanding the zone matrix on the SAS Connectivity Module	270
4.9.2	Configuring a user-defined zone from the CLI	272
4.10	Configuring external SAS ports for SAS tape	280
4.11	Firmware updating	289
4.11.1	SAS Connectivity Module firmware	290
4.11.2	SAS RAID Controller Module firmware	294
4.11.3	Updating firmware for SAS Connectivity Card	304
4.12	Firmware update for disk drives	307
4.12.1	Firmware update for internal Blade HDD	307
4.12.2	HDD firmware updates using SAS Connectivity Module	312
4.12.3	HDD firmware updates using SAS RAID Controller Module	312
4.13	IBM System Storage multipath driver	313
4.13.1	IBM Subsystem Device Driver Device Specific Module	313
4.13.2	IBM Subsystem Device Driver Path Control Module	314
Chapter 5.	AMM user interface guide	317
5.1	Introduction	318
5.2	Command-line interface	318
5.2.1	Connecting to the CLI	319
5.2.2	Command help	320
5.2.3	Targeting	320
5.2.4	Complete CLI example: Configuring the AMM	322
5.3	Monitors	325
5.3.1	System status	326
5.3.2	Event log	327
5.3.3	LEDs	329
5.3.4	Power management	331
5.3.5	Hardware vital product data	340
5.3.6	Firmware vital product data	344

5.3.7 Remote Chassis	346
5.4 Blade tasks	348
5.4.1 Blade Power/Restart	349
5.4.2 Remote Control Status	352
5.4.3 Updating blade firmware	362
5.4.4 Configuration	364
5.4.5 Serial Over LAN	374
5.5 I/O module tasks	374
5.5.1 I/O Module Power/Restart	375
5.5.2 Configuration	376
5.5.3 Updating I/O module firmware	379
5.6 Storage tasks	380
5.7 Management module control	382
5.7.1 General Settings	382
5.7.2 Login profiles	386
5.7.3 Alerts	394
5.7.4 Managing alerts from the command line	398
5.7.5 Passive air filter reminder	400
5.7.6 Serial port	400
5.7.7 Port assignments	401
5.7.8 Network interfaces	402
5.7.9 Network protocols	404
5.7.10 Miscellaneous services	411
5.7.11 Configuring services from the CLI	411
5.7.12 Chassis Internal Network (CIN)	414
5.7.13 Security	415
5.7.14 File management	416
5.7.15 Update AMM firmware	418
5.7.16 Configuration management	418
5.7.17 Restart AMM	425
5.7.18 License Manager	426
5.8 Service tools	426
5.8.1 AMM Service Data	427
5.8.2 Blade Service Data	429
5.8.3 AMM Status	431
5.8.4 Service Advisor	433
Abbreviations and acronyms	435
Related publications	439
IBM Redbooks	439
Other publications	439
Online resources	440

How to get Redbooks..... 441

Help from IBM 441

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.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	IBM Systems Director Active	Redbooks (logo)  ®
BladeCenter®	Energy Manager™	Storwize®
DS6000™	Lotus®	System Storage®
DS8000®	POWER®	System x®
Enterprise Storage Server®	Power Systems™	WebSphere®
IBM®	POWER7®	X-Architecture®
IBM Flex System™	Redbooks®	xSeries®
	Redpaper™	z/OS®

The following terms are trademarks of other companies:

Intel, Intel Xeon, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Linear Tape-Open, LTO, Ultrium, the LTO Logo and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

Preface

IBM® BladeCenter® remains an innovative solution to running business solutions. IBM BladeCenter builds on the IBM commitment to integrating server, storage, and networking functionality with technology exchange and heterogeneous management. IBM BladeCenter offers the ease, density, availability, affordability, and scalability that are central to the blade technology promise.

IBM BladeCenter S combines the power of blade servers with integrated storage. It can hold up to six blade servers and up to 12 shared hot-swap 3.5-inch disk drives in just 7U of rack space.

BladeCenter S is the ideal solution for a branch office or distributed environment where servers, switches, and shared storage are all in one unit, or in environments where only 110V power is available.

This IBM Redbooks® publication provides a stand-alone reference compendium that you can use to quickly and easily set up a BladeCenter S. The book includes these sections:

- ▶ An overview of IBM BladeCenter servers and technology
- ▶ A technical review of the BladeCenter S and its options
- ▶ An in-depth explanation of storage zoning and configuration
- ▶ Step-by-step setup guides for both the advanced management module and Storage Configuration Manager

This book was written for a technical audience with limited or no experience with IBM BladeCenter solutions. After reading it, you should be able to successfully implement the BladeCenter S, customized to your specific needs.

Authors

This book was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Raleigh Center.



David Watts is a Consulting IT Specialist for IBM Redbooks in Raleigh NC in the US. He manages residencies and produces IBM Redbooks publications on hardware and software topics that are related to IBM Flex System™, IBM System x®, and BladeCenter servers and associated client platforms. He has authored over 200 books, papers, and Product Guides. He holds a Bachelor of Engineering degree from the University of Queensland (Australia), and has worked for IBM in both the United States and Australia since 1989. David is an IBM Certified IT Specialist, and a member of the IT Specialist Certification Review Board.



Josh Corder is a Platform Systems Engineer for a Fortune 50 retailer. He has more than 10 years experience designing, developing, deploying, and supporting server environments on multiple platforms that include IBM Power Systems™. His specialties are IBM AIX®, BladeCenter, and hardware solution design for large scale distributed computing environments. He recently worked with a cross-functional team on BladeCenter S system deployment.



Guy Kempny is an IT Consultant for CSSAU. He specializes in server virtualization and consolidation, Voice over IP solutions, and networking. Guy worked for IBM Australia for 19 years in various roles, including Project Management, IT Architect, and Technical Marketing. He has experience with x86 and IBM z/OS® platforms, speech software, IBM Lotus® and IBM WebSphere®. He is experienced with server design solutions based on IBM System x and BladeCenter systems. Guy was an IT Specialist for IBM corporate sports sponsorship and large-scale events, including IBM Program Manager for Sydney 2000 Olympic Games. Guy has authored five previous IBM Redbooks publications.

Thanks to the authors of the previous edition of this book:

- ▶ David Watts
- ▶ Michael Hurman
- ▶ Leimar Braz da Silva

Thanks to the authors of the IBM Redpaper™ *Implementing the IBM BladeCenter S Chassis*, REDP-4357, which formed the basis of this book:

- ▶ David Watts
- ▶ Justin Morosi
- ▶ Michael Hurman

Thanks to the following people for their contributions to this project:

Tamikia Barrow
Deana Coble
Mary Comianos
Shari Deiana
Linda Robinson
International Technical Support Organization

Meleata Pinto
David Tareen
IBM Marketing

Ke Jie Cao
Carrie JC Chang
Andy Ehrenzeller
Sharon HY Hsu
Phil Johnson
Rick CH Lin
William WJ Liu
Marc Stracuzza
Chelsea CH Wu
Joyce PY Yen
IBM Development

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and

relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:

<http://www.facebook.com/IBMRedbooks>

- ▶ Follow us on Twitter:

<http://twitter.com/ibmredbooks>

- ▶ Look for us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>



Introduction to the IBM BladeCenter S chassis

The IBM BladeCenter S is designed for small and midsized offices, and for distributed environments. The BladeCenter S is a high-density, high-performance integrated rack-mounted server system. It supports up to six blade servers that can share common resources, such as power, cooling, management, I/O resources, and storage within a single BladeCenter S chassis.

This chapter introduces IBM BladeCenter with the following topics:

- ▶ 1.1, “IBM BladeCenter” on page 2
- ▶ 1.2, “Why BladeCenter S” on page 4
- ▶ 1.3, “BladeCenter concepts and terminology” on page 5
- ▶ 1.4, “Disk Storage Module and Storage concepts” on page 8
- ▶ 1.5, “Blade servers” on page 11
- ▶ 1.6, “BladeCenter S server support matrix” on page 26

1.1 IBM BladeCenter

Since 2002, there have been numerous improvements and enhancements to the original BladeCenter. However, the core concepts and terminology have remained the same. This section contains a summary of the most important concepts and components that are used throughout this paper.

Currently, there are four chassis in the BladeCenter family:

- ▶ IBM BladeCenter S has internal storage, autosensing power supplies (110 V or 220 V), and a simple “select and click” setup wizard. It is designed for small to medium size businesses and remote offices.
- ▶ IBM BladeCenter E provides the greatest blade density per rack of the BladeCenter family, high levels of energy efficiency, and support for a wide range of common I/O fabrics.
- ▶ IBM BladeCenter H delivers high performance, extreme reliability, and ultimate flexibility for the most demanding IT environments.
- ▶ IBM BladeCenter HT models are designed for high-performance flexible telecommunications environments. They support high-speed internetworking technologies, such as 10G Ethernet, and provide a robust platform for next-generation networks (NGNs).

All four chassis share a common set of blades and standard switch modules. Additionally, BladeCenter H and HT offer high-speed I/O bays for high-speed switches such as 10 Gb Ethernet or QDR InfiniBand.

The IBM BladeCenter S is a departure from the rest of the BladeCenter family because it is specifically designed to be used outside of the data center. Acting on feedback from the small to medium size marketplace, IBM created a chassis that has similar features to the other models, but in a much more flexible and customizable form factor. The BladeCenter S uses the existing product portfolio of the BladeCenter family, and adds a few new model-specific options.

The BladeCenter S is shown in Figure 1-1.



Figure 1-1 IBM BladeCenter S

One of the most unique aspects of the BladeCenter S is its onboard SAS/SATA storage capability. The chassis can accommodate up to twelve 3.5-inch hard disk drives in two standard storage modules. These disks can be assigned and accessed directly by the blades in the chassis. For more information about the BladeCenter S chassis, see Chapter 2, “BladeCenter S technical overview” on page 29.

Although the BladeCenter S has many unique features, its ultimate strength lies in its ability to use almost all of the existing BladeCenter blade servers and I/O modules. Because of this unprecedented interoperability, BladeCenter S can be configured to provide enterprise level functionality and availability in virtually any environment.

The BladeCenter S chassis allows for either six single-slot blade servers or three double-slot blade servers. However, several blade server models and widths can be intermixed in one chassis simultaneously to support virtually any requirement (subject to power and cooling requirements). For more information about each of the current Blade models, see 1.6, “BladeCenter S server support matrix” on page 26.

1.2 Why BladeCenter S

IBM BladeCenter S combines the power of blade servers with integrated storage, all in an easy-to-use package that is designed specifically for the office and distributed enterprise environment.

This configuration provides the following cost benefits over traditional rack mounted servers, among others:

- ▶ Blades and modules use the space inside their chassis efficiently, fitting more computing density into the same physical space.
- ▶ Blade nodes share the management, networking, power, and cooling modules, offering lower overhead and cost savings.
- ▶ In contrast to traditional rack-mounted servers, most blades and chassis modules can be replaced without tools or special knowledge. This advantage translates to improved reliability, faster service restoration after an outage, and cheaper support costs.
- ▶ Replaceable blades, storage, and networking modules mean that you can add new and alternative technologies without replacing entire servers, enduring long outages, or having to go through painful migrations.
- ▶ Blades make it easier than ever to try new ideas and technologies to improve your business.

Examples of good solutions for BladeCenter S

Company A has an older application that is central to their business model. It requires an older version of Linux, is not virtualized, and the cost to move away from the system is expensive. In the meantime, they want to test customer analytic software that requires Windows Server 2012. Their storage requirements are low, but the new software has robust system requirements.

Company A can benefit greatly from the BladeCenter S product line. They can use an entry level HS23E blade to support older applications, and add a more powerful x86 blade to support the new software. Using the drive and storage modules in the chassis provides all of their business requirements in one package. They would have four remaining slots for growth, increasing their speed to market and lowering their overall support costs.

Company B is a large pharmacy retailer with several hundred locations throughout the United States. Each location has nearly a hundred clients that depend on a back-office server for the point of sale system. If the server crashes, the entire location cannot service their customers. They have no onsite IT personnel and no real data center environment in their stores. The business is losing money as their rack mounted servers age in the environment. Company B

must remain flexible because retail trends change quickly and they do not want to fall behind the competition.

Company B is also a good example of an environment where the BladeCenter S can be a great benefit. The solution provides a flexible “store in a box” solution that can run in the manager’s office or any secured location on the existing power infrastructure. Store employees can be used for support by working with remote personnel off-site. Adding two blades in a clustered configuration and using the SAS RAID Modules provides a highly available solution that had plenty of room for growth. It also provides support for Windows, Linux, or AIX across multiple blade types.

1.3 BladeCenter concepts and terminology

This section describes the main terms and concepts that are described in this book.

Figure 1-2 shows an illustration of the internal components of BladeCenter S.

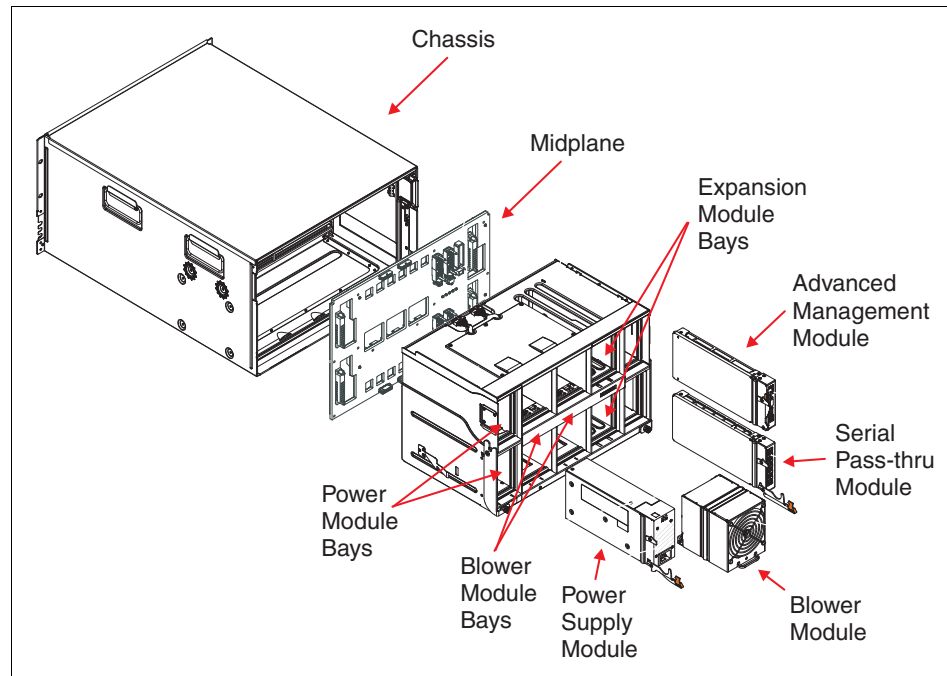


Figure 1-2 Exploded view of BladeCenter S components

Figure 1-3 shows an illustration of the storage module for the BladeCenter S.

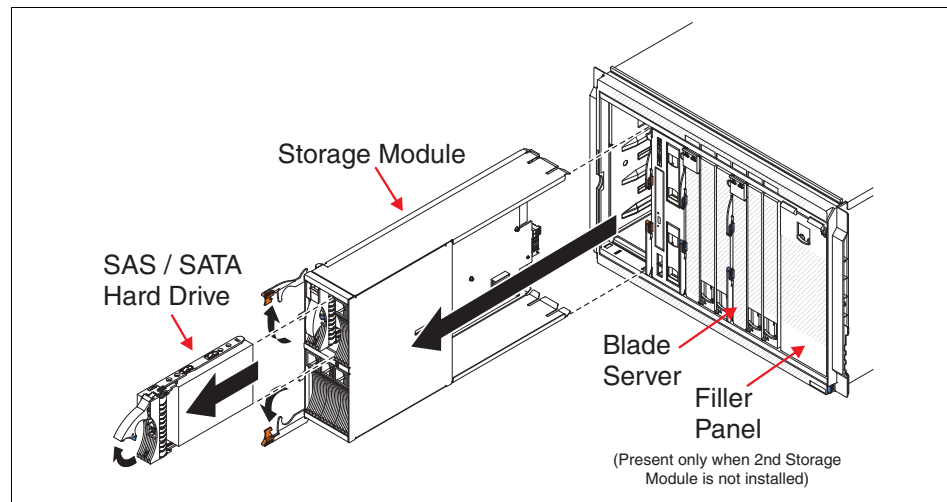


Figure 1-3 Exploded view of a storage module for BladeCenter S

The following are the commonly used terms:

► Chassis

The term chassis typically refers to the physical frame of the BladeCenter, including the interconnects that are contained within the frame: The midplane, power supply, and blower modules.

Although the chassis does not possess any inherent intelligence, it does contain a significant amount of circuitry. This circuitry is often referred to as paths within the chassis. These paths comprise the backbone of the BladeCenter and allow it to share the servers, switches, and power.

► Blade servers

Any server that is designed in the standard BladeCenter form factor is considered to be a blade server, or *blade*. Blades are universal in size and shape. They can be inserted in any of the existing BladeCenter portfolio. However, processor power demands might prevent their usage in all chassis.

Blades consist of a system board, processors, memory, expansion ports, and two redundant midplane connections. They do not contain a power supply, cooling fan, or any directly accessible I/O connections. Blades rely on the chassis to provide all necessary power, cooling, connectivity, and management.

► Midplane

The midplane is the physical circuit board that is responsible for providing all power and connectivity to the chassis' blades. The midplane is set up so that there is a series of upper connection points and an identical set of lower connection points. These provide power and redundancy. On the opposite side of the midplane are other numerous connection points, which allow for power supply, blower, and expansion module bay connectivity.

The power supply and blower connections on the midplane function independently of their upper or lower status. However, the expansion bays are uniquely pathed to upper or lower connections points as they relate to blades. The midplane does not possess any intelligence. It is strictly a pass-through mechanism for blade, module bay, and power connectivity.

► I/O module bays

There are several I/O module bays, power supply bays, and management module bays on all BladeCenter models. BladeCenter S also has a serial pass-through bay and two storage module bays. These bays are all directly connected to the midplane. However, they do not necessarily correlate to the upper or lower connections of the blade servers.

Power supply and blower modules are independent of blade connectivity. The management module bay can communicate to a blade through the upper or lower midplane connection. The expansion module bays have committed communication paths that are mapped directly to upper or lower connections for the blade slots in the chassis.

► Advanced management module

The advanced management module (AMM) is the center point for the BladeCenter infrastructure intelligence. The AMM is the primary means of management for the chassis, and controls all aspects of power, connectivity, and communication. It uses an upgradeable firmware and web user interface to run all routine hardware-based management tasks for blades, expansion modules, and configuration of storage modules.

The AMM also acts as a proxy for expansion modules. This configuration allows access by using direct (that is, IP address) or indirect (that is, internal chassis) methods for specific module management.

► Serial Pass-thru Module

When installed in a BladeCenter S, the Serial Pass-thru Module provides direct serial console access to each blade slot in the system. This optional module can be installed only in the Serial Pass-thru Module bay of a BladeCenter S.

The module has six external RJ45 console access ports on it, each of which is physically pathed directly to a blade slot. The module was designed for

serial console access only, and it is not intended for use by modems or other serial port devices.

- Expansion card

To provide access to the I/O module bays in a BladeCenter, it is sometimes necessary to install an expansion card (sometimes referred to as a *daughter card*) on the system board of a blade server. When installed in a blade server, the card enables extra paths to specific I/O module bays. The card typically provides two paths, one to each I/O module bay, for redundancy.

- Storage module

The concept of a chassis with a self-contained disk subsystem or storage module is unique to the BladeCenter S. The module is fundamentally a collection of disk drives that are made accessible through a SAS module and a SAS daughter card. The SAS module is responsible for both the provisioning of physical disk drives through zoning and for failover redundancy when two SAS modules are present.

When installed, the SAS expansion card acts as an extra RAID controller for the blade server. The expansion card can address only those disks that are assigned to it from the SAS module, and can create arrays only from those disks.

1.4 Disk Storage Module and Storage concepts

A storage module and the hard disk drives installed in that storage module are commonly referred to as *integrated shared storage*. There are various hard disk drive types available, so it is important to understand the features and benefits of each type. This section explains the types that are supported in IBM BladeCenters. Certain considerations must be taken into account because there might be specific hardware requirements to support certain types.

- SAS disk: Serial-Attached SCSI disks are designed for high performance requirements where maximum throughput and transaction capability is needed.
- SATA disk: Serial Advanced Technology Attachment disks are designed to provide lower-cost mass storage capacity, when compared to SAS disk. They are designed for systems where performance is not a requirement.

- Near line (NL) disks: NL disks are designed to provide lower-cost mass storage capacity, and can be either SATA or SAS disks.

1.4.1 Serial Advanced Technology Attachment (SATA)

Serial Advanced Technology Attachment (SATA or Serial ATA) is a successor of the widely used Parallel Advanced Technology Attachment (PATA) or Enhanced Integrated Drive Electronics (EIDE) interface used to attach separate drive options, including HDDs.

Traditional or desktop SATA drives are intended for use in 8x5 hours of operation (eight hours per day, five days per week) in low I/O single user desktop workload environments. They do not fit well into server environments.

IBM SATA HDDs provide reliable and most energy-efficient and cost-efficient storage per GB for lightly loaded departmental applications that store user data, such as file servers and email servers. They are also good for infrequent bandwidth-intensive sequential workloads such as archives, imaging, multimedia libraries, and disk backups.

1.4.2 Serial-Attached SCSI (SAS)

The serial-attached Small Computer System Interface (serial-attached SCSI, or SAS) connectivity technology is an evolution of the parallel SCSI Interface. It is intended to overcome performance and scalability limitations of bus topology while providing enterprise-class reliability and software stack compatibility.

The most recent SAS specification features 6 Gbps SAS connectivity. Because of its high performance, reliability, and scalability features, the SAS interface is widely used in the IBM System x server systems for both internal and external storage connectivity for wide range of applications and usage patterns.

In general, three types of devices form the SAS topology: SAS initiators, SAS or SATA targets, and SAS expanders:

- The initiators are the SAS controllers, that is, the IBM SAS RAID controllers or SAS Host Bus Adapters (HBAs).
- The targets are the end-point devices, such as disk or tape drives. SAS targets can be directly connected to the SAS initiator ports, or indirectly through SAS expanders (or even a sequence of SAS expanders).
- The SAS expander is a switch device that connects more target devices to the initiator than the number of ports the initiator has. This dramatically increases SAS fabric scalability without sacrificing reliability and performance. In addition, expanders support wide SAS links (or aggregated links) that consist

of several narrow SAS links for expander-expander or expander-initiator connections to increase overall performance of the fabric.

1.4.3 Near line disk drives (NL disks)

Data that are stored on an NL disk drive are intended to be accessed infrequently, but require 24x7 availability. From the application perspective, these drives are commonly used for storing archives, document images, multimedia libraries, and backups. There are two types of NL drives: NL SATA and NL SAS.

NL SATA

NL SATA is also commonly referred as *Enterprise SATA*. These disks use native SATA interfaces, and have the same capacity and performance characteristics as traditional or desktop SATA drives. However, NL SATA drives have better reliability and tolerance to vibration than traditional SATA drives, and are designed for 24x7 hours of operation.

In general, reliability and tolerance to vibration of NL SATA drives are twice that of traditional SATA drives. Vibration tolerance is important for deployment of multi-drive arrays, such as RAID arrays, to eliminate risk of read/write errors and retry cycles because of HDD rotational vibration interference.

Because of these advantages, IBM System x servers always use NL SATA drives as they offer almost twice the reliability, better support of multi-drive RAID array deployments, and 24x7 hours of operation (24 hours per day, 7 days per week) in multi-user workload environments. They do so without significant cost disadvantage when compared to desktop SATA drives.

NL SAS

NL SAS has the same performance, capacity, and reliability characteristics as NL SATA drives. The only difference is that NL SAS drives provide native SAS interface capabilities, including dual-RAID.

Redundant Array of Independent Disks (RAID)

To increase performance and reliability of the disk subsystem, *Redundant Array of Independent Disk* (RAID) arrays are commonly used. A RAID array is a group of physical disks that uses certain common method to distribute data across the disks. The data are distributed by *stripe units*. A stripe unit is the portion of data that are written to one disk drive immediately before the write operation continues on next drive. When the last drive in array is reached, the write operation continues on the first drive in the block that is adjacent to the previous stripe unit written to this drive, and so on.

The group of stripe units that are subsequently written to all drives in the array (from the first drive to the last drive) before write operation continues on the first drive, called a *stripe*. The process of distributing data in this way is called *striping*. A stripe unit is a minimal element that can be read from or written to the RAID array. Stripe units can contain data or recovery information.

The particular striping method that is used for data distribution is also known as the *RAID level*. The RAID level reduces availability, performance, and available storage capacity because achieving redundancy always lessens disk space by the amount reserved for storing recovery information.

There are basic RAID levels (0, 1, 5, and 6) and spanned RAID levels (00, 10, 50, and 60). *Spanned RAID arrays* combine two or more basic RAID arrays to provide higher performance, capacity, and availability by overcoming limitation of the maximum number of drives per array supported by a particular RAID controller.

1.5 Blade servers

IBM BladeCenter servers support a wide selection of processor technologies and operating systems. This flexibility allows you to run all of your diverse workloads inside a single architecture. The slim, hot-swappable blade servers fit in a single chassis similar to books in a bookshelf. Each blade server is an independent server with its own processors, memory, storage, network controllers, operating system, and applications. The blade server simply slides into a bay in the chassis and plugs into a midplane or backplane, sharing power, fans, diskette drives, switches, and ports with other blade servers.

The benefits of the blade approach are obvious to anyone tasked with running down hundreds of cables strung through racks just to add and remove servers. With shared switches and power units, precious space is freed up, and blade servers enable higher density with far greater ease.

Note: This book covers only a subset of the blade servers that are supported by the IBM BladeCenter S chassis, specifically the latest models. Table 1-8 on page 27 shows a complete list of the blade servers that are supported in the IBM BladeCenter S.

The following servers are covered in this section:

- ▶ 1.5.1, “BladeCenter HS23 server” on page 12
- ▶ 1.5.2, “BladeCenter HS23E server” on page 14
- ▶ 1.5.3, “BladeCenter HX5 server” on page 16

- ▶ 1.5.4, “BladeCenter PS700, PS701, PS702 servers” on page 18
- ▶ 1.5.5, “BladeCenter PS703 server” on page 24

1.5.1 BladeCenter HS23 server

The IBM BladeCenter HS23 server types 7875 and 1929 are next-generation high density, high performance, single-width blade servers. These servers can support up to two multi-core Intel Xeon microprocessors. They are ideally suited for medium and large businesses for virtualization, hosted client, SAP, and enterprise applications.

Figure 1-4 shows the HS23 server with its cover removed.

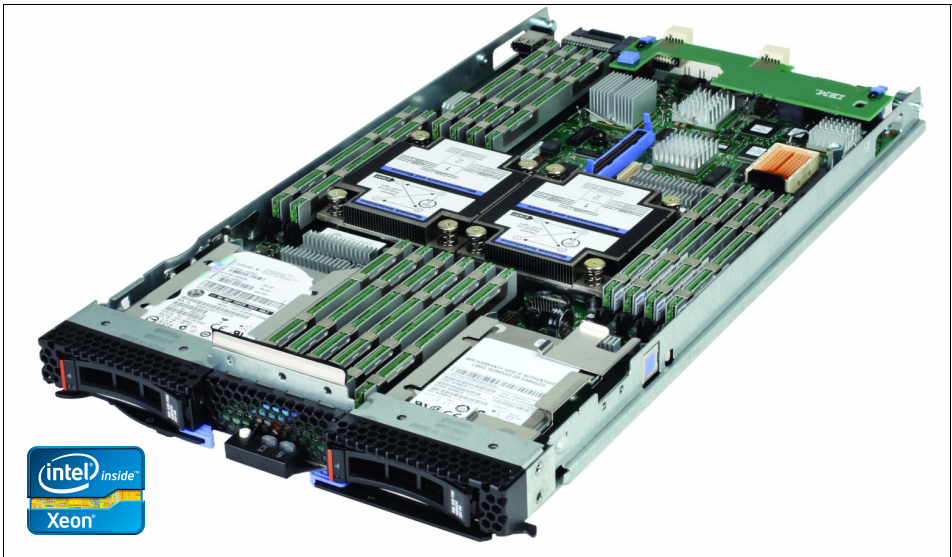


Figure 1-4 BladeCenter HS23

Table 1-1 lists some of the standard features and specifications of the HS23 server.

Table 1-1 HS23 server specifications

Components	Specifications
Processor	Up to two Intel Xeon processor E5-2600 product family processors with eight-core (up to 2.7 GHz), six-core (up to 2.9 GHz), quad-core (up to 3.3 GHz), or dual-core (up to 3.0 GHz). Two QPI links up to 8.0 GT/s each. Up to 1600 MHz memory speed. Up to 20 MB L3 cache.
Chipset	Intel C600.

Components	Specifications
Memory	Up to 16 DDR3 DIMM sockets (8 DIMMs per processor) using very low profile (VLP) DIMMs. Support for up to 1600 MHz memory speed, depending on the processor. Four memory channels per processor (2 DIMMs per channel).
Memory maximums	Up to 512 GB with 16x 16 GB RDIMMs and two processors.
Memory protection	ECC, Chipkill, memory mirroring, and memory rank sparing.
Disk drive bays	Two 2.5" hot-swap SAS/SATA drive bays that support SAS, SATA, and SSD drives.
Maximum internal storage	Up to 1.8 TB with 900 GB 2.5" SAS HDDs, up to 2 TB with 1 TB 2.5" NL SAS HDDs, up to 2 TB with 1 TB 2.5" SATA HDDs, or up to 512 GB with 256 GB 2.5" SATA SSDs. Intermix of SAS and SATA HDDs and SSDs is supported.
RAID support	RAID 0, 1, 1E, and 10 with integrated LSI SAS2004 controller.
Network interfaces	Two Gigabit Ethernet ports and two 10 Gb Ethernet ports with integrated Emulex BladeEngine 3 (BE3) controller.
PCI Expansion slots	One CIOv slot (PCIe 3.0 x8) and one CFFh slot (PCIe 3.0 x16). Two extra PCIe 2.0 x8 standard form factor slots (slot 1 is full-height full-length, slot 2 is full-height half-length) with the optional PCI Express Gen 2 Expansion Blade II. One HS23 supports up to four PCIe expansion blades (8 slots). Up to four optional GPU expansion blades with either NVIDIA Tesla M2090, M2075, or M2070Q graphics processing units.
Ports	One internal USB port (for embedded hypervisor).
Hot-swap components	Hard disk drives.
Systems management	UEFI, IBM Integrated Management Module II (IMM2) with Renesas SH7757 controller, Predictive Failure Analysis, light path diagnostics panel, Automatic Server Restart, IBM Systems Director, and IBM Systems Director Active Energy Manager™, IBM ServerGuide.
Security features	Power-on password, administrator's password, Trusted Platform Module (TPM 1.2).
Video	Matrox G200eR2 video core with 16 MB video memory that is integrated into the IMM2. Maximum resolution is 1600x1200 at 75 Hz with 16 M colors (32 bits per pixel).
Operating systems supported	Microsoft Windows Server 2012, 2008 R2, and 2008 (x64), Red Hat Enterprise Linux 5 (x64) and 6 (x86 and x64), SUSE Linux Enterprise Server 10 (for AMD64/EM64T) and 11 (for x86 and AMD64/EM64T), VMware ESX 4.1 and ESXi 4.1, and VMware vSphere 5.

For more information about the HS23, see the IBM Redbooks product guide, available at:

<http://www.redbooks.ibm.com/abstracts/tips0843.html>

1.5.2 BladeCenter HS23E server

The IBM BladeCenter HS23E server is a performance for value blade server that is optimized for energy efficiency and density by offering flexible configuration options. Designed specifically for use in business critical and entry virtualization applications, the blade offers higher performance with 1600 MHz memory and optimal processor performance in a standard 30 mm form factor.

The HS23E supports the latest Intel Xeon processor E5-2400 product family, two ports of 1 Gb Ethernet, high-capacity, high-throughput memory, and high speed I/O, including Virtual Fabric adapters for IBM BladeCenter. In addition, the HS23E is compatible with the BladeCenter E, S, H, and HT chassis.

Figure 1-5 shows a blade server HS23E with its top cover removed.

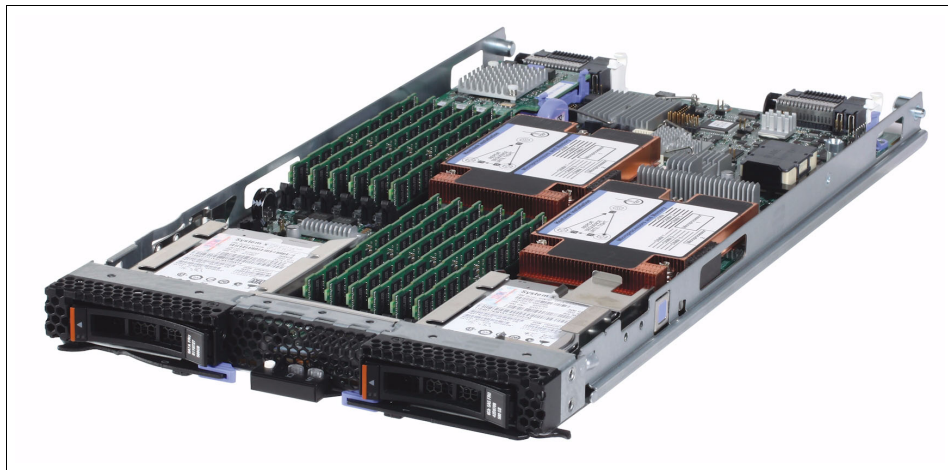


Figure 1-5 BladeCenter HS23E

Table 1-2 lists some of the standard features and specifications of the HS23 server.

Table 1-2 HS23E server specifications

Components	Specifications
Processor	Up to two Intel Xeon processor E5-2400 product family processors with eight cores (up to 2.3 GHz), six cores (up to 2.4 GHz), or four cores (up to 2.2 GHz), one QPI link up to 8.0 GTps, up to 1600 MHz memory speed, up to 20 MB L3 cache; one Intel Xeon processor E5-1410 with four cores at 2.8 GHz, 10 MB L3 cache, and 1333 MHz memory speed; or one Intel Pentium processor 1400 product family with two cores up to 2.8 GHz, 5 MB L3 cache, and 1066 MHz memory speed.
Chipset	Intel C600 series.
Memory	Up to 12 DDR3 DIMM sockets (six DIMMs per processor) using Very Low Profile (VLP) DIMMs. Support for up to 1600 MHz memory speed depending on the processor. Three memory channels per processor (two DIMMs per channel).
Memory maximums	Up to 192 GB with 12x 16 GB RDIMMs and two processors.
Memory protection	ECC, Chipkill, memory mirroring, and memory sparing.
Disk drive bays	Two 2.5" hot-swap SAS/SATA drive bays that support SAS, SATA, and SSD drives.
Maximum internal storage	Up to 1.8 TB with 900 GB 2.5-inch SAS HDDs, up to 2 TB with 1 TB 2.5-inch NL SAS or SATA HDDs, or up to 400 GB with 200 GB 2.5-inch SATA SSDs. An intermix of SAS and SATA HDDs and SSDs is supported by the optional H1135.
RAID support	Up RAID 0 and 1 with C105 (support for SATA HDDs only). Optional RAID 0, 1, 10, and 1E with H1135 (support for SAS/SATA HDDs and SSDs).
Network interfaces	Two Gigabit Ethernet ports with an integrated Broadcom BCM5718 controller.
PCI Expansion slots	One CIOv slot (PCIe 3.0 x8) and one CFFh slot (PCIe 3.0 x16). Two extra PCIe 2.0 x8 standard form factor slots (slot 1 is full-height full-length, slot 2 is full-height half-length) with the optional PCI Express Gen 2 Expansion Blade II. One HS23 supports up to four PCIe expansion blades (8 slots). Up to four optional GPU expansion blades with either NVIDIA Tesla M2090, M2075, or M2070Q graphics processing units.
Ports	One internal USB port (for embedded hypervisor).
Hot-swap components	Hard disk drives and solid-state drives.

Components	Specifications
Systems management	UEFI, Renesas SH7757 controller-based IBM Integrated Management Module II (IMM2) with remote presence (graphics, keyboard and mouse, and virtual media), Predictive Failure Analysis, light path diagnostics panel, Automatic Server Restart, IBM Systems Director, IBM Systems Director Active Energy Manager, IBM ServerGuide, and IBM FastSetup.
Security features	Power-on password, administrator's password, Trusted Platform Module (TPM 1.2).
Video	Matrox G200eR2 video core with 16 MB video memory that is integrated into the IMM2. Maximum resolution is 1600x1200 at 75 Hz with 16 M colors (32 bits per pixel).
Operating systems supported	Microsoft Windows Server 2008 R2 and 2008 (x64), Red Hat Enterprise Linux 5 (x64) and 6 (x86 and x64), SUSE Linux Enterprise Server 10 (x64) and 11 (x86 and x64), VMware ESX 4.1 and ESXi 4.1 embedded hypervisor, VMware vSphere 5 and 5.1.

For more information about the HS23E, see the IBM Redbooks product guide, available at:

<http://www.redbooks.ibm.com/abstracts/tips0887.html>

1.5.3 BladeCenter HX5 server

The IBM BladeCenter HX5 Type 7873, 7872, 1910, and 1909 blade servers are high-density, scalable blade servers that are ideally suited for high performance and virtualized environments. A BladeCenter HX5 can be combined with the IBM MAX5 for BladeCenter expansion blade to provide memory expansion for medium to large businesses.

The IBM BladeCenter HX5 server is a blade server that is based on the fifth generation of the IBM Enterprise X-Architecture®. It delivers innovation with enhanced scalability, reliability, and availability features to enable optimal performance for databases, enterprise applications, and virtualized environments.

The IBM BladeCenter HX5 supports up to two processors, using latest "EX" generation of Intel Xeon processor E7 family. Two HX5 servers can be connected together for a high-performance single image with four processors and up to 1 TB of RAM in a blade form factor. For applications that must maximize available memory but that do not need four processors, a single HX5 server can be attached to an MAX5 memory expansion blade to form a single image with two processors and up to 1.25 TB of RAM. This level of processing and memory capacity is ideal for large-scale database or virtualization requirements.

Figure 1-6 shows a four socket HX5 blade server.

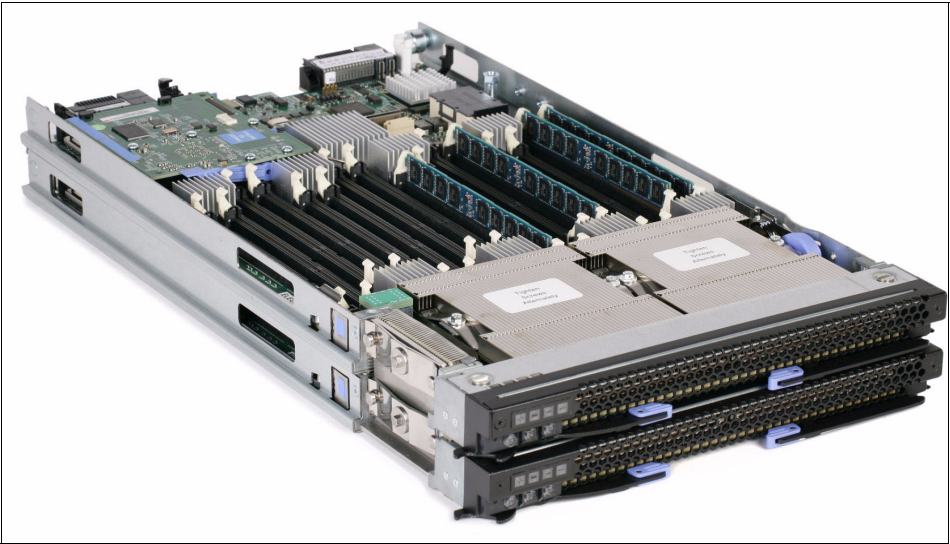


Figure 1-6 Two IBM BladeCenter HX5 servers forming one single 4-way server

Table 1-3 lists some of the standard features and specifications of the HX5 server.

Table 1-3 HX5 server specifications

Components	Specifications
Processor	Machine type 7873: Intel Xeon E7-8800, E7-4800, and E7-2800 families, up to 10 cores Intel Xeon 7500 and 6500 processors; 4/6/8 cores, up to 2.66 GHz. Up to two processors per single wide HX5; scalable to four processors.
Chipset	Machine type 7873: Intel Xeon E7-8800, E7-4800, and E7-2800 families, up to 10 cores.
Memory	Single node: 16 DIMM sockets. Two nodes: 32 DIMM sockets total. Single node + MAX5: 40 DIMM sockets total (MAX5 adds 24 sockets).
Memory maximums	Machine type 7873 supports the use of 32 GB DIMMs: <ul style="list-style-type: none">▶ Single node: 512 GB.▶ Two nodes: 1 TB.▶ Single node + MAX5: 1.25 TB.
Memory protection	ECC, ChipKill, Memory Mirroring, Memory Sparing, Redundant Bit Steering (MAX5 or servers with E7 processors only, x4 DIMMs only).
Disk drive bays	Two non-hot-swap bays per single-wide HX5 supporting solid-state drives.

Components	Specifications
Maximum internal storage	Up to 800 GB of solid-state storage per single-wide HX5 (with 400 GB SSDs).
RAID support	Optional RAID-0, -1, -1E.
Network interfaces	Broadcom 5709S onboard NIC with dual Gigabit Ethernet ports with TOE Some models: Emulex Virtual Fabric 10 Gb Expansion Card (CFFh).
PCI Expansion slots	One CIOv slot (standard PCIe daughter card) and one CFFh slot (high-speed PCIe daughter card) for total of eight ports of I/O to each blade. This number includes four ports of high-speed I/O Scalable, and up to 16 ports of I/O in 4-socket, double wide form factor.
Ports	One internal USB port (for embedded hypervisor).
Hot-swap components	Hard disk drives and solid-state drives.
Systems management	Integrated systems management processor.
Security features	Power-on password, administrator's password, Trusted Platform Module (TPM 1.2).
Video	Integrated Matrox G200eV video controller.
Operating systems supported	Microsoft Windows, Red Hat Linux, SUSE Linux, VMware.

For more information about the HX5, see the IBM Redbooks product guide, available at:

<http://www.redbooks.ibm.com/abstracts/tips0824.html?Open>

1.5.4 BladeCenter PS700, PS701, PS702 servers

The BladeCenter PS700, PS701, and PS702 blades are Power Systems blades for 64-bit applications. Based on IBM Performance Optimization with Enhanced RISC (IBM POWER®) Architecture technologies, they are designed to minimize complexity, improve efficiency, automate processes, reduce energy consumption, and scale easily. The IBM POWER7® processor-based blades support AIX, IBM i, and Linux operating systems. Their ability to coexist in the same chassis with other IBM BladeCenter blade servers enhances the ability to deliver the rapid return of investment (ROI) that is demanded by clients and businesses.

Figure 1-7 shows the IBM BladeCenter PS700, PS701, and PS702 blade servers.



Figure 1-7 IBM BladeCenter PS702, BladeCenter PS701, and BladeCenter PS700

BladeCenter PS700 server

The PS700 blade server (8406-70Y) is a single socket, single wide 4-core 3.0 GHz POWER7 processor-based server. The POWER7 processor is a 64-bit, 4-core with 256 KB L2 cache per core and 4 MB L3 cache per core.

The PS700 blade server has eight DDR3 memory DIMM slots. The industry standard VLP DDR3 Memory DIMMs are either 4 GB or 8 GB running at 1066 MHz. The memory is supported in pairs, so the minimum memory required for the PS700 blade server is 8 GB (two 4 GB DIMMs). The maximum memory that can be supported is 64 GB (eight 8 GB DIMMs).

The blade server has two Host Ethernet Adapters (HEA) 1 GB integrated Ethernet ports that are connected to the BladeCenter chassis fabric (midplane). The PS700 has an integrated SAS controller that supports local (onboard) storage, integrated USB controller and Serial over LAN console access through the service processor, and the BladeCenter Advance Management Module.

It supports two onboard disk drive bays. The onboard storage can be one or two 2.5-inch SAS HDD or SSD drives. The integrated SAS controller supports RAID 0, RAID 1, and RAID10 hardware when two HDDs or solid-state drives (SSDs) are used.

The PS700 also supports one PCIe CIOv expansion card slot and one PCIe CFFh expansion card slot. Table 1-4 shows the specification for the BladeCenter PS700.

Table 1-4 PS700 specifications

Component	Specifications
Processor	Single four-core, 64-bit POWER7 3.0 GHz processor with 256 KB per processor core L2 cache and 4 MB per processor core L3 cache.
Chipset	64-bit POWER7 processors (12S technology).
Memory	Eight VLP DIMM slots. Supports 4 GB DDR3 and 8 GB DDR3 at 1066 MHz.
Memory maximums	64 GB maximum.
Memory protection	IBM Chipkill ECC detection and correction.
Disk drive bays	First DASD bay: Zero or one 2.5" SAS HDD. Second DASD bay: Zero or one 2.5" SAS HDD.
Maximum internal storage	SAS HDDs are 300 GB and 600 GB.
RAID support	RAID 0, RAID 1, and RAID10 hardware when two HDDs or SSDs are used.
Network interfaces	Two 1 GB Ethernet ports (HEA) (two on each side).
PCI Expansion slots	1Xe expansion card (CIOv). 1 SAS Pass-through using 1Xe. 1 High-Speed expansion card (CFFh).
Hot-swap components	Hot-swappable disk bays (in BladeCenter S chassis). Hot-plug power supplies and cooling fans (on chassis).
Systems management	Integrated systems management processor, IBM Systems Director Active Energy Manager, light path diagnostics panel, Predictive Failure Analysis, Cluster Systems Management (CSM), Serial Over LAN, IPMI compliant.
Video	No on-board video chips, and does not support KVM connections.
Operating systems supported	AIX V5.3 or later, AIX V6.1 or later. IBM i 6.1 or later. SUSE Linux Enterprise Server 10 for POWER (SLES10 SP3) or later; SLES11 SP1 or later. Red Hat Enterprise Linux 5.5 for POWER (RHEL5.5) or later; RHEL5.1 or later.

For more information about the PS700, see *IBM BladeCenter PS700, PS701, and PS702 Technical Overview and Introduction*, REDP-4655, available at:
<http://www.redbooks.ibm.com/redpapers/pdfs/redp4655.pdf>

BladeCenter PS701 server

The PS701 blade server (8406-71Y) is a single socket, single-wide 8-core 3.0 GHz POWER7 processor-based server. The POWER7 processor is a 64-bit, 8-core processor with 256 KB L2 cache per core and 4 MB L3 cache per core.

The PS701 blade server has 16 DDR3 memory DIMM slots. The industry-standard VLP DDR3 memory DIMMs are either 4 GB or 8 GB running at 1066 MHz. The memory is supported in pairs, so the minimum memory that is required for PS701 blade server is 8 GB (two 4 GB DIMMs). The maximum memory that can be supported is 128 GB (16x 8 GB DIMMs).

The PS701 blade server has two HEA 1 GB integrated Ethernet ports that are connected to the BladeCenter chassis fabric (midplane). The PS701 also has an integrated SAS controller that supports local (onboard) storage, integrated USB controller and Serial over LAN console access through the service processor, and the BladeCenter Advance Management Module.

The PS701 has one onboard disk drive bay. The onboard storage can be one 2.5-inch SAS HDD or SSD drive. The PS701 also supports one PCIe CIOv expansion card slot and one PCIe CFFh expansion card slot. Table 1-5 shows the specifications for the BladeCenter PS701.

Table 1-5 PS701 specifications

Component	Specifications
Processor	Single four-core, 64-bit POWER7 3.0 GHz processor with 256 KB per processor core L2 cache and 4 MB per processor core L3 cache.
Memory	16 VLP DIMM slots; Supports 4 GB DDR3 and 8 GB DDR3 at 1066 MHz.
Memory maximums	128 GB maximum.
Memory protection	IBM Chipkill ECC detection and correction.
Disk drive bays	One disk bay, supporting one 2.5-inch SAS HDD.
Maximum internal storage	SAS HDDs are 300 GB and 600 GB.
RAID support	n/a.
Network interfaces	Two 1 GB Ethernet ports (HEA) (two on each side).

Component	Specifications
PCI Expansion slots	One CIOv PCIe expansion card slot and one CFFh PCIe high-speed expansion card slot.
Hot-swap components	Hot-swappable disk bays (in BladeCenter S chassis). Hot-plug power supplies and cooling fans (on chassis).
Systems management	Integrated systems management processor, IBM Systems Director Active Energy Manager, light path diagnostics panel, Predictive Failure Analysis, CSM, Serial Over LAN, IPMI compliant.
Video	No on-board video chips, and does not support KVM connections.
Operating systems supported	AIX V5.3 or later, AIX V6.1 or later. IBM i 6.1 or later. SUSE Linux Enterprise Server 10 for POWER (SLES10 SP3) or later; SLES11 SP1 or later. Red Hat Enterprise Linux 5.5 for POWER (RHEL5.5) or later; RHEL5.1 or later.

For more information about the PS701, see *IBM BladeCenter PS700, PS701, and PS702 Technical Overview and Introduction*, REDP-4655, available at:

<http://www.redbooks.ibm.com/redpapers/pdfs/redp4655.pdf>

BladeCenter PS702 server

The PS702 blade server (8406-71Y +FC 8358) is a two socket, double-wide 16-core 3.0 GHz POWER7 processor-based server. The POWER7 processor is a 64-bit, 8-core with 256 KB L2 cache per core and 4 MB L3 cache per core.

The PS702 combines a single-wide base blade (PS701) and an expansion unit (feature code 8358), referred to as a double-wide blade, that occupies two adjacent slots in the BladeCenter chassis.

The PS702 blade server has 32 DDR3 memory DIMM slots. The industry-standard VLP DDR3 memory DIMMs are either 4 GB or 8 GB running at 1066 MHz. The memory is supported in pairs. The minimum memory that is required for the PS702 blade server is 8 GB (two 4 GB DIMMs). The maximum memory that can be supported is 256 GB (32x 8 GB DIMMs).

The PS702 blade server has four Host Ethernet Adapter 1 GB integrated Ethernet ports that are connected to the BladeCenter chassis fabric (midplane). The PS702 also has an integrated SAS controller that supports local (onboard)

storage, integrated USB controller and Serial over LAN console access through the service processor, and the BladeCenter Advance Management Module.

The PS702 blade server has two disk drive bays: One on the base blade and one on the expansion unit. The onboard storage can be one or two 2.5-inch SAS HDD or SSD drives. The integrated SAS controller supports RAID 0, RAID 1, and RAID 10 hardware when two HDDs or SSDs are used.

The PS702 supports two PCIe CIOv expansion card slots and two PCIe CFFh expansion card slots. Table 1-6 shows the specifications of the BladeCenter PS702.

Table 1-6 PS702 specifications

Component	Specifications
Processor	Two eight-core, 64-bit POWER7 3.0 GHz processor with 256 KB per processor core L2 cache and 4 MB per processor core L3 cache.
Memory	32 VLP DIMM slots. Supports 4 GB DDR3 and 8 GB DDR3 at 1066 MHz.
Memory maximums	256 GB maximum.
Memory protection	IBM Chipkill ECC detection and correction.
Disk drive bays	Two disk bays (one on each of the blade). On the base card, it can have one 2.5-inch SAS HDD. On the expansion unit, it can have one 2.5-inch SAS HDD.
Maximum internal storage	SAS HDDs are 300 GB and 600 GB.
RAID support	Hardware mirroring RAID 0, RAID 1 or RAID 10 when two HDDs are used.
Network interfaces	Four 1 GB Ethernet ports (HEA) (two on each system board).
PCI Expansion slots	Two CIOv expansion card slots and two CFFh expansion card slots.
Hot-swap components	Hot-swappable disk bays (in BladeCenter S chassis). Hot-plug power supplies and cooling fans (on chassis).
Systems management	Integrated systems management processor, IBM Systems Director Active Energy Manager, light path diagnostics panel, Predictive Failure Analysis, CSM, Serial Over LAN, IPMI compliant.
Video	No on-board video chips, and does not support KVM connections.

Component	Specifications
Operating systems supported	AIX V5.3 or later, AIX V6.1 or later. IBM i 6.1 or later1. SUSE Linux Enterprise Server 10 for POWER (SLES10 SP3) or later; SLES11 SP1 or later. Red Hat Enterprise Linux 5.5 for POWER (RHEL5.5) or later; RHEL5.1 or later.

For more information about the PS702, see *IBM BladeCenter PS700, PS701, and PS702 Technical Overview and Introduction*, REDP-4655, available at:

<http://www.redbooks.ibm.com/redpapers/pdfs/redp4655.pdf>

1.5.5 BladeCenter PS703 server

The BladeCenter PS703 server is a single-wide server that is based on POWER7 processors with up to 16 cores (8 per processor).

The POWER7 processor-based PS703 blade supports the AIX, IBM i, and Linux operating systems. The ability to coexist in the same chassis with other IBM BladeCenter blades servers enhances its ability to deliver rapid ROI demanded by clients and businesses.

PS704 withdrawn: The PS704 (double-wide version of the PS703) was withdrawn in 2012.

Figure 1-8 shows the IBM BladeCenter PS703 server.

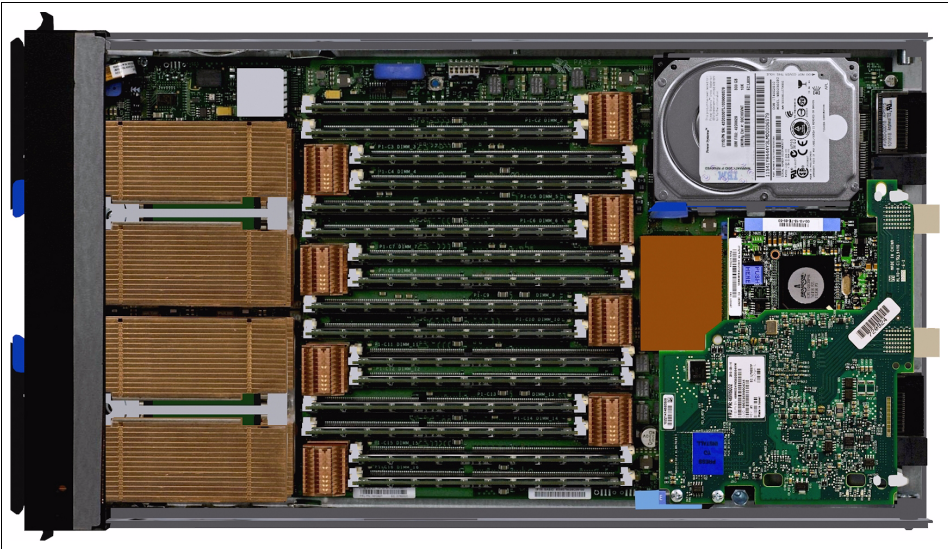


Figure 1-8 The IBM BladeCenter PS703

Table 1-7 summarizes the PS703 specifications.

Table 1-7 PS703 blade server specifications

Component	Specifications
Processor	Two 64-bit, 8-core 2.4 GHz processors with 256 KB L2 cache per core and 4 MB L3 cache per core.
Memory	16 VLP DDR3 memory RDIMM slots. The industry standard VLP DDR3 memory DIMMs are either 4 GB, 8 GB, or 16 GB running at 1066 MHz. Minimum memory that is required is 16 GB.
Memory maximums	256 GB.
Memory protection	Memory Scrubbing, ECC, and Chipkill.
Disk drive bays	One disk drive bays supports one 2.5-inch SAS HDD or two 1.8-inch SAS SSDs.
Maximum internal storage	One 600 GB 2.5-inch SAS10K non- hot-swappable HDD. Two 177 GB 1.8-inch SATA SSDs (requires feature number 4539).
RAID support	RAID 0, RAID 1, and RAID 10 when two HDDs or solid-state drives (SSDs) are used.

Component	Specifications
Network interfaces	Two 1-Gigabit Ethernet ports
PCI Expansion slots	<ul style="list-style-type: none"> – One CIOv expansion card slot (PCIe). – One CFFh expansion card slot (PCIe).
Hot-swap components	Hot-swappable disk bays (in BladeCenter S Chassis) Hot-plug power supplies and cooling fans (on chassis)
Systems management	Integrated systems management processor, IBM Systems Director Active Energy Manager, light path diagnostics panel, Predictive Failure Analysis, Cluster Systems Management for AIX (CSM), Serial Over LAN.
Video	No on-board video chips and no support for KVM connections.
Operating systems supported	AIX V5.3 or later, AIX V6.1 or later, AIX 7.1 or later. IBM i 6.1 or later, IBM i 7.1 or later. Novell SUSE Linux Enterprise Server 11 Service Pack 1 for POWER. Red Hat Enterprise Linux 5.6 for POWER or later. Red Hat Enterprise Linux 6.0 for POWER, or later.

For more information about the PS703, see *IBM BladeCenter PS703 and PS704 Technical Overview and Introduction*, REDP-4744, available at:

<http://www.redbooks.ibm.com/abstracts/redp4774.html>

1.6 BladeCenter S server support matrix

The BladeCenter can support a mixture of Power and IBM xSeries® blade servers. Table 1-8 on page 27 provides a more comprehensive list of the supported blade types and maximum numbers for the BladeCenter S chassis. It is important to understand that although there might be space to populate all bays, consider the limitations imposed by the power requirements for the entire BladeCenter.

Table 1-8 The blade servers that are supported in the BladeCenter S chassis

Blade	Machine type	Available	Blade width	Max blade number in BladeCenter S
HC10	7996	Withdrawn	1 slot	6
HS12	8014, 8028	Yes	1 slot	6
HS20	8832	Withdrawn	1 slot	6
HS20	8843	Withdrawn	1 slot	6
HS21	8853	Withdrawn	1 slot	6
HS21XM	7995	Withdrawn	1 slot	6
HS22	7870	Withdrawn	1 slot	Processors 95 W and lower: 6 Processors 130 W: 5
HS22V	7871	Withdrawn	1 slot	Processors 95 W and lower: 6 Processors 130 W: 5
HS23	7875	Yes	1 slot	6
HS23E	8038	Yes	1 slot	6
HX5	7872, 7873	Yes	1 or 2 slots	Single wide with processors 105 W & lower: 5 Single wide with processors 130 W: 4 HX5+MAX5 double-wide: 2
LS20	8850	Withdrawn	1 slot	6
LS21	7971	Withdrawn	1 slot	6
LS41	7972	Withdrawn	2 slot	3
JS12	7998-60X	Withdrawn	1 slot	6
JS21	8844	Withdrawn	1 slot	6
JS22	7998-61X	Withdrawn	1 slot	6
QS21	0792	Withdrawn	1 slot	6
QS22	0793	Withdrawn	1 slot	6
PS700	8406-70x	Yes	1 slot	6
PS701	8406-71x	Yes	1 slot	6
PS702	8406-71x	Yes	2 slots	3
PS703	7891-73x	Yes	1 slot	6
PS704	7891-74x	Withdrawn	2 slots	3



BladeCenter S technical overview

This chapter provides concise information about the components within the BladeCenter S chassis so you can better understand how they work before you start your deployment. The BladeCenter S is unique in the BladeCenter family because it has integrated internal storage that the Blade servers can access.

This chapter covers the following topics:

- ▶ 2.1, “BladeCenter S chassis” on page 31
- ▶ 2.2, “Storage modules” on page 34
- ▶ 2.3, “Drives” on page 37
- ▶ 2.4, “SAS Connectivity Module” on page 39
- ▶ 2.5, “SAS RAID Controller Module” on page 44
- ▶ 2.6, “SAS adapters” on page 51
- ▶ 2.7, “External SAS connectivity: Storage” on page 54
- ▶ 2.8, “Media tray” on page 55
- ▶ 2.9, “System LED panels with light path diagnostics” on page 58
- ▶ 2.10, “Advanced management module” on page 62
- ▶ 2.11, “Serial Pass-thru Module” on page 66
- ▶ 2.12, “I/O module bays” on page 68
- ▶ 2.13, “SAS tape storage for IBM BladeCenter” on page 75
- ▶ 2.14, “BladeCenter S Office Enablement Kit” on page 78
- ▶ 2.15, “Extra rack options” on page 80

- ▶ 2.16, “Power supply modules and redundancy” on page 82
- ▶ 2.17, “Power management policies” on page 86
- ▶ 2.18, “IBM uninterruptible power supply offerings” on page 95

2.1 BladeCenter S chassis

The IBM BladeCenter S (machine type 8886 and 7779) is designed to be used outside of a data center. It shares similar features to the other BladeCenter models, but offers a more flexible and customizable form factor. In addition, it uses the existing product portfolio of the BladeCenter family, and has model-specific options.

Figure 2-1 shows a populated BladeCenter S with two storage units, housing 12 disk drives.



Figure 2-1 BladeCenter S

The most stand out features is its onboard SAS/SATA storage capability. The BladeCenter S chassis can accommodate up to two storage modules. Two disk storage modules are available: Ones with six 3.5-inch drive bays and ones with twelve 2.5-inch drive bays. These disks can then be assigned directly to blade servers by using predefined or user definable customer configurations. The two Disk Storage Modules can support up to a total of 24 TB of share storage.

Both storage modules are accessible to all blades through a single SAS I/O module. However, with the addition of a second matching SAS I/O module, you can achieve higher levels of availability. When two matching modules are present, the modules provide redundant functionality, with each module able to access all hard disk drives in both storage modules. This enterprise-class redundant architecture allows for transparent data protection of all storage that is

contained within the storage modules. You can also replace either module while online.

The BladeCenter S can use 110 V electrical power, which is of particular interest to U.S.-based clients. Previously, all BladeCenter chassis required 220 V connections, which are readily available in most data centers. Most small to medium size offices in the US operate on standard 110 V power only. Although 220 V power is available, it is typically available only at circuit breakers. To accommodate the growing diversity of office locations and facility amenities, the BladeCenter S was designed with the ability to operate on either 110 V or 220 V power using its autosensing power supplies.

The BladeCenter S chassis is a robust and flexible physical platform. Its modular tool-free design allows easy access and maintenance. All external components (except running blade servers) are hot swappable, and release levers/handles are clearly marked.

The key features of the BladeCenter S are indicated in Figure 2-2 (front view) and Figure 2-3 on page 33 (rear view).

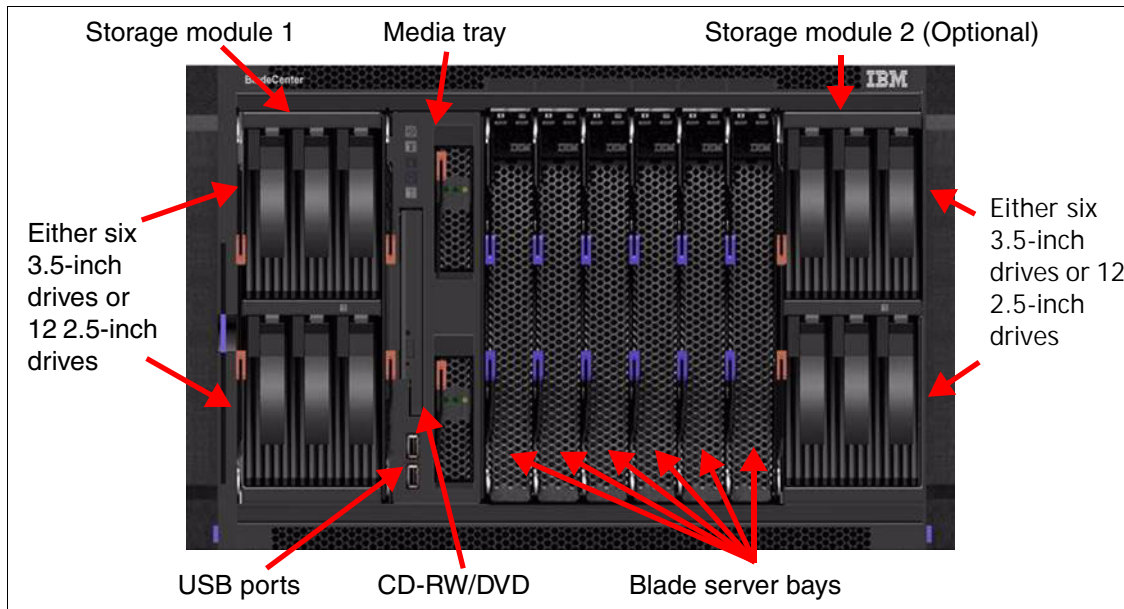


Figure 2-2 The front of the BladeCenter S chassis

Figure 2-3 shows the rear view of the BladeCenter chassis.

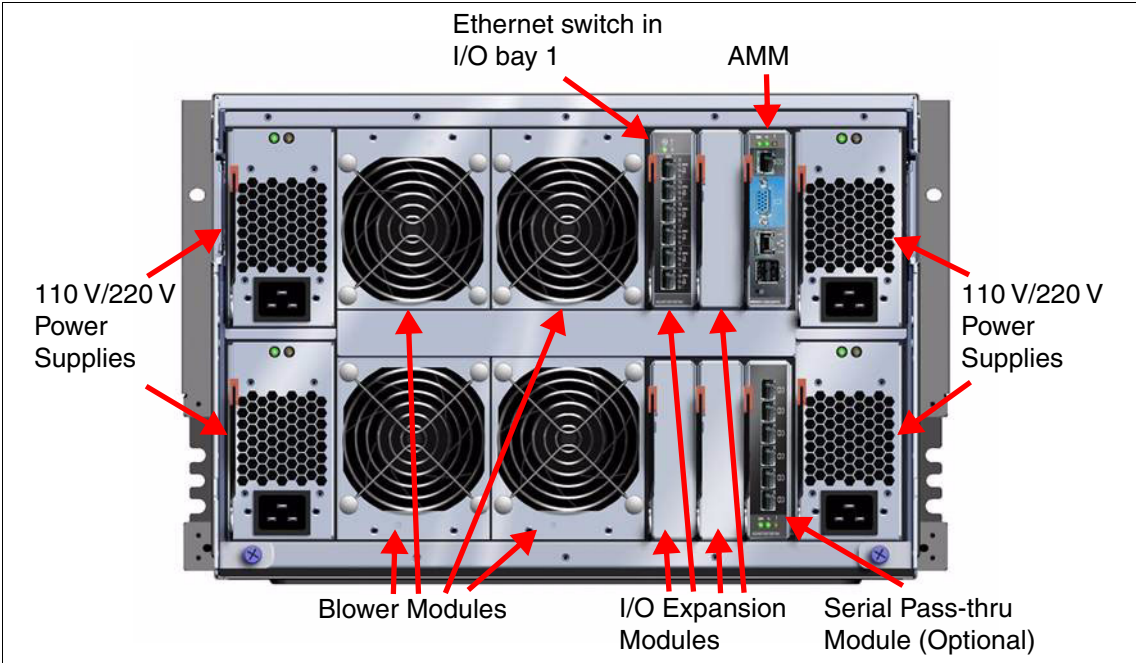


Figure 2-3 The rear of the BladeCenter S chassis

The BladeCenter S chassis allows for either six single-slot blade servers or three double-slot blade servers or a combination of the two. The BladeCenter S, like other BladeCenter chassis, supports both x86 and Power Systems blade servers. Different blade server models can be intermixed in a chassis simultaneously to support virtually any requirement (subject to power and cooling requirements).

Table 2-1 highlights the major features of the IBM BladeCenter S. Two models are available in specific locations, where the only difference is the input connectors on the power supplies.

Table 2-1 BladeCenter S features at a glance

Feature	Specification	
Machine type	8886-1MX	8886-1NG
Availability	Worldwide	Denmark, Switzerland, Sweden, China, Taiwan
Rack form factor (H x D)	7U x 28.9 inches (733.4 mm)	

Feature	Specification	
Disk storage modules (std/max)	1/2	
DVD/CD drives standard	1x CD-RW / DVD-ROM (in media tray)	
USB ports standard	2x USB 2.0 ports (in media tray)	
Serial pass-through capability	Yes	
Number of blade server slots	6 (30 mm blade servers)	
Number of I/O switch module bays	Four hot-swap	
Switch modules standard	None	
Power supply size standard	950 Watts AC (110 V) or 1450 Watts AC (220 V)	
Power input connectors	IEC 320 C20	IEC 320 C14
Number of power supplies (std/max)	2/4	
Number of blowers (std/max)	4/4	
Dimensions	Height: 12.0 inches (306 mm) Width: 17.5 inches (444 mm) Depth: 28.9 inches (733 mm)	

2.2 Storage modules

The storage module is fundamentally a collection of disk drives, which are made accessible to blade servers through the SAS switch module in the chassis and a SAS expansion card in each blade. You can install a maximum of two storage modules in the BladeCenter S chassis.

Two disk storage modules are available, ones with six 3.5-inch drive bays or ones with twelve 2.5-inch drive bays. You cannot mix a 2.5-inch storage module and a 3.5-inch storage module in the same chassis. Intermixing of SAS-based and SATA-based hard disks within the same storage module is supported. You can easily and quickly assign the drives directly to blades by using built-in predefined configurations or through user-defined custom configurations.

Four power supplies are required for the BladeCenter S chassis to support two Storage Modules. When adding a second Storage Module to the BladeCenter S chassis, you might need to add two extra power supplies, depending on your current configuration.

Part number information is shown in Table 2-2.

Table 2-2 Part number information

Part number	Feature code	Description
43W3581	1583	IBM BladeCenter S 6-Disk Storage Module
49Y3234	A3KS	IBM BladeCenter S 12-Disk Storage Module

Figure 2-4 shows the IBM BladeCenter S 6-Disk Storage Module.

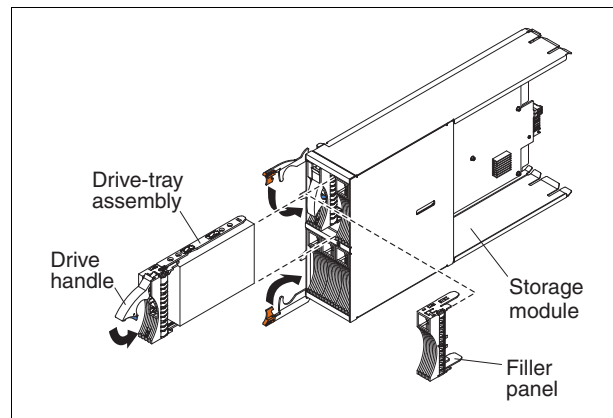


Figure 2-4 IBM BladeCenter S 6-Disk Storage Module

Figure 2-5 shows the BladeCenter S with 12-drive Disk Storage Modules.



Figure 2-5 BladeCenter S with 12-drive Disk Storage Modules installed

Both storage modules are accessible to all blades through one or two SAS switch modules. The use of the second SAS switch module provides higher levels of availability. When two SAS switch modules are installed, the modules provide redundant functionality because each module is able to access all hard disk drives in both storage modules. This enterprise-class redundant architecture allows transparent data protection of all storage that is contained within the storage modules. You can also replace either module while they are online.

12-drive DSM: The 12-drive disk storage module is only supported by the SAS RAID Controller Module.

The SAS switch module is responsible for both the provisioning of physical disk drives through zoning, and for failover redundancy when two SAS switch modules are present.

The SAS adapter in each blade server can address only those disks that are assigned to it from the SAS switch module, and can create arrays only from those disks.

The SAS Connectivity Card (CIOv) does not contain its own RAID controller. Instead, it passes through the RAID functions of the onboard RAID controller in the server. The ServeRAID H1135 adapter (CIOv) is supported by the BladeCenter HS23E server, and provides RAID functions in lieu of an onboard RAID controller.

Within each disk storage module, hard disk drives are numbered 1 through 6 from left to right, top to bottom.

To access the hard disks in the disk storage module, you must install these components:

- ▶ At least one SAS switch module. If you install a single SAS switch module, it controls access to both disk storage modules in the BladeCenter S chassis.
- ▶ A SAS adapter in each of the blade servers that accesses the integrated storage of the BladeCenter S.

To remove the standard storage module, unlatch the release handles on the front of the module and pull it straight out from the chassis. To reinstall the storage module, ensure that the release handles are at a 90° angle to the front of the module. Then, gently insert the module into the left-side storage module bay, ensuring that the release handles face the left side of the chassis. After you insert the module, lower the release handles and secure them flush against the module.

To install the optional storage module, first remove the drive cage filler by pulling it straight out from the chassis. Next, ensure that the release handles are at a 90° angle to the front of the module. Then, gently insert it into the right-side storage module bay, ensuring that the release handles face the left side of the chassis (release handles should be next to blade bay six). After you insert the module, lower the release handles and secure them flush against the module.

Depending upon the predefined storage configuration policy that you selected, it might be necessary to reselect a new zone configuration. Predefined storage configuration policies are specific and require a thorough understanding to ensure correct data protection.

For storage zone configuration information, see Chapter 3, “Getting started using the BladeCenter S chassis” on page 99.

Important: Insertion of the optional storage module 2 does not automatically provide data redundancy. It might be necessary to reselect a new storage configuration policy to achieve cross-module data protection.

2.3 Drives

The BladeCenter S chassis can have a maximum of two storage modules installed. A storage module and the hard disk drives installed in that storage module are commonly referred to as *integrated shared storage*. This storage is integrated in the BladeCenter S chassis and shared among the blade servers in the BladeCenter S system. Within each storage module, hard disk drives are numbered 1 through 6 from left to right, and top to bottom.

Cooling requirements: Because of the cooling design of the BladeCenter S, each hard disk drive location must contain either a hard disk or a drive filler.

The BladeCenter S Chassis storage module supports several disk drive types. For more information, see 1.4, “Disk Storage Module and Storage concepts” on page 8. It is important to understand the features and benefits of each type because there might be specific hardware requirements to support certain types.

- **SAS disk:** Serial Attached SCSI disks are designed and used for high performance requirements where maximum throughput and transaction capability is needed.

- ▶ **SATA disk:** Serial Advanced Technology Attachment disks are designed to provide lower-cost mass storage capacity, when compared to SAS disk. they are used in systems where performance is not a requirement.
- ▶ **Near line (NL) disks:** The NL disk is designed to provide lower-cost mass storage capacity, and can be either a SATA or SAS disk.

Drive support: The SAS RAID Controller Module (43W3584) supports only SAS and NL SAS drives. The SAS Connectivity Module (39Y9195) supports all drive types. SSD drives are not supported at the time of writing.

The drives listed in Table 2-3 are supported by the 6-drive disk storage module and available at the time of writing.

Table 2-3 Available drives for 6-drive disk storage module in BladeCenter S

Part number	Feature Code	Hard disk drive	SAS Connectivity Module	SAS RAID Controller Module	Maximum quantity
3.5 inch Hot-Swap SAS					
44W2234	5311	300 GB 15 K SAS	Yes	Yes	12 (6 per DSM)
44W2239	5312	450 GB 15 K SAS	Yes	Yes	12 (6 per DSM)
44W2244	5313	600 GB 15 K SAS	Yes	Yes	12 (6 per DSM)
3.5 inch Hot-Swap SATA					
43W7630	5561	1 TB 7.2 K Dual Port SATA	Yes	No	12 (6 per DSM)
3.5 inch Hot-Swap NL SAS					
42D0777	5418	1 TB 7.2 K NL SAS	Yes	Yes	12 (6 per DSM)
42D0767	5417	2 TB 7.2 K NL SAS	Yes	Yes	12 (6 per DSM)

The drives listed in Table 2-4 are supported by the 12-drive disk storage module and available at the time of writing.

Table 2-4 Available drives for 12-drive disk storage module in BladeCenter S

Part number	Feature Code	Hard disk drive	SAS Connectivity Module	SAS RAID Controller Module	Maximum quantity
42D0637	5599	IBM 300GB 2.5in SFF Slim-HS 10K 6Gbps SAS HDD	No	Yes	12 per DSM (24 total)
90Y8877	A2XC	IBM 300GB 2.5in SFF 10K 6Gbps HS SAS HDD	No	Yes	12 per DSM (24 total)
90Y8872	A2XD	IBM 600GB 2.5in SFF 10K 6Gbps HS SAS HDD	No	Yes	12 per DSM (24 total)
81Y9650	A282	IBM 900GB 2.5in SFF HS 10K 6Gbps SAS HDD	No	Yes	12 per DSM (24 total)
42D0677	5536	IBM 146GB 2.5in SFF Slim-HS 15K 6Gbps SAS HDD	No	Yes	12 per DSM (24 total)
81Y9670	A283	IBM 300GB 2.5in SFF HS 15K 6Gbps SAS HDD	No	Yes	12 per DSM (24 total)

2.4 SAS Connectivity Module

The SAS Connectivity Module (part number 39Y9195) is a SAS expander. It provides the connectivity and access between the blades and the disks in the disk storage modules. It also provides four external SAS ports for further connectivity. The data paths are controlled by predefined or user-defined zone configurations. These paths are provided:

- ▶ Internal paths in the chassis from the blades to the disks
- ▶ Internal paths in the chassis from the blades to the external ports of the SAS Connectivity Module

Each blade must have a suitable SAS adapter installed to allow it to connect to the storage through the SAS Connectivity Module.

The SAS Connectivity Module *only* provides the connectivity between the SAS devices that are installed in the BladeCenter S. The blade server's onboard RAID controller (or the ServeRAID H1135 adapter in the case of the HS23E) provides fault tolerance.

You can install up to two SAS Connectivity Modules in the BladeCenter S:

- ▶ The SAS Connectivity Modules are installed in I/O module bays 3 and 4.
- ▶ If you install only one SAS Connectivity Module, you must install it in I/O module bay 3.

Restriction: The 12-drive DSM is not supported with the SAS Connectivity Module. Instead, you must use the SAS RAID Controller Module.

The part number information is shown in Table 2-5.

Table 2-5 Part number information

Part number	Feature code	Description
39Y9195	2980	IBM BladeCenter SAS Connectivity Module

Figure 2-6 shows the SAS Connectivity Module.



Figure 2-6 The IBM SAS Connectivity Module

2.4.1 Features and specifications

The SAS Connectivity Module supports the following features:

- ▶ Based on the Vitesse 7157 controller
- ▶ Serial SCSI Protocol (SSP)
- ▶ Serial Management Protocol (SMP) as defined in the SAS specification
- ▶ 14 internal x1 links to blade servers
- ▶ Four external x4 links for storage servers
- ▶ Link error detection

Figure 2-7 shows the external features of the SAS Connectivity Module.

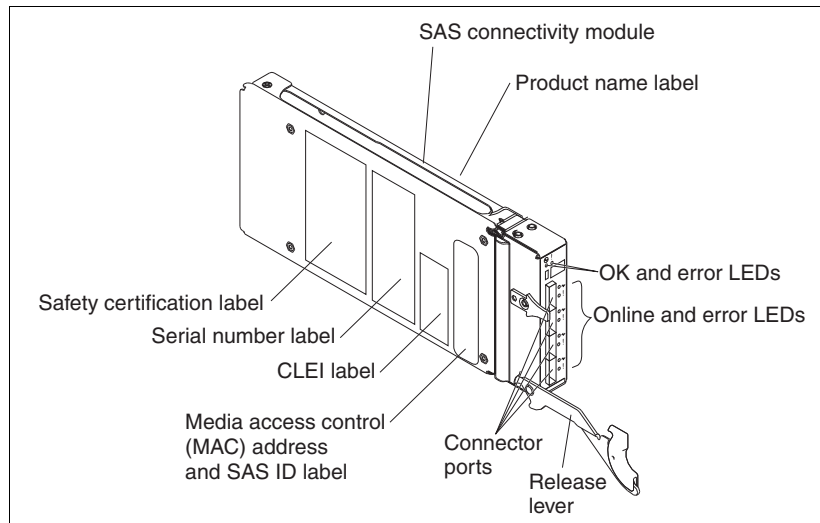


Figure 2-7 Major components of the SAS Connectivity Module

Table 2-6 lists the specifications of the device.

Table 2-6 SAS Connectivity Module specifications

Type	Specifications
Built-in diagnostic tests	Power-on self-test (POST) is run on all functional components. Port operational tests include internal, external, and online tests.
User interface	LED indicators display link activity and faulty connections

Type	Specifications
Fabric management	<ul style="list-style-type: none"> ▶ Telnet and command-line interface (CLI) ▶ Web-browser interface ▶ Advanced management module web interface ▶ Storage Configuration Manager interface ▶ SAS module Simple Network Management Protocol (SNMP) agent: Enables a network management workstation to receive configuration values and SAS link data through SNMP and the Ethernet interface.
Dimensions	Width: 112 mm (4.41 in.) Height: 29 mm (1.14 in.) Depth: 260 mm (10.25 in.) Weight: 0.91 kg (2 lb)
Electrical	Power source loading: 2 amps maximum at 12 V dc Heat output: 20 watts maximum Operating voltage: 12 V dc Circuit protection: Internally fused

2.4.2 SAS Connectivity Module administration tools

You can administer the SAS Connectivity Module by using a number of management tools.

Note: You must assign an IP address to the SAS Connectivity Module before you can manage it. You can do this by using the advanced management module (AMM). The IP address that you select must be on the same subnet as the AMM.

The following management tools are available to administer the SAS Connectivity Module:

- ▶ AMM browser interface
- ▶ SAS Connectivity Module browser interface
- ▶ Storage Configuration Manager
- ▶ Telnet and the CLI

Depending on the task that you are required to perform, select one of these tools:

- ▶ The CLI interface provides you with the most functions, but generally is not required for day-to-day administration use.
- ▶ Storage Configuration Manager is the most versatile and simplest of the web-based tools available to use with the SAS Connectivity Modules.

For more information about the Storage Configuration Manager, see 4.2, “Understanding storage zones” on page 168. Chapter 4, “Configuring storage” on page 165 provides a summary of the features and usage of each web-based tool.

You can also configure a management station that supports SNMP to receive information from the SAS Connectivity Module through its SNMP agent.

As with all BladeCenter I/O modules, the SAS Connectivity Module comes standard with an intuitive LED system that you can use to quickly diagnose problems with the module or external port connections. These LEDs are shown in Figure 2-8. You can use the management tools to further diagnose a problem if a problem occurs.

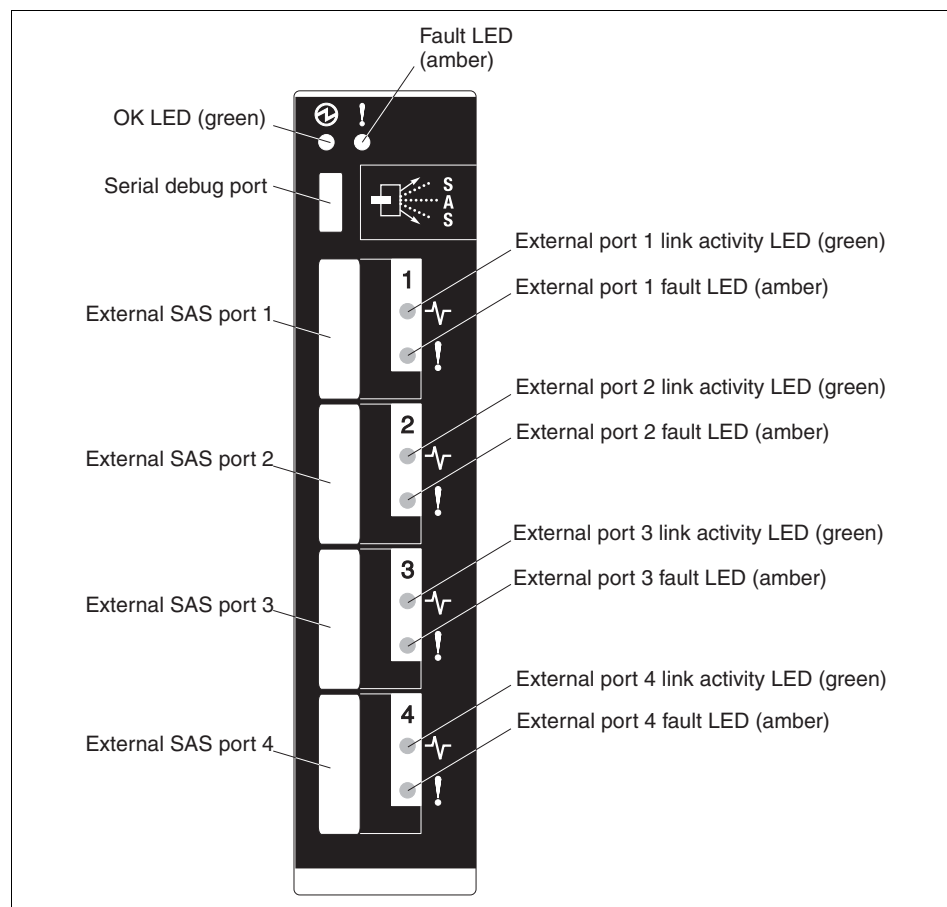


Figure 2-8 Ports and LED indicators on the SAS Connectivity Module

2.5 SAS RAID Controller Module

The SAS RAID Controller Module (part number 43W3584) is often called the RSSM or RAID SAS Switch Module. It provides RAID functions to the BladeCenter S disk subsystem by providing redundant SAN shared storage capability. It supports RAID 0,1,5, and 10 and uses a battery-backed cache to the controllers for reliability using battery backup units. Use the SAS RAID Controller Module when you require maximum performance, reliability, and flexibility with regards to storage allocation.

The part number information is shown in Table 2-7.

Table 2-7 Part number information

Part number	Feature code	Description
43W3584	5453	IBM BladeCenter S SAS RAID Controller Module (Includes one battery backup unit)
00Y3447	7589	IBM BladeCenter RAID Battery Backup Module (replacement)

The SAS RAID Controller Module is shown in Figure 2-9.



Figure 2-9 IBM SAS RAID Controller Module

The SAS RAID Controller Module includes two built-in subsystems:

- ▶ A RAID Controller subsystem for management of disks
- ▶ A SAS switch subsystem for management of zone configuration information

The SAS RAID Module Firmware Update Package Version 1.2.4.011 enables the BladeCenter S chassis to support a single RAID controller configuration. When in the single controller configuration, the SAS RAID Controller Module must be installed in I/O Bay 3.

Every SAS RAID Controller Module is also shipped with a Battery Backup Unit. Although the SAS RAID Controller module can function without the Battery Backup Unit installed, there are performance advantages when it is used. For more information, see 2.5.4, “Battery Backup Units” on page 49.

Unlike the SAS Connectivity Module that allocates entire physical disks to blades, the SAS RAID Controller Module allocates storage by mapping volumes. The high-level process involves the following steps:

1. One or two disks are assigned specifically as global spares. This is not a requirement, but this configuration provides more redundancy to your storage configuration.
2. The remaining disks are then grouped to form a storage pool or pools. You can form multiple storage pools if you have enough disks. The RAID level that you select determines the minimum number of disks that are required per storage pool at the time of creation.
3. The storage pool is then carved up into volumes that meet your sizing requirements. Volumes are the basic unit of storage that is provided to the blades.

Note: Each blade that you want to map a volume to must have a SAS Expansion Card installed. No further configuration of the SAS Expansion Card is required.

4. The new volumes are then mapped to a single blade, or multiple blades if shared storage is required between the blades. You do not have to map a volume to a blade at time of creation, but the blade has access to this volume until the mapping process is completed.
5. This volume is then formatted by the operating system that runs on the respective blade.

The maximum configurable size for Volumes and Storage Pools within the IBM SAS RAID Controller Module varies based on the version of firmware that is

installed on the modules. Table 2-8 lists the maximum volume size for different RAID configurations on firmware level 1.2.

Table 2-8 Maximum volume and pool size for firmware version 1.2.x.xxx

RAID level	Maximum volume size	Maximum pool size
RAID 0	11 TB	11 TB
RAID 1	1 TB	1 TB
RAID 5	9.5 TB	9.5 TB
RAID 10	5.5 TB	5.5 TB

Table 2-9 lists the maximum volume size for different RAID configurations and firmware level 1.0.

Table 2-9 Maximum volume/pool size for firmware version 1.0.x.xxx

RAID level	Maximum volume size	Maximum pool size
RAID 0	2 TB	8 TB
RAID 1	1 TB	1 TB
RAID 5	2 TB	8 TB
RAID 10	2 TB	5.5 TB

2.5.1 Features and specifications

The SAS RAID Controller Module supports the following features:

- ▶ Six internal 1X SAS 3.0 Gb host connectivity to six blade slots
- ▶ Two internal 4X SAS 3.0 Gb to two disk storage module (DSM) systems
- ▶ 1 GB total memory cache per controller (2 x 512 MB)
- ▶ 1 Gb Ethernet for RAID management
- ▶ 10/100 Ethernet for switch management
- ▶ RAID 0,1,5, and 10
- ▶ Serial SAS Protocol
- ▶ SMP as defined in the SAS specification
- ▶ 14 internal x1 links to Blade servers
- ▶ SAS and NL SAS disk (no SATA disk support)
- ▶ Hot-swap capable
- ▶ Supports Microsoft clustering (version specific)
- ▶ Supports VMware VMotion (version specific)

Table 2-10 lists the SAS RAID Controller Module specifications.

Table 2-10 SAS RAID Controller Module specifications

Type	Specifications
Built-in diagnostic tests	Power-on self-test (POST) is run on all functional components. Port operational tests include internal, external, and online tests.
User interface	LED indicators display link activity and faulty connections
Fabric management	<ul style="list-style-type: none">▶ Telnet and CLI▶ Web-browser interface▶ AMM web interface▶ Storage Configuration Manager interface▶ SAS module SNMP agent: Enables a network management workstation to receive configuration values and SAS link data through SNMP and the Ethernet interface.
SAS RAID Controller Module Dimensions	Width: 112 mm (4.41 in) Height: 29 mm (1.14 in) Depth: 260 mm (10.25 in) Weight: 0.91 kg (2 lb)
Battery Backup Unit dimensions	Depth: 414.08 mm (16.3 in) Width: 78.65 mm (3.10 in) Height: 22.4 mm (0.88 in) Weight: 1.32 Kg (2.91 lb)
Electrical	Power source loading: 2 amps maximum at 12 V dc Heat output: 20 watts maximum Operating voltage: 12 V dc Circuit protection: Internally fused

The maximum configurable size for volumes and storage pools within the IBM SAS RAID Controller Module (RSSM) varies based on the version of firmware that is installed on the modules.

2.5.2 SAS RAID Controller Module administration tools

You can administer the SAS RAID Controller Module by using a number of management tools.

Note: You must assign a unique IP address to both the SAS switch subsystem and RAID controller subsystem before you can manage the SAS RAID Controller Module. You assign these IP addresses by using the AMM.

The IP addresses you choose must be on the same subnet as the AMM.

The following management tools are available to administer the SAS RAID Controller Module:

- ▶ AMM browser interface
- ▶ SAS Switch browser interface
- ▶ Storage Configuration Manager
- ▶ Telnet and the CLI

Note: The command-line interface through Telnet is the most comprehensive tool when it comes to pure functionality. However, from an ease of use perspective the Storage Configuration Manager is the tool of choice.

2.5.3 Comparison table of the two SAS module types

Table 2-11 provides an overview of the comparative features of the two SAS modules that are offered for BladeCenter S.

Table 2-11 SAS module comparison table

Feature or requirement	SAS Connectivity Module	SAS RAID Controller Module
Minimum number of modules required	1	1 ^a
RAID support	None locally. Requires SAS Expansion Card to manage RAID. 0, 1 and 0+1.	0,1,5, and 0+1.
Disk support	SAS, SATA, SAS NL, or intermix.	SAS, SAS NL, or intermix of both.
Spare drive	Cannot assign spare drive. Spare drive is controlled by using blade only.	Global: Provides protection for all drives of a supported type with the disk storage modules.
Storage Allocation to Blades	Through physical disk allocation.	Through volume mapping.
Cache Memory protection	Feature not available.	Yes, using the Battery Backup Units ^b .
External SAS expansion ports	Yes	Yes

a. Requires firmware 1.2.4.011 or higher to support single stand-alone SAS RAID controller

- b. Although not mandatory, install a Battery Backup Unit for performance improvements and reliability.

Use with an ICPM: If you are using an Intelligent Copper Pass-thru Module (ICPM) for Ethernet connectivity, the following ICPM ports must be connected to the same network as the AMM:

- ▶ A chassis with a single RSSM in I/O bay 3 must have port 7 connected.
- ▶ A chassis with a single RSSM in I/O bay 4 must have port 14 connected.
- ▶ A chassis with two RSSMs must have port 7 and port 14 connected.

These connections are required for correct operation of the SAS RAID Controller Module. This configuration allows the RSSMs to be managed either with the CLI or Storage Configuration Manager (SCM).

For more information, see *IBM SAS RAID Controller Module Installation and User's Guide*, which is available at:

<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5078491>

2.5.4 Battery Backup Units

Battery Backup Units (part number: 22R6833) are installed to provide backup for the cache in the SAS RAID Controller Module. They provide enough reserve power to store data in cache for 72 hours in the event of a power failure. This reserve can be monitored by using the Storage Configuration Manager interface.

The Battery Backup Unit is shown in Figure 2-10.



Figure 2-10 Battery Backup Module for SAS RAID Controller Module

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

The Backup Battery Units automatically recharge after they are inserted into the IBM BladeCenter S chassis. However, like all batteries, they degrade over time. Therefore, install them immediately so that they can begin recharging. Do not remove them from the BladeCenter S chassis for prolonged periods of time.

The Backup Battery Unit has an expiration date that ensures it has at least 72 hours of capacity left after you are notified that the device is expired. You receive your first notification within 90 days of expiration. A second and final notification occurs 15 days before expiration. Replace the Backup Battery Units before the final expiration date occurs. The replacement part number is 00Y3447. If the Backup Battery Units expire, the RAID Controller enters a cache write-through

mode until new Backup Battery Units are installed. This causes a significant delay in processing speed.

2.6 SAS adapters

Table 2-12 lists the SAS adapters (available and withdrawn) and the BladeCenter servers that support them.

Table 2-12 SAS adapters that are supported by the blade servers (Y = supported, N = not supported)

Expansion cards	Part number (w = withdrawn)	Feature code ^a	HS12 — 8028	HS22 — 7870	HS22V — 7871	HS23 — 7875	HS23E — 8038	HX5 — 7872/7873	PS700/1/2 — 8406	PS703/4 — 7891
SAS Connectivity Card (CFFv)	43W3974 (w)	1591	Y	N	N	N	N	N	N	N
SAS Expansion Card (CFFv)	39Y9190 (w)	2979	Y	N	N	N	N	N	N	N
SAS Expansion Card (CFFv)	44E5688 ^b (w)	A3J9	Y	N	N	N	N	N	N	N
SAS Connectivity Card (CIOv)	43W4068	1041 / 8246	N	Y	Y	Y	N	Y ^c	Y	Y
ServeRAID MR10ie (CIOv)	46C7167 (w)	5752 / 8257	Y ^d	Y	Y	N	N	N	N	N
ServeRAID H1135 (CIOv)	90Y4750	A1XJ	N	N	N	N	Y	N	N	N

a. Two feature codes: x-config and e-config. One feature code: x-config.

b. Replaces 39Y9190.

c. Requires solid-state drive (SSD) Expansion Card, part number 46M6908.

d. Requires serial-attached SCSI (SAS) Connectivity Card, part number 43W3974.

This section describes the adapters that are still available:

- ▶ SAS Connectivity Card (CIOv), 43W4068
- ▶ ServeRAID H1135 (CIOv), 90Y4750

2.6.1 SAS Connectivity Card (CIOv)

The SAS Connectivity Card (CIOv) for IBM BladeCenter (part number 43W4068) is an expansion card that offers the ideal way to connect the supported BladeCenter servers to a wide variety of SAS storage devices. Using 3 Gbps,

full-duplex, SAS technology, the SAS Connectivity Card can connect to external IBM System Storage® solutions and to multiple Disk Storage Modules in the BladeCenter S. The card routes the pair of SAS channels from the blade's onboard SAS controller to SAS switches installed in the BladeCenter chassis.

The part number information is shown in Table 2-13.

Table 2-13 Part number information

Part number	Feature code	Description
43W4068	1041	SAS Connectivity Card (CIOv) for IBM BladeCenter

The SAS Connectivity Card (CIOv), shown in Figure 2-11, is a SAS bridge card that is used with blade servers that possess a CIOv interface. The SAS Connectivity Card (CIOv) connects unused SAS ports of the onboard SAS controller on the blade server to the blade's midplane connector. The onboard SAS controller is then able to connect to SAS storage through SAS modules in switch bays 3 and 4 in the BladeCenter chassis.

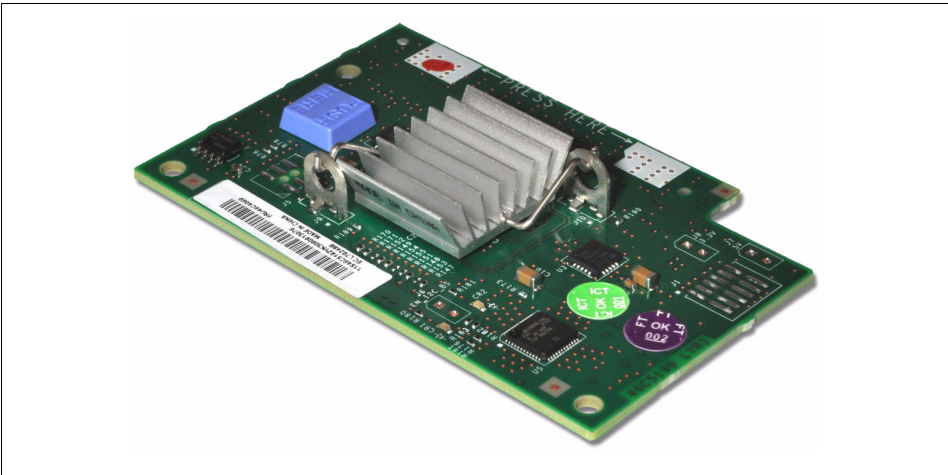


Figure 2-11 The SAS Connectivity Card (CIOv) for IBM BladeCenter

The SAS Connectivity Card (CIOv) has the following features:

- ▶ CIOv form factor
- ▶ Provides external connections for the two SAS ports of a blade server's onboard LSI 1064e disk storage controller
- ▶ Support for two full-duplex SAS ports at 3 Gbps maximum per channel
- ▶ Support for SAS, SSP, and SMP protocols

For more information, see the following publications:

- ▶ *SAS Connectivity Card (CIOv) for IBM BladeCenter*, found at:
<http://www.redbooks.ibm.com/abstracts/tips0701.html>
- ▶ *SAS Connectivity Card (CIOv) Installation and User Guide*, found at:
<http://ibm.com/support/entry/portal/docdisplay?lnodocid=MIGR-5079707>

2.6.2 ServeRAID H1135 (CIOv) Controller

The IBM ServeRAID H1135 Controller (part number 90Y4750) enables you to use RAID technology to manage hard disk drive configurations and integrate SAS technology into your storage infrastructure. You can install the IBM ServeRAID H1135 Controller in an IBM BladeCenter HS23E blade server.

The part number information is shown in Table 2-14.

Table 2-14 Part number information

Part number	Feature code	Description
90Y4750	A1XJ	ServeRAID H1135 Controller for IBM Flex System and BladeCenter

The ServeRAID H1135 Controller has the following specifications:

- ▶ Based on the LSI SAS2004 6 Gbps SAS 4-port controller
- ▶ Up to 6 Gbps throughput per port
- ▶ CIOv form factor
- ▶ PCIe 2.0 x4 host interface
- ▶ Two SAS ports that are routed internally to the two hot-swap drive bays
- ▶ Two SAS ports that are routed externally to the chassis I/O bays 3 and 4
- ▶ Support for SAS/SATA HDD and SSD drives
- ▶ Support for RAID 0, 1, 1E, and 10, and non-RAID
- ▶ Support for up to two RAID volumes
- ▶ Support for up to 10 drives in one RAID volume
- ▶ Support up to 14 volume drives, including up to two hot-spare drives
- ▶ Support for virtual drive sizes greater than 2 TB
- ▶ Fixed stripe size of 64 KB
- ▶ S.M.A.R.T. support

- ▶ Support for MegaRAID Storage Manager management software
- ▶ Support for connectivity to the EXP2512 and EXP2524 storage expansion enclosures
- ▶ Support for connectivity to the BladeCenter S disk storage modules (through SAS Connectivity Modules or SAS RAID Controller Modules), tape drives, and external storage systems
- ▶ Support for operations as a RAID controller for the internal drives and as an HBA for the external storage at the same time

Figure 2-12 shows the ServeRAID H1135 (CIOv) Controller.

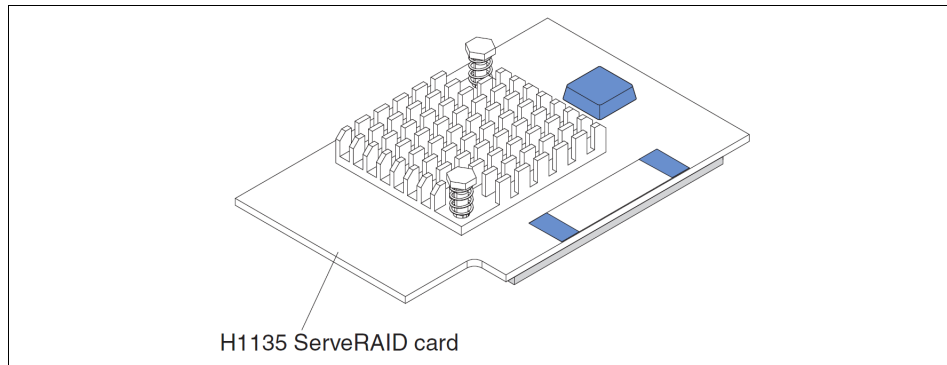


Figure 2-12 The ServeRAID H1135 (CIOv) Controller

For more information, see the following publications:

- ▶ *IBM ServeRAID Adapter Quick Reference*, TIPS0054, at:
<http://www.redbooks.ibm.com/abstracts/tips0054.html?Open#H1135>
- ▶ *ServeRAID H1135 SAS/SATA Controller Installation and User Guide* at:
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5088601>

2.7 External SAS connectivity: Storage

Both the SAS Connectivity Module and SAS RAID Controller Module have four external SAS ports. These ports allow connections to external SAS devices, such as tape drives and external storage. These external ports are routed internally to the blades within the BladeCenter S chassis.

Table 2-15 lists the supported IBM external storage devices.

Table 2-15 External storage support

SAS storage targets	Supported by SAS Connectivity Module	Supported by SAS RAID Controller Module
DCS3700	Yes	No
DS3200	Yes	No
DS3500	Yes	No
DS3950	No	No
EXP395	No	No
EXP2500	Yes	No
EXP3000	Yes	No

For specific support information, see the IBM System Storage Interoperation Center (SSIC) at:

<http://ibm.com/systems/support/storage/ssic/interoperability.wss>

2.8 Media tray

The media tray for the BladeCenter S is a hot swappable module that consists of the system LED panel, CD-RW/DVD drive, two v2.0 USB ports, and two battery backup module bays. The system LED panel provides light path diagnostic LEDs, and power and location indicators. A brief description of each indicator is included in this section.

The two battery-backup-unit (BBU) module bays on the front of the media tray are reserved for future use. A battery backup filler must be installed in both bays to ensure effective cooling of the BladeCenter.

The use of the modular flash drive port is currently not supported.

Figure 2-13 shows the features of the media tray.

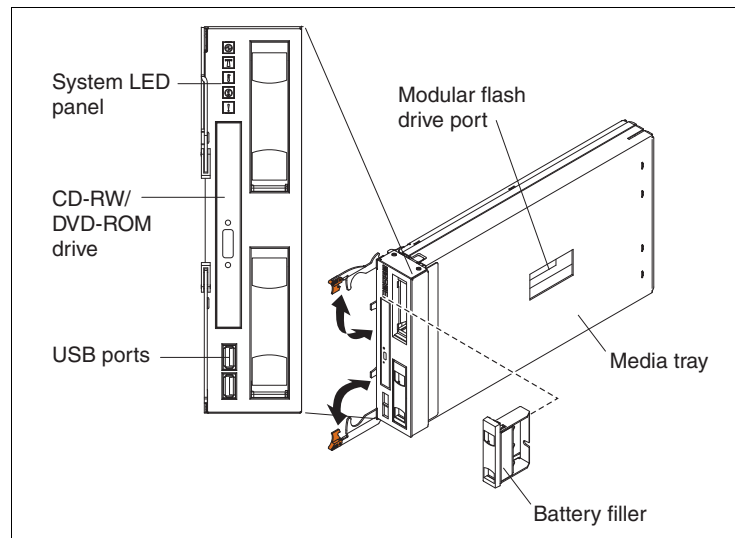


Figure 2-13 Features of the media tray for the BladeCenter S

The CD-RW/DVD-ROM drive is a compact optical drive that is available to any blade server in the chassis. The drive can be used to install operating systems, update drivers, or to archive data for recordable CD media.

Supported optical drives are listed in Table 2-16.

Table 2-16 Part number information

Part number	Feature code	Description
46M0901	4161	IBM UltraSlim Enhanced SATA DVD-ROM
46M0902	4163	IBM UltraSlim Enhanced SATA Multi-Burner

For blade servers to access the drive, it must be assigned to a specific blade bay. You can do this by physically pressing the Media Tray Assignment button on the front of the blade server that you want to use. Or you can use the menu in the AMM's remote control interface.

When assigned, the drive is exclusively available to the blade server to which it is assigned. If a Media Tray Assignment button is pressed on another blade or assigned to another blade server through the AMM, ownership and exclusive access of the drive are immediately transferred to the destination blade server.

Assignment button: The Media Tray Assignment button on the front of blade servers or the media tray owner in the AMM's remote control interface includes both the CD-RW/DVD drive and the two USB ports on the front of the BladeCenter S. When the corresponding button is pressed on another server (or the drive is reassigned in the AMM), all access from the original blade server is immediately ended.

The USB ports that are provided on the front of the media tray enable blade servers within the chassis to access external USB devices. Access to the USB ports is achieved by physically pressing the Media Tray Assignment button on the front of the blade server you want. You can also use the menu in the AMM's remote control interface. When assigned, the ports are exclusively available to the blade server to which they are assigned.

The following types of USB devices are supported:

- ▶ USB memory keys
- ▶ IBM RDX USB 3.0 Disk Backup Solution (see 2.13.3, "IBM RDX USB.3.0 Disk Backup Solution" on page 78)
- ▶ USB diskette drive

Just like the optical drive, if a Media Tray Assignment button is pressed on another blade or the drive assigned to another blade server through the AMM, ownership and exclusive access of the USB ports is immediately transferred to the destination blade server. Any file transfer in progress is immediately stopped.

To remove the media tray, unlatch the release handles on the front of the module and pull it straight out from the chassis. To reinstall the media tray, ensure that the release handles are at a 90 degree angle to the front of the module. Then, gently insert it into the media tray bay, ensuring that the release handles face the left side of the chassis (the System LED panel is at the top of the module). After you insert the media tray, lower the release handles and secure them flush against the module.

Figure 2-14 shows media tray removal.

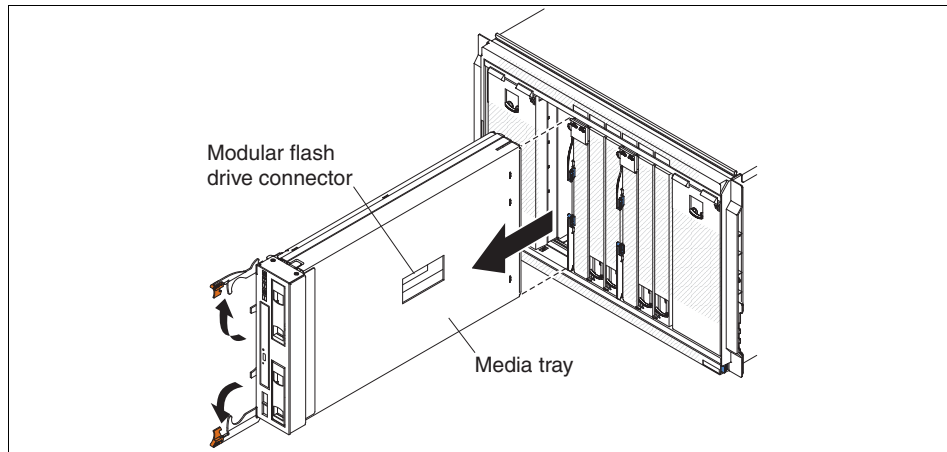


Figure 2-14 Media tray removal

2.9 System LED panels with light path diagnostics

On the BladeCenter S, there are two System LED window panels. These LEDs provide system information and status and part of the Light Path Diagnostics feature.

Their locations can be found:

- At the back of the chassis between the I/O modules (Figure 2-15)

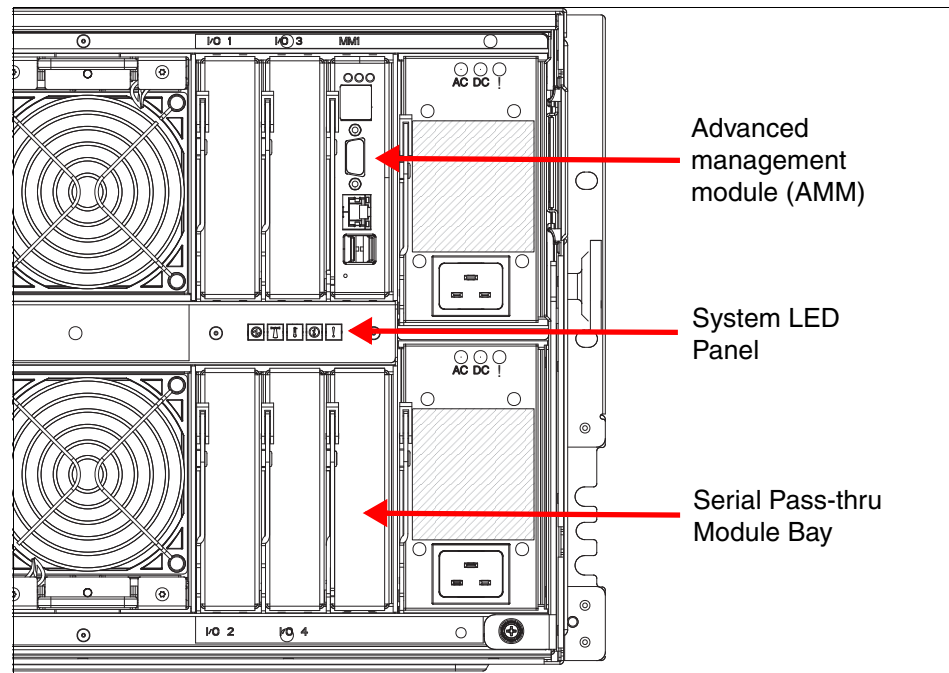


Figure 2-15 The alternate System LED panel is on the back of the BladeCenter S

- On the top corner of the media tray on the front of the chassis (Figure 2-16)

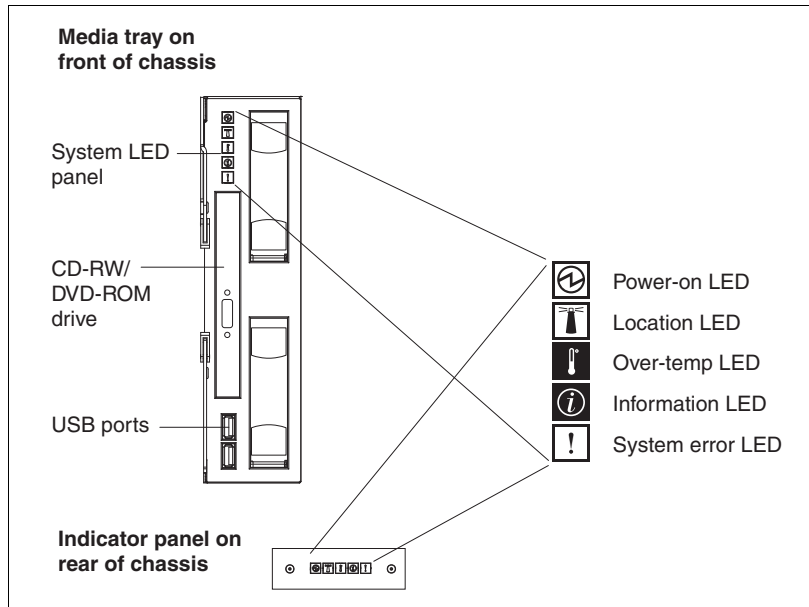







Figure 2-16 The LED window on the front and rear of the chassis

Light path diagnostics uses the system LEDs to display status information about the chassis and components, and whether they are operating correctly. One or more system faults can be indicated by an amber light that is displayed on the chassis system LED window. The individual components can also have amber lit LEDs indicating a fault when the chassis system LED window has solid lit amber LED indicators. These indicators assist you in resolving hardware faults quickly.

Table 2-17 is a summary of the system LED panel indicators.

Table 2-17 LED indicators on the system LED panel

Symbol	LED indicator	Description
	Power-on LED Lit (green)	<ul style="list-style-type: none"> ▶ On: Power is present in the BladeCenter S chassis. ▶ Off: The power subsystem, AC power, or the LED has failed.
	Location LED Lit or flashing (blue)	<ul style="list-style-type: none"> ▶ On or set to flash manually from the AMM to visually identify the BladeCenter S chassis within a rack or when a problem has occurred. Useful when referencing the chassis while conducting remote support.
	Over-temperature LED Lit (Amber)	<ul style="list-style-type: none"> ▶ On indicates that the BladeCenter S chassis temperature has exceeded the threshold level or a blade server reports an over-temperature condition. ▶ The BladeCenter S chassis might have already taken corrective action, such as increasing the fan speed. This LED turns off automatically when there is no longer an over-temperature condition.
	Information LED Lit (Amber)	<ul style="list-style-type: none"> ▶ On indicates that a noncritical event has occurred that requires attention. Events include the wrong I/O module being inserted into a bay, power demands within the BladeCenter S chassis exceeding the capacity of the installed power modules, and the AMM event log becoming full. You can turn off the information LED through the web interface or the IBM Director console.
	System error LED	<ul style="list-style-type: none"> ▶ This amber LED is lit solid to indicate that a critical system error has occurred. These errors include component failure on the chassis or blades.

2.9.1 Module LEDs

The individual modules have LEDs to indicate their system status. Table 2-18 lists a general summary of these LEDs.

Table 2-18 Summary of the available module LED indicators

LED indicator	Description
Advanced management module error LED	This amber LED is lit to indicate that a critical system error has occurred on the AMM.
Power module AC power LED	This green LED is lit when power is available. If it is off, there is no power to the power supply.
Power module DC power LED	This green LED is lit when power is available. If it is off, there is no power to the power supply.

LED indicator	Description
Power module fault LED	This amber LED is lit to indicate that the power module is faulty and requires replacement.
Fan module fault LED	This amber LED is lit to indicate that the fan module is faulty and requires replacement.
Disk storage module fault LED	This amber LED is lit to indicate that the disk storage module is faulty and requires attention or replacement.
Hard disk fault LED	This LED is lit to indicate the hard disk has failed.

Note: Refer to the individual documentation shipped with each I/O module for LED indicator status.

2.10 Advanced management module

The Advanced Management Module (AMM) is a hot-swappable module that can be used to configure and manage any installed BladeCenter components. It provides system management functions and keyboard, video, mouse (KVM) multiplexing for all blade servers in the BladeCenter S unit that support KVM.

The BladeCenter S chassis ships standard with one AMM, and can support only one AMM in the chassis.

The AMM communicates with all components in the BladeCenter unit, detecting their presence or absence, reporting their status, and sending alerts for error conditions when required.

Figure 2-17 shows the AMM.



Figure 2-17 Advanced management module

Configuration is done by using the AMM's web-based user interface. The web interface communicates with the management and configuration application, which is part of the upgradeable firmware that is installed in the management module. You can use the AMM's user interface to perform the following tasks:

- ▶ Defining the login IDs and passwords
- ▶ Configuring security settings, such as data encryption and user account security (for AMMs only)
- ▶ Selecting recipients for alert notification of specific events
- ▶ Monitoring the status of the BladeCenter unit, blade servers, and other BladeCenter components
- ▶ Discovering other BladeCenter units in the network and allowing access to them through their management module web interfaces (for AMMs only)
- ▶ Controlling the BladeCenter unit, blade servers, and other BladeCenter components
- ▶ Accessing the I/O modules to configure them
- ▶ Changing the startup sequence in a blade server
- ▶ Setting the date and time
- ▶ Using a remote console for the blade servers
- ▶ Changing ownership of the keyboard, video, and mouse

- Changing ownership of the removable-media drives and USB ports (the removable-media drives in the BladeCenter unit are viewed as USB devices by the blade server operating system).

2.10.1 AMM connections and indicators

The AMM has several input and output connectors on its external panel. The connections include a serial port, video connection, remote management port (Ethernet), and two USB v2.0 ports for a keyboard and mouse.

Figure 2-18 shows the location of the AMM and its external ports and LEDs.

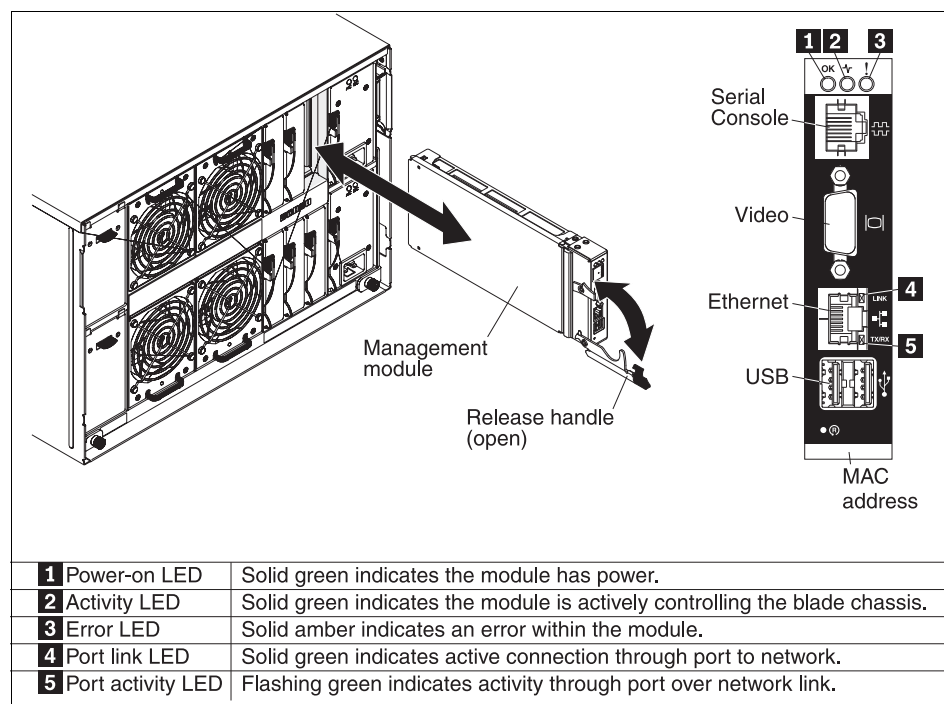


Figure 2-18 AMM connections and indicators

The following features are depicted in Figure 2-18:

- Serial connector
Use this connection to configure and manage the BladeCenter components over a serial line by using the management module CLI. This connector provides local access to the CLI and redirection to the Serial over LAN (SOL) interface of any processor blade server.

For example, you can connect a notebook computer to the serial connector and a terminal emulator program to configure the IP addresses, user accounts, and other management settings through the CLI user interface. For more information, see the *IBM Management Module Command Line Interface Reference Guide* at:

<http://www.ibm.com/systems/bladecenter/support/>

► Video connector

Use this connector to connect a compatible video monitor to the BladeCenter unit. The video connector provides an external monitor display for blade servers only. It does not allow direct access to the web-interface of the AMM. To view the video output of a powered-on blade server, press the Monitor icon on the front of the blade. Only one blade server can be selected at a time using the external video connector.

► Ethernet connector

Use this port to directly connect to the AMM by using a notebook or workstation, or to remotely connect to the AMM through the Ethernet network. This port provides isolated connectivity only to the management module and any IP addressable expansion modules. These modules must be on the same IP subnet as the AMM. When expansion modules are on the same subnet as the AMM, they can be directly accessed by using their management address. The AMM acts as a proxy for any management requests to expansion modules received on its Ethernet connection so long as the addresses are on the same subnet.

Note: The AMM's Ethernet connection does not allow for internal connectivity directly to blade servers. Most blade servers can be indirectly accessed by using the remote control feature of the management module's web interface. For more information about using and configuring the AMM, see Chapter 4, "Configuring storage" on page 165.

► Two USB ports for mouse and keyboard

Use these connectors for local mouse and keyboard connectivity. Unlike the USB ports on the front of the BladeCenter S, the two rear external USB ports on the AMM are controlled and shared through the management module's KVM interface. Only the KVM interface can assign or reassign these ports.

The following management-module LEDs provide status information about the management module and the status of its Ethernet connection:

- ▶ Power-on LED: When this green LED is lit, it indicates that the management module has power.
- ▶ Active LED: When this green LED is lit, it indicates that the management module is actively controlling the BladeCenter unit. Only one management module actively controls the BladeCenter unit.
- ▶ Management module error LED: When this amber LED is lit, it indicates that an error has been detected in the management module. When this LED is lit, the BladeCenter unit system error LED is also lit.
- ▶ Ethernet Link LED: When this green LED is lit, there is an active connection through the port to the network.
- ▶ Ethernet activity LED: When this green LED is flashing, it indicates that there is activity through the port over the network link.
- ▶ Reset button: When you press this button, the blowers operate at full speed while the management module is initializing:
 - Press and release the reset button to restart the management module.
 - Press and hold the reset button for 8 seconds to restore the management module to the factory default settings.

2.11 Serial Pass-thru Module

The Serial Pass-thru Module (part number 43W3583) provides six serial port connectors that can be used to directly attach to each blade server in the BladeCenter S chassis through a four-wire serial RJ-45 connector. Port connector links bypass the AMM and provides a dedicated link directly to each blade. If used, the module must be installed in the Serial Pass-thru Module Bay.

The port connections function at speeds of up to 19.2k baud, and are intended for serial console access only. The port connectors are numbered from 1 to 6, from top to bottom, and correspond to blade servers in blade server bays 1 through 6.

Figure 2-19 shows the Serial Pass-thru Module.

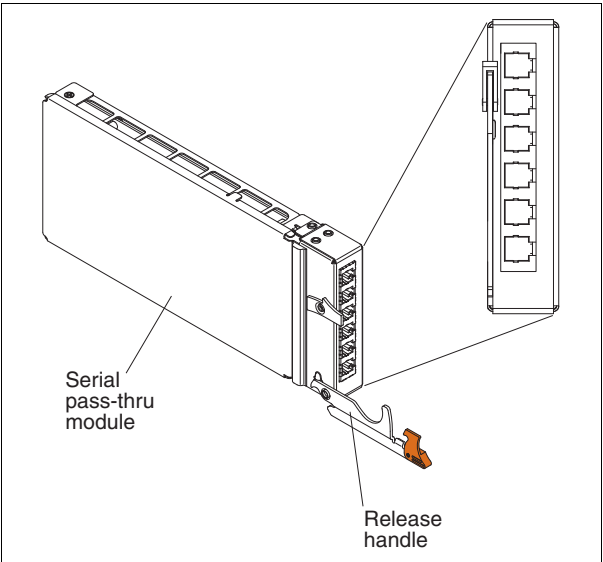
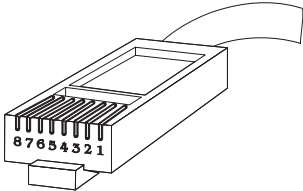


Figure 2-19 Serial Pass-thru Module

The serial cable that is required to access the ports on the Serial Pass-thru Module uses standard CTS/RTS and TXD/RXD signaling to provide console access. The cable's RJ-45 pin configuration is described in Figure 2-20.



Contact (Pin)	Signal name	Signal direction
1	RTS - Request to send	Output from blade server
2	Not used	N/A
3	RXD - Receive Data	Input from blade server
4	GND	N/A
5	Not used	N/A
6	TXD - Transfer Data	Output from blade server
7	Not used	N/A
8	CTS - Clear to send	Input to blade server

Figure 2-20 RJ-45 pin location reference diagram

To install the module, remove the module filler from the Serial Pass-thru Module Bay on the back of the BladeCenter S chassis. To do this, release the handle on the filler module and pull back firmly. To install the Serial Pass-thru Module, lower the release handle and then gently insert module into the bay, ensuring that the handle is on the same side as the AMM. After you complete the installation, lift the handle and secure it flush against the module.

2.12 I/O module bays

The BladeCenter S chassis uses a midplane design to provide connectivity between blade servers and I/O expansion modules. For more information, see 1.3, “BladeCenter concepts and terminology” on page 5. The midplane provides this connectivity through multiple dedicated paths, which are mapped from each blade server’s I/O connector to a designated expansion bay (Figure 2-21).

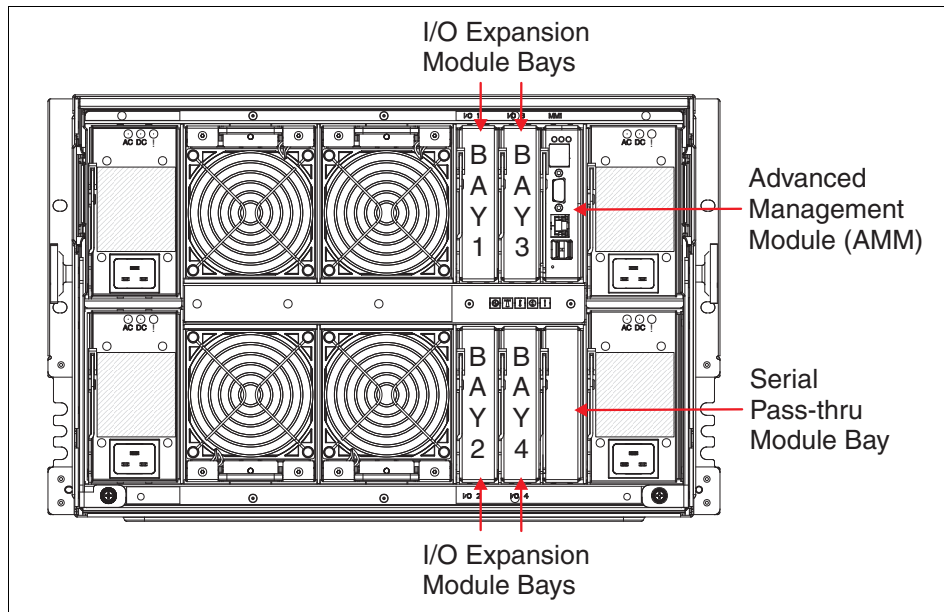


Figure 2-21 Back of BladeCenter S identifying I/O module bay numbers

In other chassis, each blade server provides two onboard Ethernet connections that are separated into unique paths out of the blade server. Each path leads to either an upper or lower midplane connector at the back of the blade server. When a blade server is inserted into the BladeCenter chassis, it connects to the midplane. It is provided power, module bay I/O access, and management control through the AMM.

In the BladeCenter S, the two onboard Ethernet connections of each blade server are mapped directly to I/O module bay 1. Because both default paths from the blade server are Ethernet, I/O module bay 1 can only support an Ethernet switch or pass-through module. See Table 2-19 on page 71 for a list of supported switch modules.

Ethernet in bay 1: You must enable at least one external port on an Ethernet switch module in I/O module bay 1 to communicate with the Ethernet controllers integrated on each blade server.

Access to I/O module bays 3 and 4 is provided through the addition of an expansion card that is installed on a blade server. The following card form factors are needed to connect to these module bays:

- ▶ CIOv
- ▶ CFFv
- ▶ Standard form factor (StFF)
- ▶ Small form factor (SFF)

Withdrawn servers: Form factors CFFv, SfFF, and SFF are not used in the servers currently available. Current servers use CIOv adapters only.

The use of an expansion card enables connectivity to more dedicated paths in a similar manner to the onboard Ethernet. One path exits through the blade server's upper midplane connector, and the other path through the lower midplane connector.

Figure 2-22 provides a simplified illustration of each blade server's connectivity to the I/O module bays of the BladeCenter S.

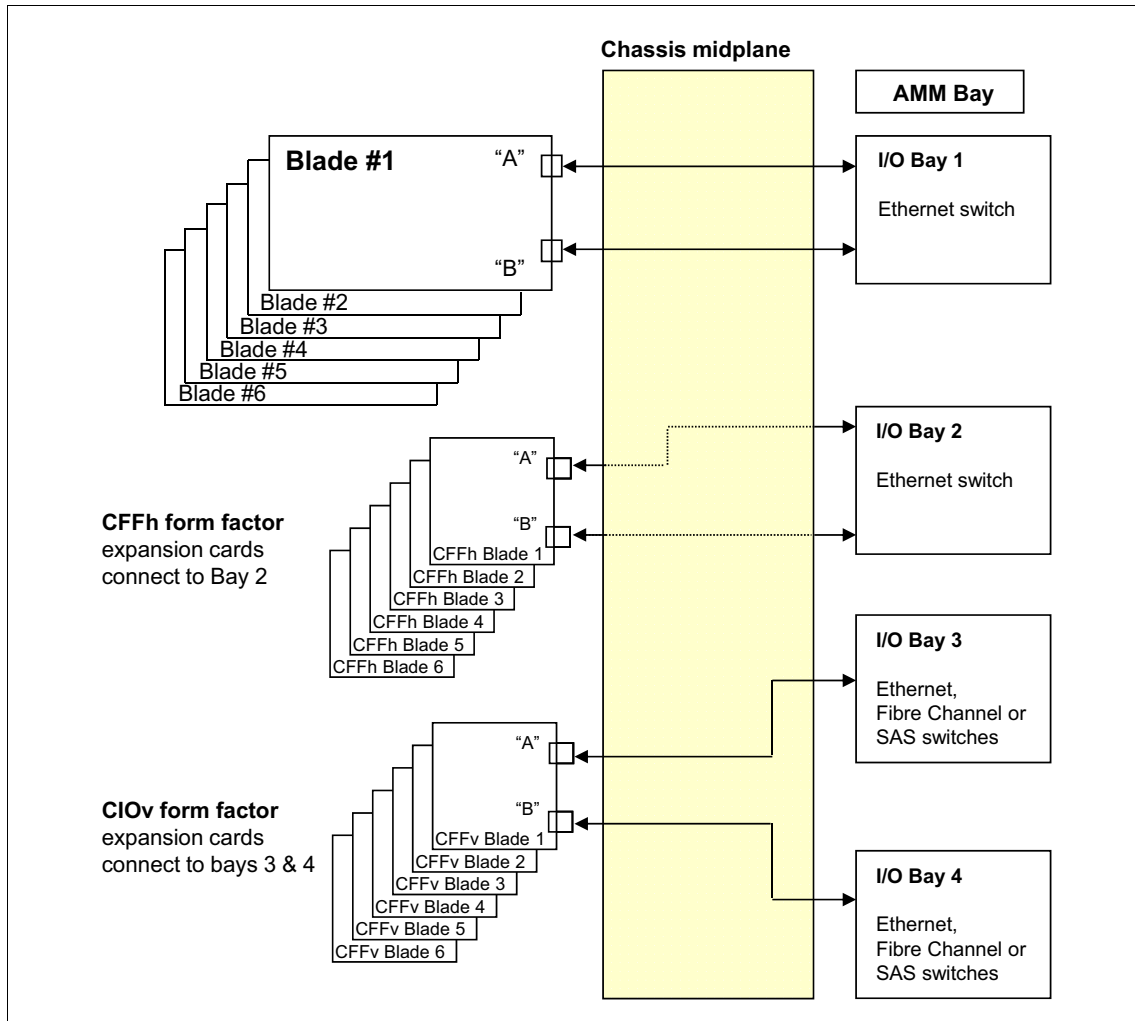


Figure 2-22 IBM BladeCenter S internal IO block diagram

Although paths enabled on the blade server by the expansion card provide independent access to their respective bays, the expansion card and I/O module technology (SAS, Ethernet, Fibre Channel, and so forth) must match.

Additionally, only one type of expansion card I/O technology can be used chassis-wide. For example, when a SAS adapter is installed in a blade server, the I/O expansion modules that are used in Expansion Bays 3 and 4 must be

SAS-based. The same holds true if a SAS module is installed in I/O Expansion Bays 3 and 4. Any adapter that is used in blade servers in the same chassis must be SAS-based.

Important: To access the storage modules in the BladeCenter, a SAS module must be installed in at least I/O bay 3 (preferably bays 3 and 4 for redundancy). The use of the SAS RAID Controller Module requires that you have one in *both* bay 3 and bay 4.

There is one exception from this rule: If you are using an Optical Pass-thru Module (OPM), you can have both Ethernet and FC expansion cards for different blades in the same chassis. OPM is compatible with both Ethernet and FC expansion cards.

2.12.1 I/O expansion module options

Table 2-19 lists all available I/O modules and indicates which ones are supported in BladeCenter S.

Note: To use the storage modules internal to the BladeCenter S chassis, you must have a SAS module in bay 3 (and optionally bay 4) along with SAS expansion cards in each blade server.

Table 2-19 BladeCenter I/O modules

I/O module ^a	Part number	Feature code (x-config/e-config)	Supported in BladeCenter S	Suitable I/O bays
SAS modules				
SAS Connectivity Module	39Y9195	2980/3267	Supported	3, 4
SAS RAID Controller Module	43W3584	3734/none	Supported	3, 4
InfiniBand Modules				
Voltaire 40 Gb InfiniBand Switch Module	46M6005	0057/3204	Not supported	
Pass-through modules				
Intelligent Copper Pass-thru Module	44W4483	5452/5452	Supported	1, 2, 3, 4 ^b
10 Gb Ethernet Pass-thru Module	46M6181	1641/5412	Not supported	

I/O module ^a	Part number	Feature code (x-config/e-config)	Supported in BladeCenter S	Suitable I/O bays
Standard Ethernet switch modules				
Cisco Catalyst Switch Module 3110G	41Y8523	2989/3173	Not supported	
Cisco Catalyst Switch Module 3110G	00Y3254	A3FD/3173	Not supported	
Cisco Catalyst Switch Module 3110X	41Y8522	2988/3171	Not supported	
Cisco Catalyst Switch Module 3110X	00Y3250	A3FC/3171	Not supported	
Cisco Catalyst Switch Module 3012 ^c	43W4395	5450/3174	Supported	1, 2, 3, 4 ^b
Cisco Catalyst Switch Module 3012	46C9272	A3FE/3174	Supported	1, 2, 3, 4 ^b
IBM Server Connectivity Module	39Y9324	1484/3220	Supported	1, 2, 3, 4 ^b
IBM L2/3 Copper GbE Switch Module	32R1860	1495/3212	Supported	1, 2, 3, 4 ^b
IBM L2/3 Fiber GbE Switch Module	32R1861	1496/3213	Supported	1, 2, 3, 4 ^b
IBM L2-7 Gb Ethernet Switch Module	32R1859	1494/3211	Supported	1, 2, 3, 4 ^b
IBM 1/10Gb Uplink ESM	44W4404	1590/1590	Supported	1, 2, 3, 4 ^b
High-speed Ethernet switch modules				
IBM Virtual Fabric 10 Gb Switch Module	46C7191	1639/3248	Not supported	
Brocade Converged 10 GbE Switch Module	69Y1909	7656/none	Not supported	
Cisco Nexus 4001I Switch Module	46M6071	0072/2241	Not supported	
Cisco Nexus 4001I Switch Module	46C9270	A3FF/2241	Not supported	
Fibre Channel I/O modules				
Brocade Enterprise 20-port 8 Gb SAN SM	42C1828	5764/none	Not supported	
Brocade 20-port 8 Gb SAN Switch Module	44X1920	5481/5869	Not supported	
Brocade 10-port 8 Gb SAN Switch Module	44X1921	5483/5045	Not supported	
Cisco 4 Gb 20 port FC Switch Module	39Y9280	2983/3242	Not supported	
Cisco 4 Gb 20 port FC Switch Module	44E5696	A3FH/3242	Not supported	
Cisco 4 Gb 10 port FC Switch Module	39Y9284	2984/3241	Supported	3, 4 ^b
Cisco 4 Gb 10 port FC Switch Module	44E5692	A3FG/3241	Supported	3, 4 ^b
QLogic 20-Port 8 Gb SAN Switch Module	44X1905	5478/3284	Supported	3, 4 ^b

I/O module ^a	Part number	Feature code (x-config/ e-config)	Supported in BladeCenter S	Suitable I/O bays
QLogic 20-Port 4/8Gb SAN Switch Module ^d	88Y6406	A24C/none	Supported	3, 4 ^b
QLogic 8 Gb Intelligent Pass-thru Module	44X1907	5482/5449	Supported	3, 4 ^b
QLogic 4/8Gb Intelligent Pass-thru Module	88Y6410	A24D/none	Supported	3, 4 ^b
QLogic Virtual Fabric Extension Module	46M6172	4799/none	Not supported	

- a. All I/O modules that are listed are supported only with the AMM.
- b. Installing this switch module in bay 3 or bay 4 requires that a suitable CIOv expansion card is installed in the blade servers. Doing so prevents the use of the BladeCenter S internal storage modules. To enable I/O module bay 2 in the BladeCenter S, a suitable CFFh expansion card must be installed in the blade servers.
- c. This I/O module is withdrawn. It is not available for ordering.
- d. Internal ports on QLogic 4/8 Gb SAN Switch and Pass-thru modules support up to 4 Gb speeds when these I/O modules are installed in I/O bays 3 and 4.

2.12.2 Using I/O bay 2

As shown in Figure 2-22 on page 70, I/O bay 2 of the BladeCenter S chassis is routed to the CFFh connector in the installed blade servers. Only Ethernet I/O modules are supported in bay 2. The only adapter that is supported in the corresponding CFFh connector is the IBM 2/4 Port Ethernet Expansion Card (CFFh). Ordering details are shown in Table 2-20.

Table 2-20 Ordering information

Part number	Feature code (x-config / e-config)	Description
44W4479	5476 / 8291	IBM 2/4 Port Ethernet Expansion Card (CFFh)

The IBM 2/4 Port Ethernet Expansion Card, when installed in a BladeCenter S chassis, provides two more Gigabit Ethernet ports to each blade server for a total of four per server. Two are provided by the onboard controller routed to the Ethernet switch in I/O bay 1.

The following are some of the high-level features included in this offering:

- ▶ Based on the Broadcom 5709 chip
- ▶ PCI Express x4 Host host interface for high-speed connection
- ▶ First TCP offload engine (TOE) on an Ethernet expansion card
- ▶ Full fast path TCP offload

- ▶ TCP, IP checksum offload
- ▶ TCP, segmentation offload
- ▶ PXE 2.0 remote boot support

Figure 2-23 shows the 2/4 port Ethernet Expansion Card.

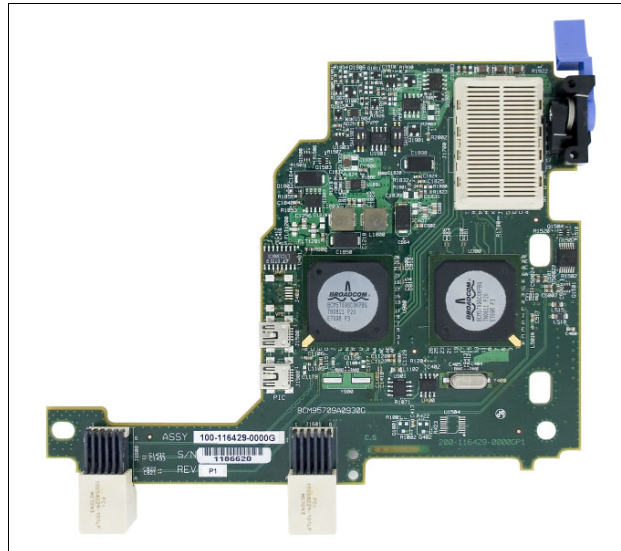


Figure 2-23 2/4 port Ethernet Expansion Card

With this card, you can take full advantage of the capabilities of the BladeCenter S chassis. The chassis provides four Ethernet ports and SAS connectivity to the internal disk storage modules from every blade with the following combination:

In each blade server:

- ▶ One SAS expansion card
- ▶ One 2/4 port Ethernet Expansion Card

In the BladeCenter S chassis:

- ▶ Ethernet switch modules in bay 1 and bay 2
- ▶ SAS switch modules in bay 3 and bay 4

2.12.3 Supported adapters

For a complete list of supported adapters that correspond to the switches you install in the BladeCenter S chassis, see the *IBM BladeCenter Interoperability Guide*, REDP-BCIG, available at

<http://www.redbooks.ibm.com/big>

2.13 SAS tape storage for IBM BladeCenter

Having a backup solution is an important component to any business. Information and systems must be able to be backed up, retained and when necessary restored. With SAS technology, IBM BladeCenter offers an affordable and convenient way to perform a backup by attaching external tape drives and autoloaders directly to the BladeCenter chassis.

BladeCenter S backup solution includes the following components:

- ▶ IBM BladeCenter S Chassis
- ▶ Blade servers
- ▶ SAS adapters
- ▶ SAS Connectivity Module
- ▶ External Tape backup unit
- ▶ SAS external cables
- ▶ Backup software

2.13.1 Tape drive guidelines

When you design a backup solution with SAS tape devices, take into account these important considerations:

- ▶ Solution components must be compatible with each other. For more information, see 2.13.3, “IBM RDX USB.3.0 Disk Backup Solution” on page 78.
- ▶ The backup software that is used must support the proposed operating environment, including connectivity topologies, tape devices, and operating systems.
- ▶ Simultaneous access by several servers cannot be handled by the tape device, so this situation must be avoided.
- ▶ Do not mix both tape devices and disk storage devices on the same HBA port because this can lead to significant performance degradation of the backup operation.

- ▶ If an SAS connectivity module is used for both disk and tape operations for different servers, implement zoning to isolate the different types of traffic.
- ▶ LAN-free backup is possible. However, it must be supported by the backup software that you use. Also, it causes loss of path redundancy because one SAS HBA port is dedicated to disk storage access, and the other is dedicated to tape unit access. Check the documentation that comes with the backup application for support of LAN-free backup for SAS-attached tapes and servers.
- ▶ Plan to use dedicated backup servers and LAN-based backup operations. This configuration provides high availability for business-critical data on production servers with dual-path connections to disk storage. It also provides a convenient way to back up data at the same time.

2.13.2 Supported tape drives

Table 2-21 lists the supported tape drives. For the latest information, see the *IBM BladeCenter Interoperability Guide*, REDP-BCIG, available at:

<http://www.redbooks.ibm.com/big>

Tip: Use this table only as a starting point. Some combinations are not supported. Verify configuration support by using the IBM System Storage Interoperation Center (SSIC) at:

<http://ibm.com/systems/support/storage/ssic/interoperability.wss>

Table 2-21 Supported SAS tape drive configurations

IBM Model	Controller Type	Options
TS2230 - 3580-H3L	SAS RAID	Ultrium 3 HH Drives
TS2240 - 3580-H4S	SAS RAID	Ultrium 4 HH Drives
TS2240	SAS RAID	Ultrium 4 Drives
TS2250	SAS RAID	Ultrium 5 Drives
TS2250	SAS RAID	Ultrium 5 HH Drives
TS2260	SAS RAID	Ultrium 6 Drives
TS2340	SAS RAID	Ultrium 4 Drives
TS2350	SAS RAID	Ultrium 5 Drives

IBM Model	Controller Type	Options
TS2900	SAS RAID	Ultrium 3 HH Drives
	SAS RAID	Ultrium 4 HH Drives
	SAS RAID	Ultrium 4 HH V2 Drives
	SAS RAID	Ultrium 5 HH Drives
	SAS RAID	Ultrium 6 HH Drives
TS3100 - 3573	SAS RAID	Ultrium 3 HH Drives
	SAS RAID	Ultrium 3 HH V2 Drives
	SAS RAID	Ultrium 4 Drives
	SAS RAID	Ultrium 4 HH Drives
	SAS RAID	Ultrium 4 HH V2 Drives
	SAS RAID	Ultrium 5 Drives
	SAS RAID	Ultrium 5 HH Drives
	SAS RAID	Ultrium 5 HH V2 Drives
	SAS RAID	Ultrium 6 HH Drives
TS3200 - 3573	SAS RAID	Ultrium 3 HH Drives
	SAS RAID	Ultrium 3 HH V2 Drives
	SAS RAID	Ultrium 4 Drives
	SAS RAID	Ultrium 4 HH Drives
	SAS RAID	Ultrium 4 HH V2 Drives
	SAS RAID	Ultrium 5 Drives
	SAS RAID	Ultrium 5 HH Drives
	SAS RAID	Ultrium 5 HH V2 Drives
	SAS RAID	Ultrium 6 HH Drives
TS3310 - 3576	SAS RAID	Ultrium 4 Drives
	SAS RAID	Ultrium 5 Drives

IBM Model	Controller Type	Options
TS3500 - 3584	SAS RAID	Ultrium 3 Drives
	SAS RAID	Ultrium 4 Drives
	SAS RAID	Ultrium 5 Drives

2.13.3 IBM RDX USB.3.0 Disk Backup Solution

The IBM RDX solution provides all the benefits of disk, with fast, random access to data, in addition to the historic portability and durability benefits of tape. With only the native OS, RDX provides random access to data and the convenience of drag-and-drop functionality through persistent drive letter access. It can also be addressed like traditional removable tape media when used with any of the supported backup applications

The RDX cartridges are engineered to be durable so you can safely transport them off-site and provide the shelf life required for archival requirements. The carrier also supports next generation capacities of cartridges, and the cartridges can be password protected and software encrypted for extra security.

IBM RDX features high-capacity shock-resistant cartridges with up to 1 TB capacity, making your storage options flexible. Each cartridge is ruggedized to withstand a drop from up to 0.9 meters (36 in) without damage. The RDX USB 3.0 docking stations are offered in external stand-alone and internal 5.25-inch half-height units.

IBM RDX USB 3.0 Dock with Cartridge (external) includes the following items:

- ▶ One external carrier/dock (drive)
- ▶ One cartridge (either 320 GB, 500 GB, or 1 TB capacity)
- ▶ Documentation and software CD
- ▶ AC adapter (12 output; 100-240 V, 50-60 Hz input)
- ▶ 3 m external USB 3 cable

2.14 BladeCenter S Office Enablement Kit

The BladeCenter S Office Enablement Kit (part number 201886X) is an enclosure for the BladeCenter S chassis that is designed for use in offices without a dedicated server room, or where the dust level is high. The enclosure

with the BladeCenter S chassis and Flat Panel Monitor kit installed is shown in Figure 2-24.



Figure 2-24 IBM BladeCenter S Office Enablement Kit

Based on the NetBAY11, the Office Enablement Kit is an 11U enclosure with security doors, and special acoustics and air filtration to suit office environments. With the BladeCenter S chassis installed, this leaves an extra 4U of space to hold other rack devices.

The Office Enablement Kit offers the following benefits:

- ▶ **Acoustical Module:** The Office Enablement Kit comes with an acoustical module that helps make BladeCenter S quiet for the office environment, while still allowing easy access to the BladeCenter S components.
- ▶ **Locking door:** Security is an important consideration in any office environment. The Office Enablement Kit comes with a front locking door that helps ensure that your data remains safe and secure in any environment.
- ▶ **4U of extra space for other devices:** Different businesses use different tools to enable their office IT. The Office Enablement Kit includes 4U of extra space for other types of IT that an office might need. This space can take any IT that fits into a 4U or smaller standard rack space.
- ▶ **Easily mobile:** The Office Enablement Kit comes with lockable wheels to make your BladeCenter S easily transportable.

The Office Enablement Kit also supports an optional air contaminant filter for BladeCenter S chassis that are deployed in dusty environments. The IBM BladeCenter Airborne Contaminant Filter (part number 43X0340, feature code 4024) is an optional hardware kit that enables the Office Enablement Kit to use air filters. One air filter is included. Replacement air filters can be ordered in quantities of four (IBM BladeCenter Airborne Contaminant Replacement Filter (4-Pack), part number 43X0437, feature code 4025).

The enclosure has the following approximate dimensions:

- ▶ Height: 24 inches
- ▶ Width: 24 inches
- ▶ Depth: 42 inches

2.15 Extra rack options

IBM provides a number of different racks to accommodate more devices for the BladeCenter S chassis when the Office Enablement Kit is not suitable. These racks are shown in Figure 2-25.

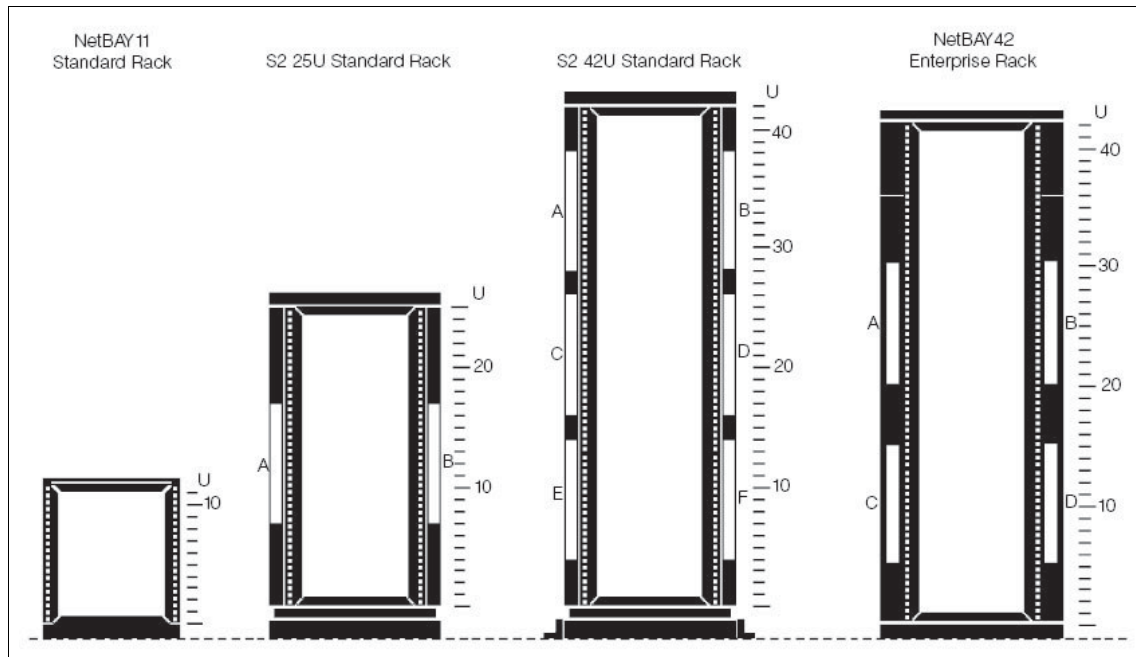


Figure 2-25 Overview of rack options from IBM

Table 2-22 summarizes the specifications of IBM rack options available for the BladeCenter S.

Table 2-22 Rack specification summary

Specifications	NetBay11 Standard Rack	S2 25U Standard Rack	S2 42U Standard Rack	S2 42U Standard Expansion Rack	NetBay42 Enterprise Rack	NetBay42 Enterprise Expansion Rack
EIA Capacity ^a	11U	25U	42U	42U	42U	42U
Sidewall compartments	0	2	6	6	4	4
Front Stabilizers	Standard	Standard	Standard	Standard	Standard	Standard
Side Stabilizers	Not needed	Not needed	Standard ^b	Not needed	Not needed	Not needed
Casters	Standard	Standard	Standard	Standard	Standard	Standard
Leveling Feet	Not avail.	Standard	Standard	Standard	Standard	Standard
Side Covers	Standard	Standard	Standard	Not needed	Standard	Not needed
Rack Attachment Kit ^c	Not avail.	Not avail.	Not needed	Standard	Not needed	Standard
Glass Front Door	Not avail.	Not avail.	Not avail.	Not avail.	Not avail.	Not avail.
Perforated front door	Standard	Standard	Standard	Standard	Standard	Standard
Perforated rear door	Not avail.	Standard	Standard	Standard	Standard	Standard
Height (inches/mm) ^d	24.1 / 611	53 / 1344	78.7 / 1999	78.7 / 1999	79.5 / 2020	79.5 / 2020
Width (inches/mm)	20.4 / 518	23.8 / 605	23.8 / 605	23.6 / 600	25.5 / 648	25.5 / 648
Depth (inches/mm)	34.4 / 873	39.4 / 1000	39.4 / 1000	39.4 / 1000	43.5 / 1105	43.5 / 1105
Empty Weight (lb/kg)	79 / 36	220 / 100	276 / 125	207/94	575/261	516/234
Maximum Load (lb/kg)	401/182	1250/567	2000/907	2000/907	2055/932	2055/932
Total Weight (lb/kg)	481/218	1470/667	2276/1032	2276/1032	2630/1193	2630/1193
Shippable Loaded ^e	Yes	Yes	No	No	Yes	Yes

a. EIA is the Electronics Industries Association; 1U = 1.75 inches (44.5 mm).

b. Side stabilizer brackets are included to bolt the cabinet to the floor. They are needed when a single, stand-alone cabinet is lightly loaded. For more information, see the installation instructions.

c. Required to attach racks together to make a suite.

d. Minimum clearance to the ceiling is 305 mm/12 in.

e. *Shippable loaded* means that the cabinet can be transported with equipment installed. Required packaging is provided. The integrator/assembler is responsible for assuring the stability of the shipped configuration.

Rack Integration Services are available from IBM.

2.16 Power supply modules and redundancy

The BladeCenter S supports up to four auto-sensing power modules that can support either 110 V or 220 V AC power. Two power modules are standard, and a maximum of four power modules are supported.

The power modules are hot swappable components and can easily be replaced during normal BladeCenter operation, assuming a redundant power policy is selected in the AMM. If a power supply fails, the cooling fans inside the power supply continue to operate normally because the power supply fans are powered from the “common” voltage from the midplane. This is important because the power supply fans cool the airflow to the storage modules.

There are two power supply options available for the IBM BladeCenter S chassis. As shown in Figure 2-26, one power supply module has a C20 power connector (part number 43W3582, feature code 4548). The other power supply module has a C14 power connector (part number 46C7438, feature code 4505). BladeCenter S models with these power supplies standard are listed in Table 2-1 on page 33.

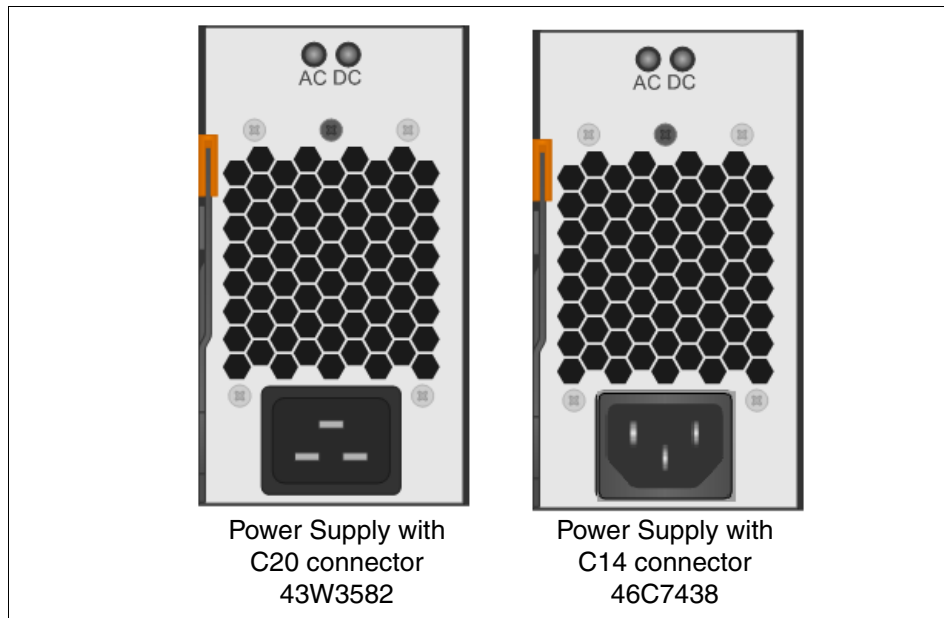


Figure 2-26 IBM BladeCenter S power supplies

Ensure that the power cord that you order matches the power supply that is configured with your BladeCenter S. The power cord has either a C20 or C14 connector on the server end and a country-specific pin configuration on the supply end.

The IBM System x PDU Guides are a good source of information for power cables with the corresponding IBM part numbers. PDFs of these guides can be downloaded from:

<http://ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS4401>

Both BladeCenter S power modules are auto-sensing, and can support either 110 V or 220 V AC power. However, do not mix voltage power sources within the same BladeCenter S chassis. If you have a mix of 110 V and 220 V input power sources, the chassis detects this mix and does not allow some power supplies to function. In this situation, the DC LEDs of the power supplies that are blocked do not illuminate. The AMM also posts messages to the error log.

2.16.1 Power supply modules

Within the BladeCenter S chassis, all power supplies are combined into a single power domain that distributes power to each of the blade servers and modules through the system midplane.

The two standard power modules are installed in bay 1 and bay 2 of the chassis. These are the top and bottom module bays on the right side when looking from the back of the chassis, as shown in Figure 2-27.

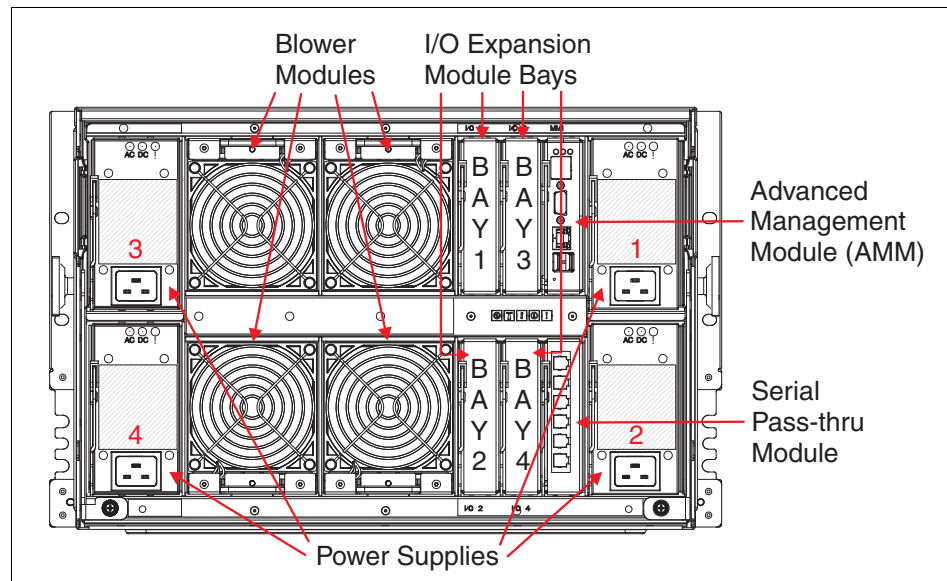


Figure 2-27 Rear view of BladeCenter S showing major components, including four power supply modules

The second pair of power modules is required in any of these situations:

- ▶ The power requirements of the installed components (servers, I/O modules, disks, and so forth) exceed the capacity of the standard two power modules.
- ▶ You install the second storage module because power modules 3 and 4 provide the fans needed to cool this second storage module.
- ▶ The power profile that you select requires more power supplies for redundancy. For more information, see 2.17, “Power management policies” on page 86.

Use the BladeCenter Power Configurator to determine whether your configuration requires the second pair of power supplies:

<http://www.ibm.com/systems/bladecenter/powerconfig>

Also, review the Power section in Chapter 2 of the *BladeCenter S Planning Guide* for details about power consumption and power management policies. This book is available at:

<http://www.ibm.com/systems/bladecenter/support/>

A power module can be removed while the BladeCenter S is powered on if a redundant power policy is selected before removal.

To remove a power supply, unlatch the release handle and slide the power module out of the power module bay. To maintain system cooling, do not operate the BladeCenter S system without a power module or power module filler in each power module bay. Install a power module or filler within one minute of the removal of a power module.

Attention: Do not operate the BladeCenter S without a power module or power module filler in each power module bay. The cooling efficiency of the BladeCenter vectored airflow design requires all bays being occupied by a device or filler.

Figure 2-28 shows how to remove the power supplies.

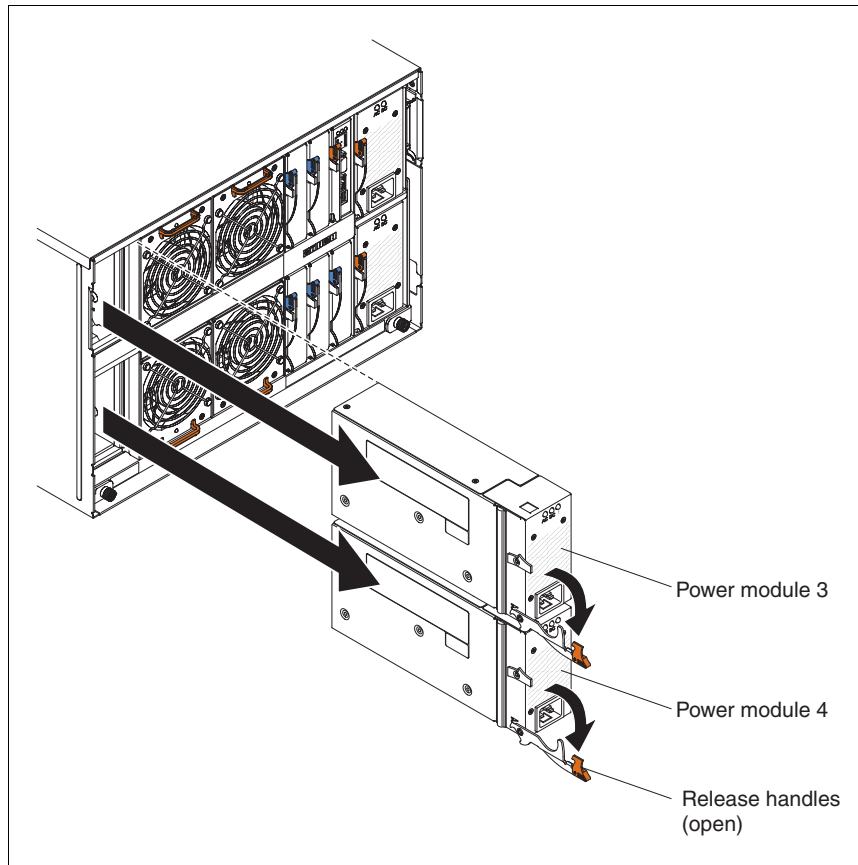


Figure 2-28 Removing optional power supply modules 3 and 4 from the back of BladeCenter S

2.16.2 Power redundancy and throttling

A key objective of the power subsystem of the chassis is to try to keep the chassis operating in the event of a power failure. This goal can be achieved through some or all of these actions:

- ▶ Install sufficient power modules so that one is redundant in the event of a power module failure.
- ▶ Connect the chassis to two separate power sources (for example, a main supply and a UPS, or two main supplies).
- ▶ Select a power management policy that includes redundancy features.

- ▶ Select a power management policy that also allows throttling when a power failure occurs. *Throttling* means that blade servers (the ones that support it) reduce their power consumption by decreasing the processor frequency. The objective of throttling is to keep the power consumption of the chassis within the remaining available power. For more information, see 2.17, “Power management policies” on page 86.

To provide true power redundancy to the BladeCenter S chassis, select a redundant power management policy. Also, distribute power sources for the power modules across at least two separate main circuits. Connect power modules 1 and 3 to a different AC power source than power modules 2 and 4 (if four power modules are installed).

2.17 Power management policies

The AMM manages devices in the chassis to stay within the available power. It does this by enforcing a *power limit*. This limit is based on the number of power modules that are installed and whether they are sourced by a 110 V supply or a 220 V supply. Different power management policies cause the AMM to adjust this power limit up or down.

A power management policy is a preconfigured set of instructions about how to manage power in the event of a failure in either input power or a power module. You specify the policy that you want to use by using the web interface of the AMM.

There are five power policies available in the AMM, broken down into three main categories:

- ▶ Redundant AC source
- ▶ Redundant power modules
- ▶ No redundancy

Under each power management policy, a blade server is prevented from powering on if it might cause the total power consumption in the chassis to exceed the power limit. Some power policies allow server processor throttling, which can increase the power limit for the chassis. Throttling might allow blade servers to power on that, under another power policy, would be prevented from powering on. When a power module or power source fails with throttling enabled, blade servers can reduce their power consumption by reducing their performance. However, blade server's processors return to their normal power states when power redundancy is restored.

Note: Some policies assume that you have 220 V power or that you have four power modules installed. Take this into consideration when you are selecting a policy.

2.17.1 Redundant AC power source policies

The first category is based on having two separate AC power sources to the chassis (for example, different circuits).

The redundancy in this category is sometimes called $N+N$ redundancy where N is the number of supplies that are sufficient to drive the chassis. $N=2$ when four power supplies are installed.

This category has the following options:

- ▶ Redundant AC Power Source
 - Input voltage: 110 V or 220 V (220 V preferred)
 - Number of power modules installed: two or four (four preferred)
 - Number of redundant power modules: two if four installed, one if two installed
 - Throttling allowed if required: No

Power limit is set to equal the capacity of N power modules. This is the most conservative approach and is preferable when all four power modules are installed. When the chassis is correctly wired with dual AC power sources, one AC power source can fail without affecting your blade server operation.

A blade might not be allowed to power on if doing so exceeds the policy power limit.

- ▶ Redundant AC Power Source with Blade Throttling Allowed
 - Input voltage: 110 V or 220 V (220 V preferred)
 - Number of power modules installed: two or four (four preferred)
 - Number of redundant power modules: two if four installed, one if two installed
 - Throttling allowed if required: Yes

This policy is similar to the Redundant AC Power Source policy except that throttling is used, if required, to keep the blades in the chassis operational.

With this policy, the power limit is the capacity of two power modules. If you use dual AC power sources, one AC power source can fail without affecting the operation of the blade servers.

If an AC power source is lost or if half of the power modules fail, processors on blade servers that can throttle do so to reduce the power that is consumed to less than or equal to the power limit. *Throttling* refers to achieving lower power consumption for a blade by temporarily reducing the processor throughput. The AMM uses power management technologies that are built into certain processors to throttle the blades.

2.17.2 Redundant power module policies

The second category is based on having a single AC power source to the chassis, but one power module more than is needed for the chassis.

The redundancy in this category is called $N+1$ redundancy where N is the number of supplies that are sufficient to drive the chassis. $N=1$ when two supplies are installed and $N=3$ when four power supplies are installed.

This category has these options:

- ▶ Redundant Power Modules
 - Input voltage: 110 V or 220 V
 - Number of power modules installed: Two or four
 - Number of redundant power modules: One
 - Throttling allowed if required: No

With this policy, the power limit equals the capacity of one less than the number of power modules installed (more than one power module must be present). One power module can fail without affecting blade server operation.

Blade servers power on only if they can operate without throttling if there is a power module failure. The number of blade servers that are allowed to power on is determined by the power available from one less than the total number of power modules. If a single power module fails, all the blade servers that are powered on continue to operate at normal performance levels. If two or more power modules fail, the BladeCenter S chassis might power off, depending on the load.

Ensure that each power module is on its own dedicated circuit so that a circuit failure (for example, a breaker trip) does not shut down more than one power module.

- ▶ Redundant Power Modules with Blade Throttling Allowed
 - Input voltage: 110 V or 220 V
 - Number of power modules installed: Two or four
 - Number of redundant power modules: One
 - Throttling allowed if required: Yes

This policy is similar to the Redundant Power Modules policy except that throttling is allowed if required to keep the blades in the chassis operational.

This policy allows you to draw more total power from the chassis than the Redundant Power Modules policy. This means that you might be able to power on blade servers that you might not otherwise be able to power on. The disadvantage is that in the case of power module failure, the management module might have to throttle down some blades to keep the chassis operational.

2.17.3 No redundancy

The third category is based on not having any redundant power management done by the AMM. There is only one policy in this category:

- ▶ Non-redundant
 - Input voltage: 110 V or 220 V
 - Number of power modules installed: Two or four
 - Number of redundant power modules: None
 - Throttling allowed if required: Yes

Blade servers are allowed to power on if the power consumed is less than or equal to the total power of all installed power modules. Throttling is used, if necessary, to restrict power consumption by the blade servers. However, if power demands exceed the capacity of the available power modules, the chassis will power down.

2.17.4 Power redundancy examples

The following examples are of the most common power configuration scenarios that are used with the BladeCenter S. A power source can be either a unique circuit breaker or a separate power feed from another part of the building. If using 110 V AC power, you must use two power feeds, each with two dedicated circuits.

Tip: The best power configuration when you are using four power modules is to have Power Modules 1 and 3 each connected to a separate dedicated circuit from one power feed in the building. Similarly, have Power Modules 2 and 4 each connected to a separate dedicated circuit from a different power feed.

Example one

The first example configuration involves both power modules being connected to a single power source. This configuration can provide power redundancy within the chassis, but not fault tolerance of the AC power that is supplied to the chassis. In other words, a power module can fail and, depending on the power requirements of the installed components, the chassis can remain functional.

However, if there is an AC power failure at the source or the power policy in the AMM is set to non-redundant and a power module fails, the chassis shuts down. This process immediately powers off all components and blade servers.

You can select either of these power management policies:

- ▶ Redundant Power Modules (with or without throttling)
- ▶ Non-Redundant

Each AC power cord must still be connected to independent power circuits (that is, separate circuit breakers) to eliminate this single point of failure.

Depending upon the power management policy that you select in the AMM and the input voltage that is used, the power modules can supply AC power as shown in Table 2-23.

Table 2-23 Available power for two power modules

Policy	110 V supply	220 V supply
Redundant Power Modules	950 W	1450 W
Non-Redundant	1900 W	2900 W

Important: Generally, use at least two power sources. Having a single power source configuration means a single point of failure, which occurs outside of the chassis’ control. To avoid this, use a second power source, such as a UPS.

Figure 2-29 shows the example configuration.

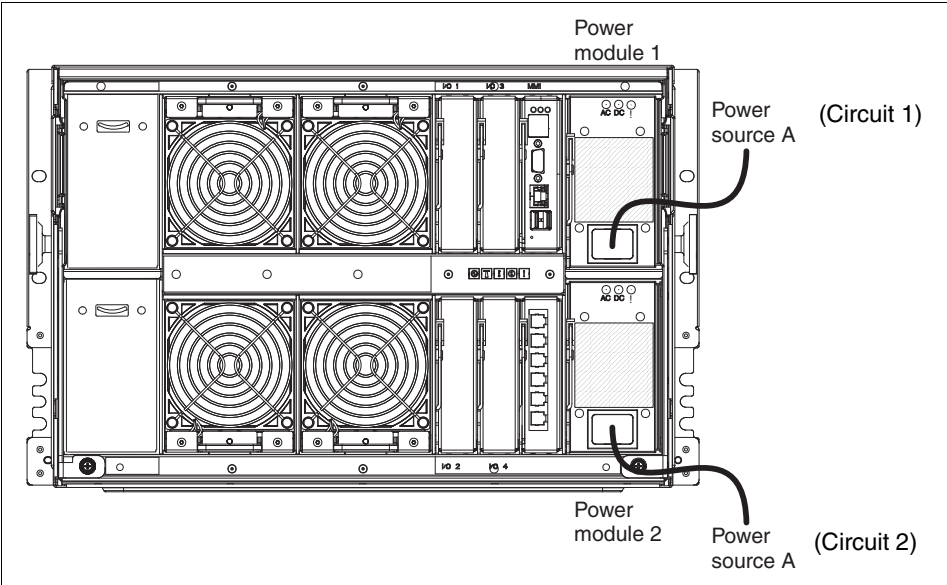


Figure 2-29 Two Power Supply Module configuration connected to same power source

Example two

The second example involves the power modules each being connected to a different power source. This configuration can provide power redundancy within the chassis and fault tolerance of the AC power that is supplied to the chassis. In other words, a power module or an AC power source can fail and, depending upon the power requirements of the installed components, the chassis can remain functional.

You can use either of these power management policies:

- Redundant AC Power Source (with or without throttling)
- Non-Redundant

Depending upon the power management policy that you select in the AMM, the power modules can supply AC power as shown in Table 2-24.

Table 2-24 Available power for two power modules

Policy	110 V supply	220 V supply
Redundant AC Power Source	950 W	1450 W
Non-Redundant	1900 W	2900 W

Tip: This power module configuration is the preferred configuration when only two power supplies are used.

Figure 2-30 shows the example configuration.

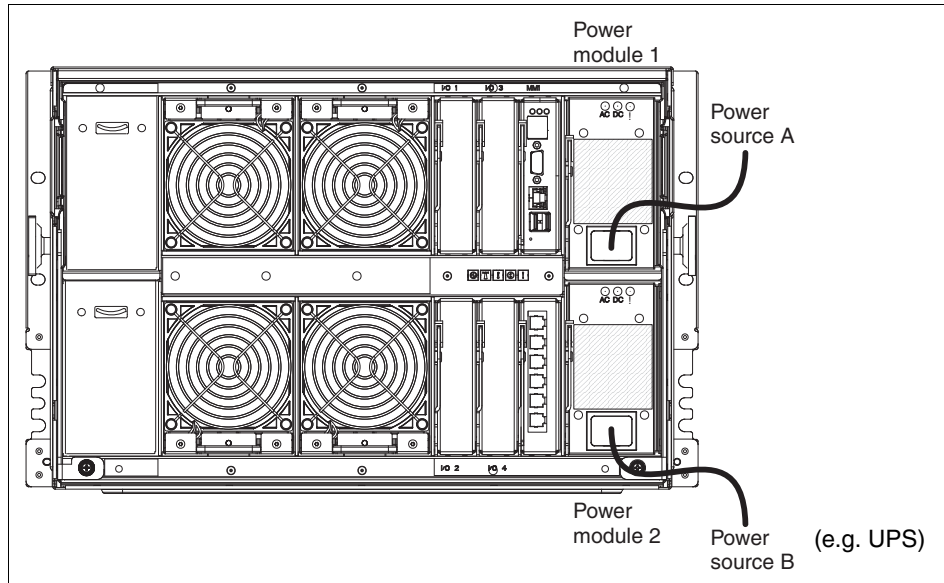


Figure 2-30 Two Power Supply Module configuration connected to different power sources

Example three

The third example involves two pairs of power modules, with each pair connected to a separate power source. This configuration can provide power redundancy within the chassis and fault tolerance of the AC power that is supplied to the chassis. If two modules or an entire power source fails, the AMM can try to throttle blade servers in an attempt to reduce the power draw below the maximum capacity of the remaining two power supplies (1900 W). If power demand cannot be reduced below the maximum available capacity, the chassis shuts down and immediately powers off all components and blades.

If two power modules or an entire power source fails, the chassis remains functional. However, half of the total power available to the chassis is lost. If a redundant power management policy is in place, the chassis continues to operate normally.

If a non-redundant power policy is set and two modules or an entire power source fail, the AMM tries to throttle blade servers to reduce the power draw

below the maximum capacity of the remaining two power supplies (2900 W). If power demand cannot be reduced below the maximum available capacity, the chassis shuts down and immediately powers off all components and blade servers.

You can select one of these power management policies:

- ▶ Redundant AC Power Source (with or without throttling)
- ▶ Redundant power modules (with or without throttling)
- ▶ Non-Redundant

Depending upon the power management policy that you select in the AMM, the power modules can supply AC power as shown in Table 2-25.

Table 2-25 Available power for four power modules

Policy	110 V supply	220 V supply
Redundant AC Power Source	1900 W	2900 W
Redundant power modules	2850 W	3562 W ^a
Non-Redundant	3477 W ^a	3562 W ^a

a. This limit is set by the AMM.

Figure 2-31 shows the example configuration.

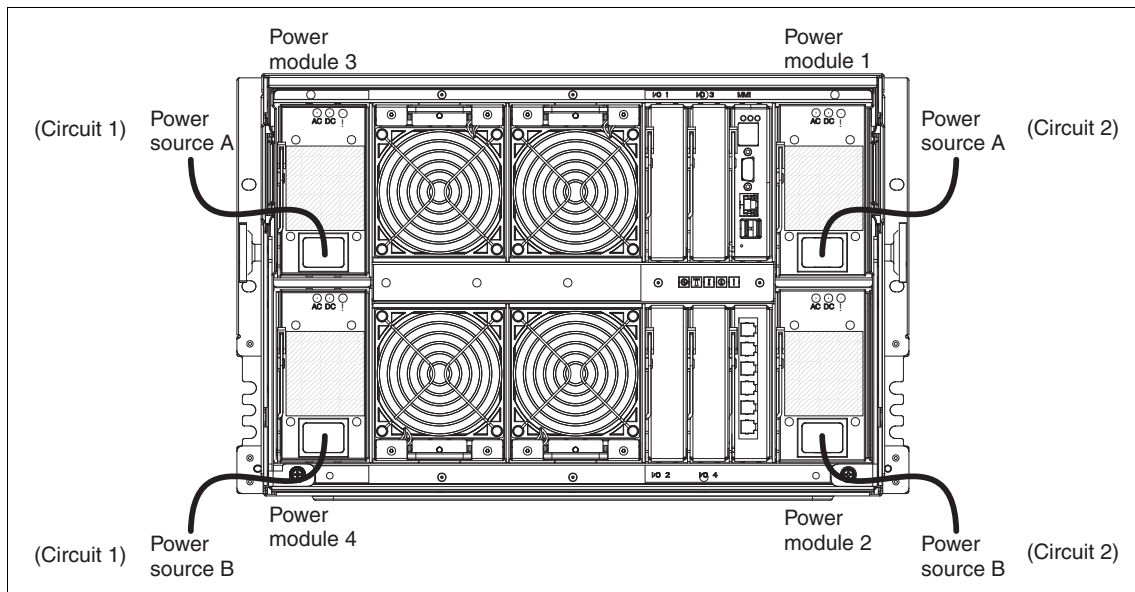


Figure 2-31 Four Power Supply Module configuration connected to two separate power sources

Example four

The fourth example involves four power modules, each connected to a separate power source. This configuration can provide power redundancy within the chassis and fault tolerance of the AC power that is supplied to the chassis.

If two modules or two power sources fail, the AMM tries to throttle blade servers to reduce the power draw below the maximum capacity of the remaining two power supplies (1900 W). If power demand cannot be reduced below the maximum available capacity, the chassis shuts down and immediately powers off all components and blade servers.

If two power modules or a power source fail, the chassis remains functional. If a redundant power management policy is in place, the chassis continues to operate normally. If a non-redundant power policy is set and two modules or a power source fail, the AMM tries to throttle blade servers to reduce power draw below the maximum capacity of the remaining power supplies (2900 W if two power supplies fail or 3562 W¹ if one power source failed). If power demand cannot be reduced below the maximum available capacity, the chassis shuts down and immediately powers off all components and blade servers.

The advantage of this configuration is that it isolates the effects of power interruption caused by events external to the chassis. In this example, up to two separate power sources can be lost and the chassis remains operational.

You can select one of these power management policies:

- ▶ Redundant AC Power Source (with or without throttling)
- ▶ Redundant power modules (with or without throttling)
- ▶ Non-Redundant

Depending upon the power management policy that you select in the AMM, the power modules can supply AC power as shown in Table 2-26.

Table 2-26 Available power for four power modules

Policy	110 V supply	220 V supply
Redundant AC Power Source	1900 W	2900 W
Redundant power modules	2850 W	3562 W ^a
Non-Redundant	3477 W ^a	3562 W ^a

a. This limit is set by the AMM.

¹ The maximum power (if the chassis is installed with the most components) that the BladeCenter S chassis can consume is calculated as 3562 W. This is despite the fact that the power supplies can generate up to 4350 W. To aid management and control, the firmware of the AMM is set to limit power consumption to 3562 W. If the need arises (for example, newer blade servers or modules with higher power requirements), this limit can be raised by using an AMM firmware update.

Figure 2-32 shows the example configuration.

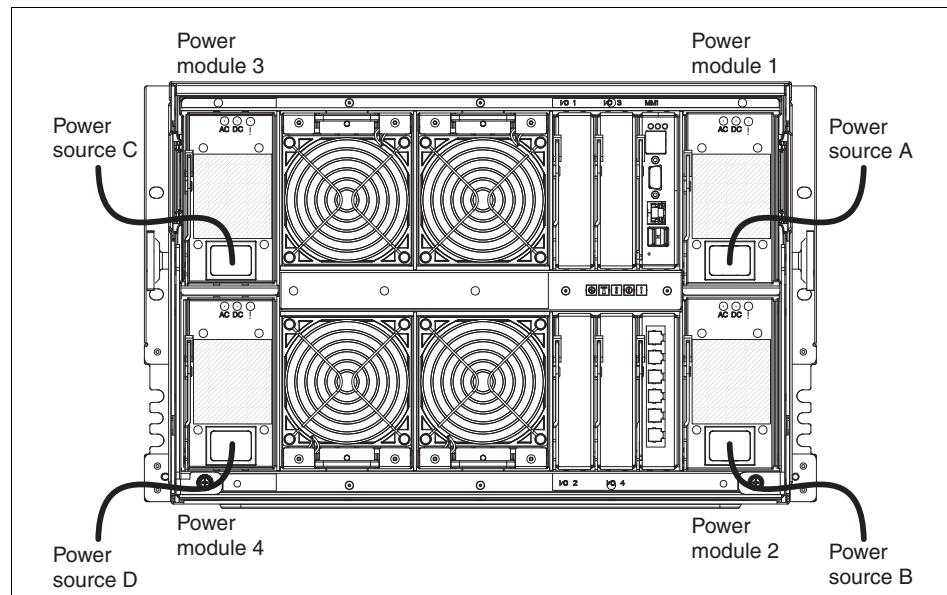


Figure 2-32 Four Power Supply Module configuration connected to four separate power sources

2.18 IBM uninterruptible power supply offerings

An uninterruptible power supply (UPS) provides emergency power to a system when there is a loss of power. A properly sized and configured UPS can perform several functions:

- ▶ Sustain the system for some time.
- ▶ Perform an orderly system shutdown so that no data is corrupted by a sudden power loss.
- ▶ Trigger a system restart when mains power returns.

To size a UPS properly, you must know the total power requirements of what will be connected to it. This information is available from the IBM Power Configurator, which can be downloaded from:

<http://ibm.com/systems/bladecenter/resources/powerconfig.html>

When the total supported power is known, an appropriately sized UPS can be selected. After you select a UPS, the solution wiring must be determined. UPS

systems have outlet and group limits, much like PDUs, and the solution must be wired so that it does not exceed the outlet or group rating of the UPS.

The chassis, external enclosures, and UPS systems must be wired according to system nameplate rating for compliance with local electrical codes and product support documentation.

The IBM BladeCenter S has four power modules that are fed from AC power connections. The BladeCenter S is unique in the BladeCenter family because it is the only system that can be powered on either 110 V and 208/220/240V. The different voltages affect maximum output. Table 2-27 lists the difference between the two power voltages.

Table 2-27 Voltage comparisons for BladeCenter S

	100-127 V	200-240 V
Power module maximum input current (amps)	11.2 A (AC)	8 A (AC)
Power module input voltage (volts)	100-127 V (AC)	200-240 V (AC)
Power module maximum power output (watts)	950 W (DC)	1450 W (DC)

IBM has a range of UPS solutions that available for the BladeCenter S as listed in Table 2-28.

Table 2-28 Supported IBM UPS units

Model	IBM UPS description
21301RX	UPS 3000 LV
21302RX	UPS 3000 HV
21304RX	UPS10000XHV
24195KX	UPS 5000
53952xx	2200VA LCD 2U Rack UPS 100 V/120 V
53953AX	3000VA LCD 3U Rack UPS 100 V/120 V
53953JX	3000VA LCD 3U Rack UPS 200 V/208 V
53956AX	6000VA LCD 4U Rack UPS 200 V/208 V
53959KX	6000VA LCD 4U Rack UPS 230 V
53959KX	11000VA LCD 5U Rack UPS 230 V

The *IBM BladeCenter Power Guides* provides more in-depth UPS solution design and list the models supported. These documents are available from:

<http://ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS4401>



Getting started using the BladeCenter S chassis

IBM offers the customer a wide range of tools for the BladeCenter S chassis. This chapter describes the use of those tools.

This chapter covers the following topics:

- ▶ 3.1, “AMM configuration” on page 100
- ▶ 3.2, “AMM Configuration Wizard” on page 103
- ▶ 3.3, “ServerGuide Scripting Toolkit” on page 148
- ▶ 3.4, “Using the command-line interfaces” on page 150
- ▶ 3.5, “IBM Fabric Manager” on page 151
- ▶ 3.6, “BladeCenter S tips and guidelines” on page 161

Start Now Advisor: Start Now Advisor was originally the preferred tool for initial setup. However, the version available at the time of writing, Version 2.2, did not support any of the currently available BladeCenter servers (HS23, HS23E, HX5). It also does not support the SAS Connectivity Card (CIOv). As a result, this chapter does not cover the use of Start Now Advisor.

3.1 AMM configuration

This section addresses connecting to the advanced management module (AMM) for the first time, and how to configure the BladeCenter S for use. There are three ways you can configure the system:

- ▶ AMM Configuration Wizard Express path
- ▶ AMM Configuration Wizard Custom path
- ▶ AMM command-line interface

When you power on the BladeCenter S for the first time, or in most cases after you replace an existing AMM, the module requires an initial setup. If this is your first use of the BladeCenter S, generally use the Express path of the wizard.

3.1.1 Setting up the advanced management module

The AMM is a powerful and robust systems management solution that provides the BladeCenter S with sophisticated configuration abilities that use self-explanatory wizards and menus.

You can easily perform initial configuration of the management module by connecting to the AMM through its Ethernet port through a switch, router, or patch cable. If the management module is not connected to a network with DHCP configured, it eventually defaults to its preconfigured static IP address, 192.168.70.125. If the management module is connected to a network and has active and correctly configured DHCP, the AMM receives its IP address, gateway, subnet mask, and DNS addresses from the DHCP server.

When the DHCP option is used with an AMM, the host name is set to its default burned-in Media Access Control (MAC) address. The MAC address is on a label on the management module, beneath the reset button. When shipped from IBM, normally there is a white tag hanging from the AMM that shows the default IP address on one side and the MAC address on the other.

Tip: To connect to the management module for the first time, it might be easier to directly connect a notebook or workstation that is configured with an IP address on the default subnet of the management module.

Figure 3-1 shows the location of the MAC address label on the AMM.

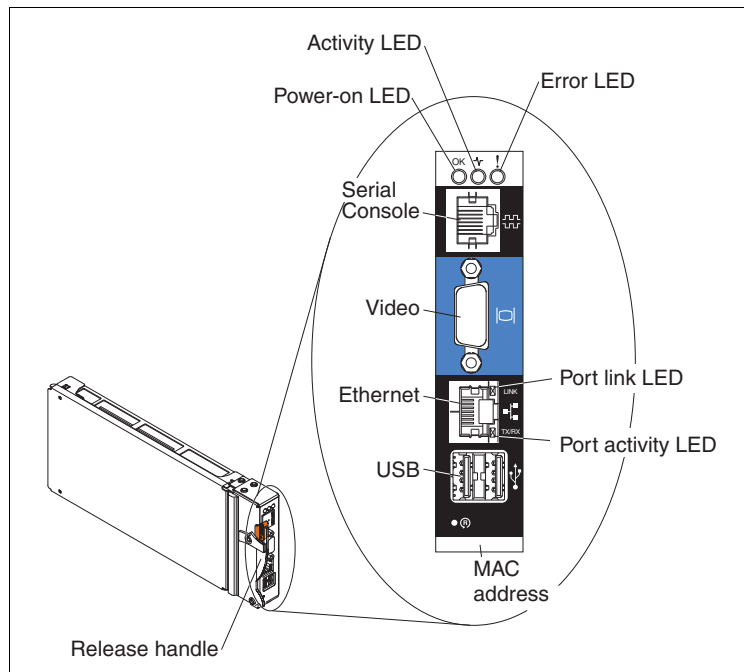


Figure 3-1 AMM showing location of MAC address label

3.1.2 Connecting to the AMM for the first time

Before initial configuration of the AMM can begin, its Ethernet port must be configured with an IP address. If the management module is going to be connected to a network using the DHCP option, all required network configuration information is automatically obtained. If the module is going to be connected using a directly connected patch cable, or a network without DHCP, the management module defaults to its preconfigured IP address settings.

DHCP timeout: You cannot connect to the AMM by using the factory-defined static IP address and default subnet until the timeout period (approximately three minutes) for the DHCP request ends.

If the management module defaults to its preconfigured settings, you can still use the DHCP configuration option. Reset the module by removing it from the chassis for two minutes and then reinserting it, or by holding in the reset pin above the MAC address for ten seconds. This causes the AMM to reboot, and the DHCP address request process begins again. If the management module is still not

accessible after three minutes, connect directly to the Ethernet port by using a notebook or workstation. Then, proceed with initial configuration or reset the AMM to its default settings.

To reset the AMM to its default settings, complete the following steps:

1. Insert a paper clip into the pin hole on the back of the advanced management module. The pin hole is directly above the MAC address label on the bottom of the AMM. See Figure 3-1 on page 101 for the exact location.
2. Push the paper clip in all the way and hold it for approximately 10 seconds. All lights on the advanced management module reset and the fans run at full speed, which is clearly audible.
3. Remove the paper clip from the pin hole.

DHCP has priority over static: By default, the AMM is configured to respond to DHCP first before using its static IP address. If the management module is connected to an Ethernet subnet with an active DHCP server, it is not accessible by using its default IP address.

If you connect to the AMM through its Ethernet interface by configuring your notebook with a static IP address, generally select a client IP address below 192.168.70.125. Do so because IP addresses 192.168.70.125 through 192.168.70.130 might already be reserved by the default IP addresses of installed I/O expansion modules. Although only one Ethernet connection or IP address might seem to exist, the module can act as a proxy for internal components, providing pass-through network access.

Ethernet connection (browser-based)

After you connect the Ethernet cable from the management module to the client computer, complete the following steps:

1. Specify a valid IP address within the address space of the subnet that is used by the AMM (for example, 192.168.70.100).
2. Make sure that the subnet of the client computer is set to the same value as the subnet used by the AMM (for example, 255.255.255.0).
3. Open a web browser on the client computer and enter the management module's default IP address (192.168.70.125) or host name if using DHCP. MMxxxxxxxxxxxx where xxxxxxxx is the MAC address of the AMM.
4. Enter the default user name, USERID, and the default password, PASSWORD to start the initial remote session. Note the number zero (0), not the letter O, in PASSWORD.
5. Set the timeout value of your session and click **Start New Session**.

After you successfully connect the client computer to the AMM for the first time, perform the initial configuration of the management module. You can use the AMM Configuration Wizard, the web interface, or the command-line interface (CLI):

- ▶ The wizard is addressed in 3.2, “AMM Configuration Wizard” on page 103.
- ▶ The CLI is described in 3.4, “Using the command-line interfaces” on page 150.
- ▶ The web interface is described in Chapter 5, “AMM user interface guide” on page 317.

For more information, see the following product documentation:

- ▶ *IBM BladeCenter Advanced Management Module for BladeCenter and BladeCenter H Installation Guide*
- ▶ *IBM BladeCenter Advanced Management Module User's Guide*
- ▶ *Advanced Management Module Command Line Interface Reference Guide*

These books are available at:

<http://www.ibm.com/systems/bladecenter/support/>

3.2 AMM Configuration Wizard

For initial configuration of a few BladeCenter S units, generally use the Express option of the AMM Configuration Wizard. This option gets the BladeCenter S up and running in the quickest manner, and requires minimal knowledge of management module configuration. For more information about the AMM and its advanced options, see Chapter 5, “AMM user interface guide” on page 317.

The initial AMM Configuration Wizard starts immediately when you log in to the management module for the first time as shown in Figure 3-2.

Welcome to the Advanced Management Module Configuration Wizard

This wizard will help you through the tasks of configuring the Advanced Management Module (AMM) and other chassis components. Please select the configuration method you wish to use:

Select how you wish to configure the chassis components

☒ **Express** Gets you up and running quicker by preselecting a number of common settings and giving you less to configure. [Details](#)

☐ **Custom** You will be prompted for the necessary information for each individual component. [Details](#)

Please note that you could lose information if you navigate away from this wizard to another web page or click the reload button on your browser.

☐ **Run this wizard on the next login.**

[Exit Wizard](#) [Next >](#)

Figure 3-2 The AMM Configuration Wizard

Tip: If the wizard does not start automatically, you can start it manually by clicking **Start Configuration Wizard** in the Configuration Management section under the MM Control heading in the left pane (Figure 3-3).

Configuration Management

Use the following links to jump down to different sections on this page.

- [Restore Defaults](#)
- [Backup Configuration to File](#)
- [Restore Configuration from File](#)
- [Save Configuration to Chassis](#)
- [Restore Configuration from Chassis](#)
- [Start Configuration Wizard](#)

Figure 3-3 Starting the configuration wizard

There are two paths in the configuration wizard:

- ▶ 3.2.1, “Using the AMM Wizard Express path” on page 107
- ▶ 3.2.2, “Using the AMM Wizard Custom path” on page 126

Express path activates the following features:

- ▶ Enabling secure web connectivity by using the Secure Sockets Layer (SSL) communication protocol, requiring only a few items to be entered for self-signed certificate generation
- ▶ Enabling secure CLI connectivity by using the Secure Shell (SSH) communication protocol
- ▶ Enabling remote notification through email for critical events
- ▶ Selecting a basic, default storage configuration
- ▶ By default, these functions are explicitly disabled when you use the Express mode:
 - Warning and informational events
 - Simple Network Management Protocol (SNMP) V1 and SNMP V3
 - Network Time Protocol (NTP)
 - Automatic export of the newly created configuration to the chassis as a backup

Custom path activates these features:

- ▶ Import of a saved configuration from the chassis or from a file on the user's computer
- ▶ Configuration of SSH and SSL for secure communication with the AMM
- ▶ Customized selection of event notifications that is based on severity categories
- ▶ Configuration of network management using SNMP V1 and SNMP V3
- ▶ Enabling of NTP to synchronize time and date
- ▶ Performance of more involved storage configuration operations
- ▶ Export of the newly created configuration to the chassis or to a file on the user's computer

Use the Custom path if you are familiar with the AMM. You can also configure or reconfigure all of the setup items that are contained in the Custom path after initial setup by using the Express method. If you need help determining which path is best for you, click the **Details** link in Figure 3-2 on page 104 for a

comparison of each path and the available options. The **Details** link loads the page that is shown in Figure 3-4.

Help for Advanced Management Module Initial Configuration Wizard		
The default values for the fields in this wizard will be the current value of each particular field as displayed in the main interface. If this is the first time that you are configuring the Management Module, the default values will, for the most part, be the factory defaults.		
If you do not wish to use this wizard or change your mind at any point, click the "Exit Wizard" button and you will return to the AMM web user interface (UI). Your selections will be discarded and no changes will be made to the existing configuration. Otherwise, when you reach the end of the wizard, you will be prompted to save all of the settings.		
There are two configuration methods that you can use: Express or Custom. The table below shows a comparison of how configuration settings are handled with each method.		
	Custom	Express
Import from a configuration file	Yes	No
General Settings (AMM descriptive name, your contact information)	Yes	Yes
Set Date and Time on AMM	Yes	Yes
Sync with Network Time Protocol (NTP) server	Yes	No
AMM Network Configuration (Set IP address, DHCP)	Yes	Yes
I/O Module Configuration (Set IP address, external port enablement)	Yes	Yes
Change default user profile credentials	Yes	Yes
Secure Sockets Layer (SSL)	Can enable or disable, choose whether to generate a certificate	Always enabled, must generate self signed certificate
Secure Shell (SSH)	Can enable or disable	Always enabled
Domain Name Service (DNS)	Can enable or disable	Can enable or disable
Event Notifications	Can enable or disable, can select any combination of informational, warning, or critical events. Can add e-mail recipient for events	Yes, critical events only, e-mail notification only. Can add e-mail recipient for events
Simple Network Management Protocol (SNMP)	Can enable or disable	Disabled
Export/save configuration to chassis	Yes, optional	Yes, automatic, not configurable
Export/save configuration to an external file	Yes, optional	No
Storage configuration	Yes	Yes

Figure 3-4 AMM Configuration Wizard help

The default values for the fields in this wizard are the current values in the AMM. If this is the first time that you configure the AMM, the default settings are the factory defaults. One exception is that the Express configuration changes certain values based on how it preselects choices.

If you do not want to use this wizard or change your mind at any point, click **Exit Wizard**. You will return to the AMM web user interface. Your selections are discarded and no changes are made to the existing configuration. Otherwise, when you reach the end of the wizard configuration steps, you are prompted to accept all of the settings.

Note: If the AMM has been configured before, you might receive errors when you use the Configuration Wizard. Errors are more likely if the firmware has been upgraded since the last configuration changes were made. Therefore, reset the AMM to factory defaults if you receive errors, the AMM firmware has changed, or you are configuring a replacement AMM. For reset instructions, see 3.1.2, "Connecting to the AMM for the first time" on page 101.

3.2.1 Using the AMM Wizard Express path

The first window in the configuration wizard asks which method to use to configure the AMM. There are two paths: Express and Custom as shown in Figure 3-5.

Welcome to the Advanced Management Module Configuration Wizard

This wizard will help you through the tasks of configuring the Advanced Management Module (AMM) and other chassis components. Please select the configuration method you wish to use:

Select how you wish to configure the chassis components

☒ **Express** Gets you up and running quicker by preselecting a number of common settings and giving you less to configure. [Details](#)

☐ **Custom** You will be prompted for the necessary information for each individual component. [Details](#)

Please note that you could lose information if you navigate away from this wizard to another web page or click the reload button on your browser.

☐ **Run this wizard on the next login.**

[Exit Wizard](#) [Next >](#)

Figure 3-5 Step 1 of the AMM Configuration Wizard

To use the Express path to configure the BladeCenter S, complete the following steps:

1. Select **Express** and click **Next** to continue.
2. The Getting Started window (Figure 3-6) provides a list of information that are used to complete the initial configuration. You can print this information for reference by clicking **View Configuration Worksheet** → **Print Worksheet**. Not all of the information is required during initial setup, and any setting can be changed after initial configuration is completed. Click **Next** to continue.

Getting Started

Some of the information provided by the wizard is based on the hardware components inserted into your chassis. At this time, ensure that all the required hardware is properly installed, then click Next.

Also at this time you may wish to make note of the information that will be needed to complete this wizard:

1. Contact information for AMM administrator
2. Network IP addresses and hostname information for the AMM
3. Network IP addresses information for any I/O modules
4. A new Login ID and password for the default "administrator" login profile
5. Relevant IP addresses for Domain Name Server (DNS)
6. Target email address and SMTP server information for event notifications

Ensure that you have the most recent firmware

You may need to update the firmware for the Management Module. This requires that you go to the ibm.com support web site and obtain the latest firmware. You will have the option of updating the firmware at the end of this wizard. The full details, including your current firmware level, are in the configuration worksheet, available from the button below.

If desired, you can also print the configuration worksheet to help you gather the needed information. To do this, click the button below.

[View Configuration Worksheet](#)

[Exit Wizard](#) [< Back](#) [Next >](#)

Figure 3-6 Step 2 of the AMM Configuration Wizard

3. The Hardware and Status Information window (Figure 3-7) provides a brief summary of the BladeCenter S chassis, and its installed blade servers and components. Click **Next** to continue.

No active zone: When you configure the chassis for the first time, you receive a warning that the SAS Connectivity Modules do not have an active zone. This is normal.

Hardware and Status Information











The hardware that was discovered in the chassis and status is shown below. In order to properly configure the chassis, all should have a normal status. If any status shows an error or you do not see hardware listed here that you have put into the chassis, then you should fix those problems before continuing with this wizard.

System Status Summary

Warnings and System Events

- [\(03/07/13 05:43:16\) I/O Module 3 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.](#)

At-a-glance System and Component Status Summary

Bay	Description	Status
<i>Blades</i>		
1	HS22_Blade_1	
2	SN#Y010UF18E0B9	
3	ADXblade1	
4	Blade13-HS22	
5	ADXblade2	
6	SN#Y111UN234018	
<i>I/O Modules</i>		
1	Ethernet SM	
3	SAS Conn Mod	
4	SAS Conn Mod	
<i>Management Modules</i>		
1	bcamm6	
<i>Power Modules</i>		

Exit Wizard< BackNext >

Figure 3-7 Step 3 of the AMM Express Configuration Wizard

4. The General Settings window (Figure 3-8) asks for the AMM name, location, and contact information. Input from these fields is intended for administrative purposes only, and is not used by the management module for host name or alert notification. If you manage multiple BladeCenter chassis, the information that is entered on this window can be useful for future reference.

Enter a reference name for the AMM (typically, the same as the host name), the specific location of the BladeCenter S chassis, and the administrator contact information. Then, click **Next**.

General Settings

General Information

The Advanced Management Module name, location and contact information fields are optional, and can contain any information you would find useful in locating and maintaining your AMM.

Advanced Management Module name:
BC6MM

Location:
IBM RTP Building 305

Administrator contact information:
David Watts

Exit Wizard < Back Next >

Figure 3-8 Step 4 of the AMM Express Configuration Wizard

5. On the AMM Network Interface window (Figure 3-9), enter the host name and IP address information for the management module.

The host name field on this window is what will be registered with DNS after the AMM is rebooted. Therefore, use a static IP assignment for the management module. On the **DHCP** menu, select **Disabled - Use Static IP Configuration** and then enter the network settings that need to be used in the Static IP Configuration section.

AMM Network Interface

AMM Network Interface (eth0)

This is the interface the Advanced Management Module uses to connect to your management network.

Interface status: **Enabled**

Hostname:
BC6MM

DHCP:
Disabled - Use static IP configuration

To manually configure the IP settings, choose "Disabled". To obtain an IP address from a DHCP server, choose "try DHCP server." In the event that the server cannot be reached, the system will failover to the static IP you enter below.

Static IP Configuration

This will be your Advanced Management Module's IP address if you select Disabled above, or in the event of failover.

IP address (default is 192.168.70.125):
9.42.171.1

Subnet mask (default is 255.255.255.0):
255.255.254.0

Gateway address:
9.42.170.1

Note: Changes to network settings will take effect after the next restart of the AMM.

Exit Wizard < Back Next >

Figure 3-9 Step 5 of the AMM Express Configuration Wizard

6. Be sure to double-check the IP address information because these settings are the active settings when the AMM reboots. If you configure the management module remotely, be sure that you can access the subnet for the IP address for which you are setting up the module.

Potentially, you might assign an IP address of a network subnet that you cannot access. If you do so, the management module can become inaccessible for further remote configuration.

AMM reboot required: Changes to the AMM network configuration are only activated after the module reboots. When you change the management module, you can undo or change settings until you restart the AMM.

7. After you review the static IP configuration settings, click **Next**.
8. The I/O Module Configuration window (Figure 3-10) is designed to gather network setting information for the I/O Expansion Modules that are installed in the BladeCenter S chassis. The network settings that are specified on this window are for the individual administrative access interfaces of the modules.

The administrative interfaces, typically web-based or Telnet-based, of most I/O Expansion Modules offer detailed information about the performance of their module and extra configuration capabilities. Configuring the modules through their administration interface is optional and not a requirement for normal operation.

I/O Module Configuration

The following I/O modules (e.g., switches, pass-through modules) were found in this chassis. Please specify the network configuration information for the components below.

☒ All I/O Modules use the same subnet mask:

☒ All I/O Modules use the same gateway:

Bay	Description	Static IP Address	Enable External Ports	Enable External Control on Ports	Preserve IP Address on Reset
1	Ethernet SM	<input type="text" value="9.42.171.89"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	SAS Conn Mod	<input type="text" value="9.42.171.67"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	SAS Conn Mod	<input type="text" value="9.42.171.68"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 3-10 I/O Module Configuration for the SAS Connectivity Module

9. If all I/O modules use the same subnet and gateway (preferred configuration), check the two option boxes. Then, enter the IP address information for each module. If you want the external ports automatically enabled on the restart of the AMM, select **Enable External Ports** for each module. If this option is not checked, the external ports/uplinks on the Ethernet switch and the SAS module are not functional after the management module restarts.

If all I/O modules do not use the same subnet and gateway, click to clear the two option boxes and enter the additional network settings in the fields next to the module's IP address.

10. Leave **Enable External Control on Ports** cleared. Only enable external control if you have the I/O modules and the advanced management module on separate subnets or VLANs.
11. If you want the user-defined IP configuration settings to be preserved when the module's factory defaults are restored, or when a reset is initiated by a source other than the management module, select **Preserve IP Address on Reset**. If this is not selected, the factory default IP configuration settings become active when the I/O module factory defaults are restored, or when an I/O module reset is initiated by a source other than the management module.
12. After you enter the network settings and select the management options, click **Next**. You can modify I/O module information further after the initial AMM configuration is completed.

If you are using the advanced management module to configure a BladeCenter S chassis that has the SAS RAID Controller Module, you must configure two IP addresses for each controller: One for the SAS Switch and another for the RAID Controller, as shown in Figure 3-11.

I/O Module Configuration

The following I/O modules (e.g., switches, pass-through modules) were found in this chassis. Please specify the network configuration information for the

☒ All I/O Modules use the same subnet mask:

☒ All I/O Modules use the same gateway:

Bay	Description	Static IP Address	Enable External Ports	Enable External Control on Ports
1	Ethernet SM	<input type="text" value="9.42.171.89"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	SAS RAID Ctrl Mod		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	└ SAS SW	<input type="text" value="9.42.171.67"/>		
	└ RAID Ctrl	<input type="text" value="9.42.171.68"/>		
4	SAS RAID Ctrl Mod		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	└ SAS SW	<input type="text" value="9.42.171.37"/>		
	└ RAID Ctrl	<input type="text" value="9.42.171.38"/>		

Figure 3-11 I/O Module Configuration for the SAS RAID Controller Module

13. On the Login Profile window (Figure 3-12), you can change the user ID and password of the AMM default login account. Change at least the password of the default USERID account. More accounts can be created after the initial AMM configuration is complete.

Default Profile

This is the default user ID. You can change both the user ID and the password here. It is **highly** recommended that you change at least the password.

Administrative (read/write access) Login ID (default is USERID):

New Password:

Confirm New Password:

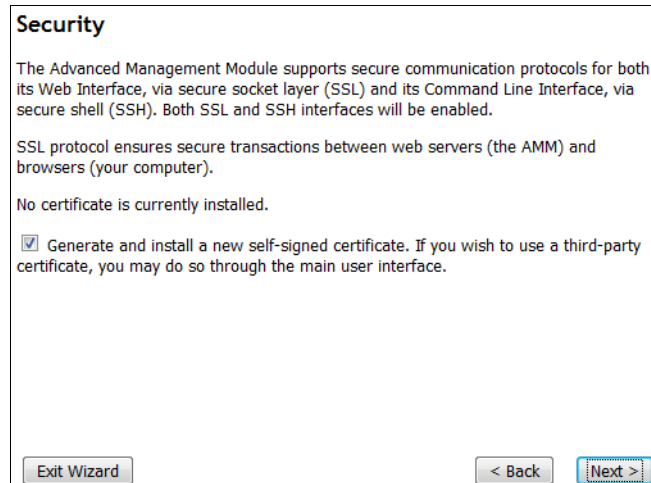
Note: You can enter additional profiles and enable LDAP verification from the main Advanced Management Module UI after completing this wizard.

Figure 3-12 Step 7 of the AMM Express Configuration Wizard

Default password: The default user name and password for the AMM (USERID and PASSWORD) have been used for years. They are well known by anyone who has worked with BladeCenter or System x servers before. Change the user name and password to prevent unauthorized access to the management module.

14. After you change the login information, click **Next**.

15. If you want to enable SSL or SSH communication protocols (Figure 3-13), check **Generate and install a new self-signed certificate** and then click **Next**.



The screenshot shows a window titled "Security". The text inside reads: "The Advanced Management Module supports secure communication protocols for both its Web Interface, via secure socket layer (SSL) and its Command Line Interface, via secure shell (SSH). Both SSL and SSH interfaces will be enabled." Below this, it says: "SSL protocol ensures secure transactions between web servers (the AMM) and browsers (your computer)." Then: "No certificate is currently installed." There is a checked checkbox followed by the text: "Generate and install a new self-signed certificate. If you wish to use a third-party certificate, you may do so through the main user interface." At the bottom, there are three buttons: "Exit Wizard", "< Back", and "Next >".

Security

The Advanced Management Module supports secure communication protocols for both its Web Interface, via secure socket layer (SSL) and its Command Line Interface, via secure shell (SSH). Both SSL and SSH interfaces will be enabled.

SSL protocol ensures secure transactions between web servers (the AMM) and browsers (your computer).

No certificate is currently installed.

☒ Generate and install a new self-signed certificate. If you wish to use a third-party certificate, you may do so through the main user interface.

Exit Wizard < Back Next >

Figure 3-13 Step 8 of the AMM Express Configuration Wizard

16. If you selected to enable SSL and SSH protocols, the SSL Server Self-signed Certificate window is displayed as shown in Figure 3-14. Complete the required information, and if you want, complete the optional data fields that will appear in the certificate. The email address that you provide in this section is not be used for alert notification.

SSL Server Self-signed Certificate	
Required Certificate Data	
Country (2 letter code)	US
State or Province	NC
City or Locality	Raleigh
Organization Name	IBM
MM Hostname	BC6MM
Optional Certificate Data	
Contact Person	John Smith
Email Address	js@example.com
Organizational Unit	IT Support
Surname	Smith
Given Name	John
Initials	US
DN Qualifier	
Years Valid	20
Exit Wizard < Back Next >	

Figure 3-14 Step 9 of the AMM Express Configuration Wizard

17. The certificate will be presented to your web browser or SSH application when you log in to the AMM after the first restart. Verify the information that is on this window, then click **Next**.

18. On the Domain Name Server window (Figure 3-15), select whether the DNS for the AMM must be enabled or disabled. If you want to enable it, enter the IP address of the DNS in your environment and click **Next**.

Note: If you do not enable DNS, you must specify IP addresses for any other protocols you want to enable such as SMTP, SNMP, and NTP.

The screenshot shows a window titled "Domain Name Server". Inside, there is a sub-header "Domain Name Server" followed by a paragraph: "If you have a dynamic host configuration protocol (DHCP) server on your network, the field(s) below may be populated with the IP addresses of the domain name servers (DNS) on your network. If your network does not have a DHCP server, and you wish to enable DNS, you will need to enter the IP address of at least one DNS." Below this text, there is a "DNS" label and a dropdown menu set to "Enabled". Underneath, there are three input fields labeled "DNS IP 1", "DNS IP 2", and "DNS IP 3". The first two fields contain the IP addresses "168.244.1.3" and "168.244.1.4" respectively. The third field contains "168.244.1.5". At the bottom of the window, there are three buttons: "Exit Wizard" on the left, and "< Back" and "Next >" on the right.

Domain Name Server	
If you have a dynamic host configuration protocol (DHCP) server on your network, the field(s) below may be populated with the IP addresses of the domain name servers (DNS) on your network. If your network does not have a DHCP server, and you wish to enable DNS, you will need to enter the IP address of at least one DNS.	
DNS	Enabled ▾
DNS IP 1	168.244.1.3
DNS IP 2	168.244.1.4
DNS IP 3	168.244.1.5
Exit Wizard < Back Next >	

Figure 3-15 Step 10 of the AMM Express Configuration Wizard

19. In the Event Notifications window (Figure 3-16), specify the recipient's contact information for event notification. The **Enable event notifications** option must be selected for alert notification to work. A test of alert notification can be sent from the **Alerts** menu of the AMM web interface after the AMM is restarted.

Tip: If you are going to rely on email event notification, be sure to conduct a test event to ensure that the email and SMTP address are entered correctly. Conduct this test through the **Alerts** menu of the AMM.

Event Notifications

BladeCenter can notify you of various events including hardware errors and temperature problems. Indicate an e-mail recipient below that will receive critical event notifications for your BladeCenter.

Use the section below to configure the first event recipient for email notification. If this is the first time you are configuring the Advanced Management Module (AMM), you will not see any information entered below. However, if you have previously configured the first event recipient in the AMM to use a notification method other than e-mail (e.g., SNMP), this wizard will reconfigure the recipient to use e-mail notification instead.

☒ Enable event notifications

Recipient Name
John Smith

E-mail address
js@example.com

SMTP server fully qualified hostname or IP address
mailserver.example.com

Figure 3-16 Step 11 of the AMM Express Configuration Wizard

20. In the Date and Time window (Figure 3-17), enter the correct date and time and select the appropriate GMT offset based on the location of the BladeCenter S. Remember to check the option for automatic adjustment of daylight saving changes, if applicable. The accuracy of this information is important when you are reviewing the event logs of the AMM.

After you have correctly set the date and time, click **Next**.

Date and Time

Setting the accurate date and time is important so that the events that occur are time stamped appropriately

Today's Date (mm/dd/yyyy):
03 / 06 / 2013

Current Time (hh:mm:ss):
13 : 38 : 11

GMT Offset:
-5:00 - Eastern Standard Time (Eastern USA, Ontario, Quebec)

☒ Automatically adjust for daylight saving changes

Exit Wizard < Back Next >

Figure 3-17 Step 12 of the AMM Express Configuration Wizard

21. If **Automatically adjust for daylight saving changes** was selected on the previous window, you are asked to select an available daylight saving time scheme, as shown in Figure 3-18. Select the appropriate scheme based on your location and click **Next**.

Observe Daylight Saving Time

Unable to automatically determine the daylight saving time to use.
Please provide the DST scheme:

Selected GMT offset: -5:00

Available schemes: USA and Canada

Exit Wizard < Back Next >

Figure 3-18 Step 13 of the AMM Express Configuration Wizard

22. Select a storage configuration. You can select one of the predefined configurations by clicking the name of the configuration. This displays a visual representation of the configuration (Figure 3-19). Then, click **Activate Selected Configuration**, which is shown at the bottom of the window.

For more information about storage configurations and zoning, see the remainder of this chapter, starting with 4.2, “Understanding storage zones” on page 168.

Click **Next** to continue.

Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date
<input type="radio"/>	✓	Predefined Config 02	Pre-defined	6	2	1	6	04/24/2002:00:00
<input type="radio"/>		Predefined Config 03	Pre-defined	6	1	2	7	04/24/2002:00:00
<input type="radio"/>		Predefined Config 04	Pre-defined	1	2	6	8	04/24/2002:00:00
<input type="radio"/>		Predefined Config 05	Pre-defined	1	1	12	9	04/24/2002:00:00
<input type="radio"/>		Predefined Config 06	Pre-defined	3	2	2	10	04/24/2002:00:00
<input type="radio"/>		Predefined Config 07	Pre-defined	3	1	4	11	04/24/2002:00:00
<input type="radio"/>		Predefined Config 08	Pre-defined	2	2	3	12	04/24/2002:00:00
<input type="radio"/>		Predefined Config 09	Pre-defined	2	1	6	13	04/24/2002:00:00
Select	Active?	Name	Type	Description		Configuration Store		Date
<input type="radio"/>		User Defined Config 01	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.		1		00/00/0000:00:00
<input type="radio"/>		User Defined Config 02	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.		2		00/00/0000:00:00
<input type="radio"/>		User Defined Config 03	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.		3		00/00/0000:00:00
<input type="radio"/>		User Defined Config 04	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.		4		00/00/0000:00:00
<div>Exit Wizard</div>								

Figure 3-19 Step 14 of the AMM Express Configuration Wizard

23. Figure 3-20 shows the details of the configuration that clicked the name of in Figure 3-19 on page 120.

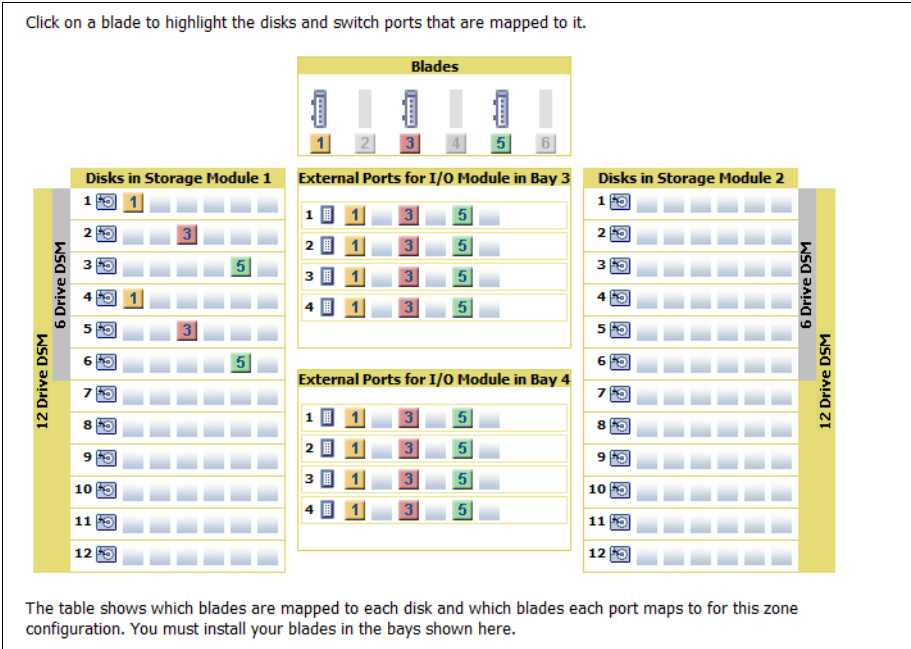


Figure 3-20 Visual representation of a configuration

24. If you are using the advanced management module to configure a BladeCenter S chassis with SAS RAID Controller Modules installed, you see only Predefined Configuration 10 as shown in Figure 3-21.

I/O Module 3 (SAS RAID Ctrl Mod) ?									
The table below lists zone configurations that is most appropriate for my current number of blades and SAS I/O Modules.									
Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date	
<input checked="" type="radio"/>	✓	Predefined Config 10	Pre-defined	6	2	12	14	04/24/2008 02:00:00	

I/O Module 4 (SAS RAID Ctrl Mod) ?									
The table below lists zone configurations that is most appropriate for my current number of blades and SAS I/O Modules.									
Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date	
<input checked="" type="radio"/>	✓	Predefined Config 10	Pre-defined	6	2	12	14	04/24/2008 02:00:00	

Figure 3-21 Configuration choices for SAS RAID Controller Module

Predefined Storage Configuration 10 for the SAS RAID Controller Module is designed so that all six blade servers have access to both SAS RAID Controller Modules in the chassis. The configuration consists of storage that is mapped to all six blade servers, two SAS RAID Controller Modules, and two fully populated disk storage modules.

Each blade server can access *all* hard disk drives in *all* disk storage module and all external ports on the SAS module, as shown in Figure 3-22.

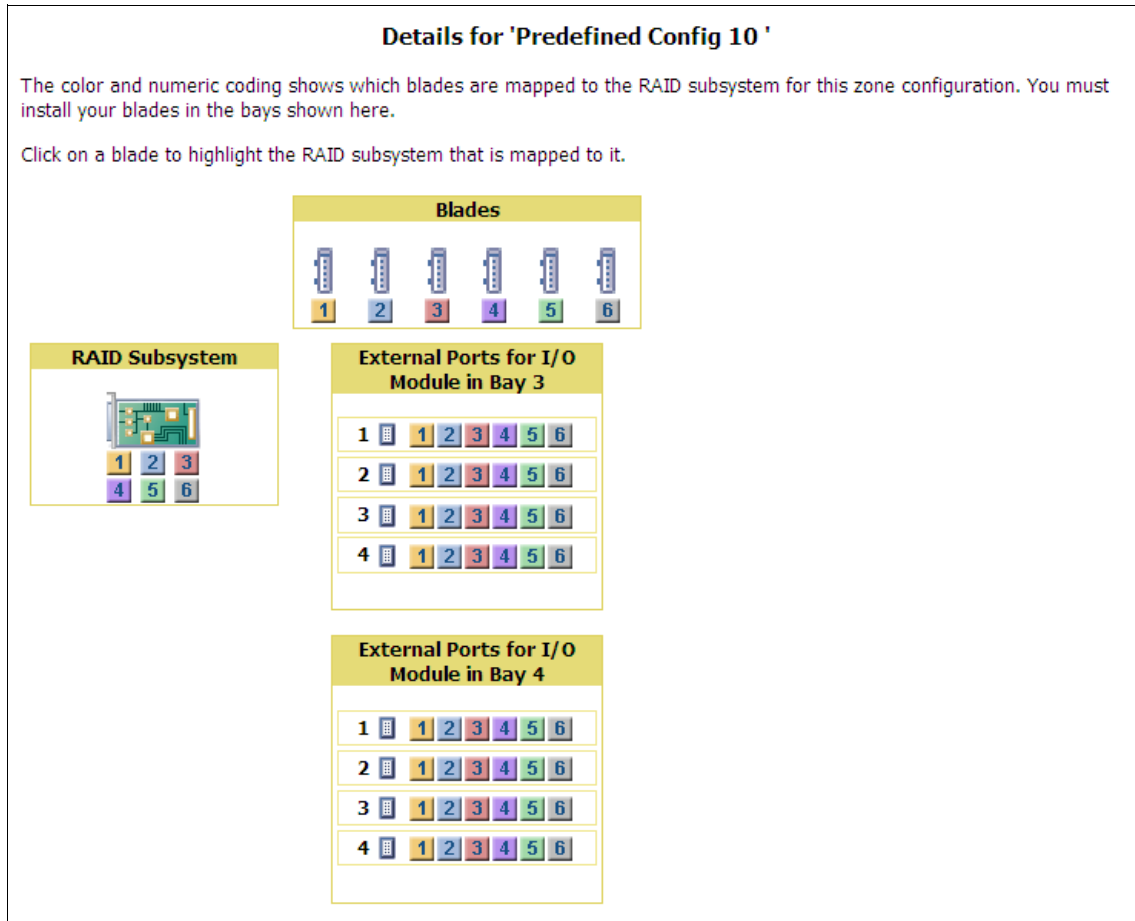


Figure 3-22 Visual representation for Predefined Configuration 10

Click **Next** to continue.

Note: The SAS Connectivity Module uses the LSI Configuration Utility in each blade server to create arrays and establish RAID support for the assigned storage. To configure RAID levels and hot-spare disks in the SAS RAID Controller Module, access the controller web interface or use Storage Configuration Manager.

25. After you complete the storage configuration for the BladeCenter S, you are presented with the Server Advisor Settings window shown in Figure 3-23. This option allows you to configure the AMM to monitor your chassis for hardware events and capture the error logs and service data. It then automatically reports the event to IBM.

Service Advisor Settings

Service Advisor resides on your Advanced Management Module (AMM) and monitors your BladeCenter Chassis for hardware events. Upon detecting a hardware event, Service Advisor captures the event, error logs, and service data, and can automatically report the event to IBM support. To send the serviceable event to IBM support, you must enable and configure Service Advisor. For each serviceable call home event IBM receives, a service ticket will be opened, and a follow-up call will be made.

☒ Enable IBM Support

Service Advisor Settings

IBM Service Support Center (Mandatory)

Enter the country code for the IBM Service Support Center. Please choose the appropriate center to satisfy your needs. A proper support center will make the handling of your Call Home request operate smoothly and easily.

IBM Support Center US - United States

Contact Information (Mandatory)

Please make sure all the fields in this section are input correctly. These configurations are necessary for Service Advisor and only valid configurations can allow Service Advisor to be enabled.

Company Name	IBM
Contact Name	John Smith
Phone	919-555-1212
Email	js@example.com
Address	3 IBM Way
City	Raleigh
State	NC
Postal code	27017

Exit Wizard< BackNext >

Figure 3-23 Service Advisor Settings window

26. After you configure the Service Advisor settings, the Wizard Configuration Summary window (Figure 3-24) is displayed. Review all information on this window. If any changes must be made, use the **Back** option to revisit the appropriate configuration wizard section. If all settings are correct, click **Save All Settings**.

You have completed entry of all the information necessary to get your chassis running and communicating with your network. Press "Save All Settings" to commit changes.

Wizard Configuration Summary

General Settings

AMM Name:	bcamm6
Location:	RTP, NC
Administrator Contact:	ITSO

AMM Network Interface

Hostname:	bcamm6
DHCP:	Disabled - Use static IP configuration
Static IP Configuration	
IP address:	9.42.171.1
Subnet mask:	255.255.254.0
Gateway address:	9.42.170.1

I/O Module Configuration

Bay 1

Static IP address:	9.42.171.89
Subnet mask:	255.255.255.0
Gateway address:	9.42.171.1
External ports:	Enabled
External control on ports:	Enabled
Preserve IP address on reset:	Enabled

Bay 3

Static IP address:	9.42.171.67
Subnet mask:	255.255.255.0
Gateway address:	9.42.171.1
External ports:	Enabled
External control on ports:	Enabled
Preserve IP address on reset:	Enabled

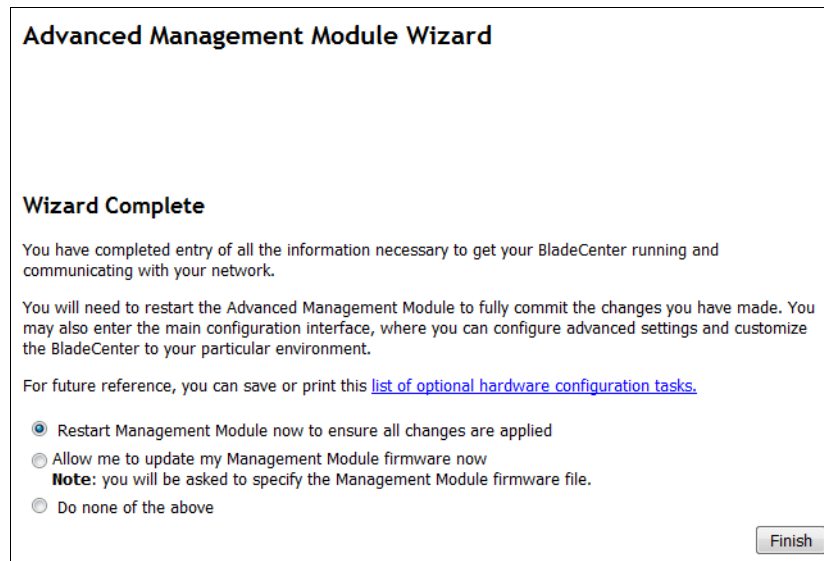
Bay 4

Static IP address:	9.42.171.68
--------------------	-------------

Figure 3-24 Summary and confirmation of the AMM Express Configuration Wizard

27. The Express path for the AMM Configuration Wizard is now complete. You are offered the option to reboot the management module, apply firmware, or do nothing. You must restart the AMM to commit and activate the settings that you entered in the wizard. Select **Reboot AMM now to ensure all changes applied** and click **Finish** (Figure 3-25).

Tip: Restarting the AMM does not affect the operation of the blade servers or the disk storage modules. The fans spin up to 100% for several seconds but then return to normal speeds (and sound volume).

The screenshot shows a web-based wizard titled "Advanced Management Module Wizard". Under the heading "Wizard Complete", it informs the user that they have completed the configuration and provides instructions on restarting the module. It includes three radio button options: "Restart Management Module now to ensure all changes are applied" (which is selected), "Allow me to update my Management Module firmware now" (with a note about specifying a firmware file), and "Do none of the above". A "Finish" button is located in the bottom right corner.

Advanced Management Module Wizard

Wizard Complete

You have completed entry of all the information necessary to get your BladeCenter running and communicating with your network.

You will need to restart the Advanced Management Module to fully commit the changes you have made. You may also enter the main configuration interface, where you can configure advanced settings and customize the BladeCenter to your particular environment.

For future reference, you can save or print this [list of optional hardware configuration tasks](#).

☒ Restart Management Module now to ensure all changes are applied

☐ Allow me to update my Management Module firmware now
Note: you will be asked to specify the Management Module firmware file.

☐ Do none of the above

Finish

Figure 3-25 Completion of the AMM Express Configuration Wizard

28. Upon clicking **Finish**, the AMM activates all changes that you made throughout the configuration wizard and reboot. Your session to the AMM ends and the browser window closes after five seconds.
- After the AMM finishes rebooting, it will be accessible by using its new IP address. If you want to configure the management module further, log in to the new address and enter the revised default user ID and password.

Tip: To track the progress of an AMM reboot, ping its new IP address by using the **ping -t** option. This begins a continuous Internet Control Message Protocol (ICMP) probe of the management module every second.

When you see replies being returned from the address of the AMM, you can log in.

3.2.2 Using the AMM Wizard Custom path

The Custom path allows you to enable and disable some functions, import and export the chassis configuration to a file, and customize the type of AMM alerts you receive and where they are sent. To use the Wizard with the Custom path option, complete these steps:

1. Activate the Custom path by selecting **Custom** and clicking **Next** as shown in Figure 3-26.

Welcome to the Advanced Management Module Configuration Wizard ?

This wizard will help you through the tasks of configuring the Advanced Management Module (AMM) and other chassis components. Please select the configuration method you wish to use:

Select how you wish to configure the chassis components

☐ **Express** Gets you up and running quicker by preselecting a number of common settings and giving you less to configure. [Details](#)

☒ **Custom** You will be prompted for the necessary information for each individual component. [Details](#)

Please note that you could lose information if you navigate away from this wizard to another web page or click the reload button on your browser.

☐ **Run this wizard on the next login.**

Figure 3-26 Step 1 of the AMM Configuration Wizard

2. The Getting Started window (Figure 3-27) provides a list of information that is used to complete the initial configuration. You can print this information for reference by clicking **View Configuration Worksheet** → **Print Worksheet**. Not all of the information is required during initial setup, and any setting can be changed after initial configuration is complete. Click Next to continue.

Getting Started

Some of the information provided by the wizard is based on the hardware components inserted into your chassis. At this time, ensure that all the required hardware is properly installed, then click Next.

Also at this time you may wish to make note of the information that will be needed to complete this wizard:

1. Contact information for AMM administrator
2. Network IP addresses and hostname information for the AMM
3. Network IP addresses information for any I/O modules
4. A new Login ID and password for the default "administrator" login profile
5. Relevant IP addresses for Domain Name Server (DNS)
6. Target email address and SMTP server information for event notifications

Ensure that you have the most recent firmware

You may need to update the firmware for the Management Module. This requires that you go to the ibm.com support web site and obtain the latest firmware. You will have the option of updating the firmware at the end of this wizard. The full details, including your current firmware level, are in the configuration worksheet, available from the button below.

If desired, you can also print the configuration worksheet to help you gather the needed information. To do this, click the button below.

[View Configuration Worksheet](#)

[Exit Wizard](#) [< Back](#) [Next >](#)

Figure 3-27 Step 2 of the AMM Configuration Wizard

3. The Hardware and Status Information window (Figure 3-28) provides a brief summary of the BladeCenter S chassis and its installed blade servers and components. Click **Next** to continue.

Note: When you configure the chassis for the first time, you will receive a warning that the SAS Connectivity Modules do not have an active zone.

Hardware and Status Information

The hardware that was discovered in the chassis and status is shown below. In order to properly configure the chassis, all should have a normal status. If any status shows an error or you do not see hardware listed here that you have put into the chassis, then you should fix those problems before continuing with this wizard.

System Status Summary

Warnings and System Events

- [\(03/07/13 05:43:16\) I/O Module 3 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.](#)

At-a-glance System and Component Status Summary

Bay	Description	Status
<i>Blades</i>		
1	HS22_Blade_1	
2	SN#Y010UF18E0B9	
3	ADXblade1	
4	Blade13-HS22	
5	ADXblade2	
6	SN#Y111UN234018	
<i>I/O Modules</i>		
1	Ethernet SM	
3	SAS Conn Mod	
4	SAS Conn Mod	
<i>Management Modules</i>		
1	bcamm6	
<i>Power Modules</i>		

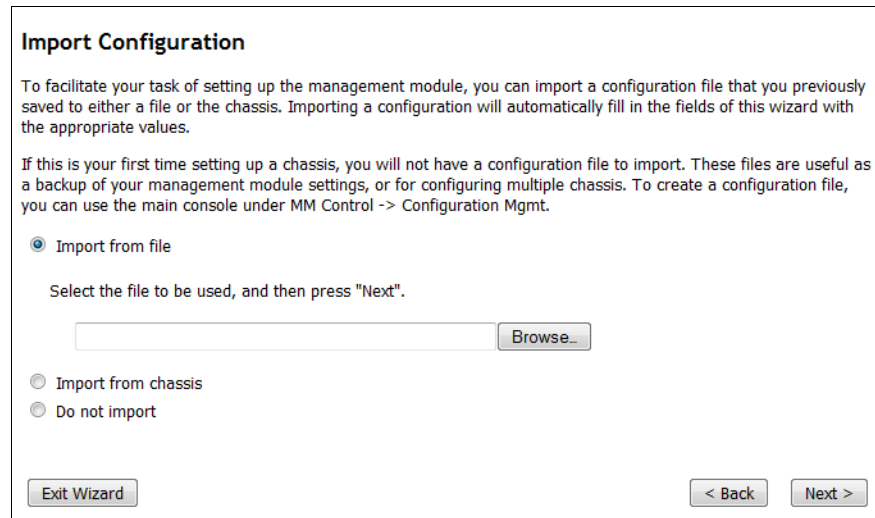
Exit Wizard

< Back

Next >

Figure 3-28 Step 3 of the AMM Express Configuration Wizard

4. The Import Configuration window (Figure 3-29) allows you to import the configuration of the AMM from the chassis, a file, or not at all. Selecting **Import from File** allows you to browse a remote location for a saved configuration. The default name of a saved file is asm.cfg.



Import Configuration

To facilitate your task of setting up the management module, you can import a configuration file that you previously saved to either a file or the chassis. Importing a configuration will automatically fill in the fields of this wizard with the appropriate values.

If this is your first time setting up a chassis, you will not have a configuration file to import. These files are useful as a backup of your management module settings, or for configuring multiple chassis. To create a configuration file, you can use the main console under MM Control -> Configuration Mgmt.

☒ Import from file

Select the file to be used, and then press "Next".

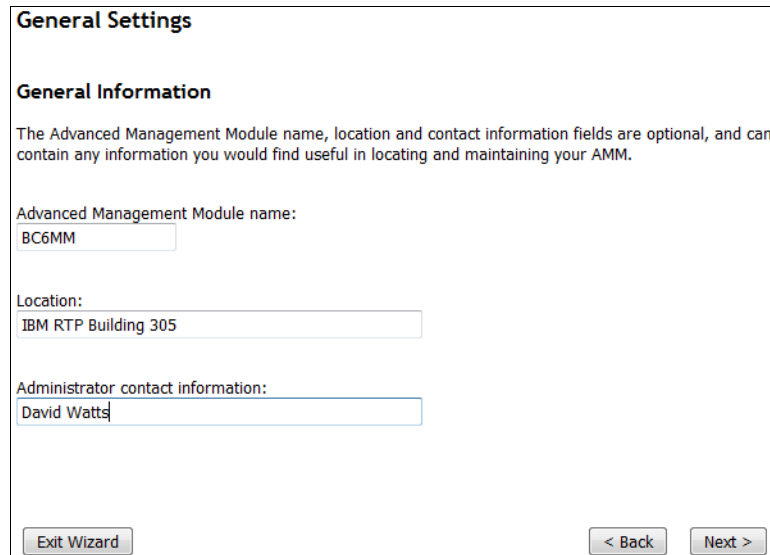
☐ Import from chassis

☐ Do not import

Figure 3-29 Import Configuration window

5. The General Settings window (Figure 3-30) asks for the AMM name, location, and contact information. Input from these fields is intended for administrative purposes only, and is not used by the management module for host name or alert notification. If you manage multiple BladeCenter chassis, the information that is entered on this window can be useful for future reference.

Enter a reference name for the AMM (typically, the same as the host name), the specific location of the BladeCenter S chassis, and the administrator contact information. Click **Next** to continue.



General Settings

General Information

The Advanced Management Module name, location and contact information fields are optional, and can contain any information you would find useful in locating and maintaining your AMM.

Advanced Management Module name:

Location:

Administrator contact information:

Figure 3-30 General Settings window

6. On the AMM Network Interface window (Figure 3-31), enter the host name and IP address information for the management module.

The screenshot shows a web-based configuration window titled "AMM Network Interface". Below the title is a sub-header "AMM Network Interface (eth0)". A descriptive text states: "This is the interface the Advanced Management Module uses to connect to your management network." The "Interface status" is set to "Enabled". The "Hostname" field contains "BC6MM". The "DHCP" dropdown menu is set to "Disabled - Use static IP configuration". A note explains: "To manually configure the IP settings, choose 'Disabled'. To obtain an IP address from a DHCP server, choose 'try DHCP server.' In the event that the server cannot be reached, the system will failover to the static IP you enter below." The "Static IP Configuration" section includes fields for "IP address (default is 192.168.70.125):" with value "9.42.171.1", "Subnet mask (default is 255.255.255.0):" with value "255.255.254.0", and "Gateway address:" with value "9.42.170.1". A bold note at the bottom states: "Note: Changes to network settings will take effect after the next restart of the AMM." At the bottom of the window are three buttons: "Exit Wizard", "< Back", and "Next >".

Figure 3-31 AMM Network Interface window

The host name field on this window is what is registered with DNS after the AMM is rebooted. For networking setup, generally use a static IP assignment for the management module. Click **DHCP** → **Disabled - Use Static IP Configuration**. Then, enter the network settings to be used in the Static IP Configuration section.

7. Be sure to double-check the IP address information because these settings are the active settings when the AMM reboots. If you configure the management module remotely, be sure that you can access the subnet for the IP address for which you are setting up the module. Potentially, you might assign an IP address of a network subnet that you cannot access. If this happens, the management module can become inaccessible for further remote configuration.

Important: Changes to the AMM network configuration are only activated after the module reboots. When you change the management module, you can undo or change settings until you restart the AMM.

8. Review the static IP configuration settings, and then click **Next**.
9. The I/O Module Configuration window (Figure 3-32) is designed to gather network setting information for the I/O Expansion Modules that are installed in the BladeCenter S chassis. The network settings that are specified on this window are for the individual administrative access interfaces of the modules.

I/O Module Configuration

The following I/O modules (e.g., switches, pass-through modules) were found in this chassis. Please specify the network configuration information for the components below.

☒ All I/O Modules use the same subnet mask:

☒ All I/O Modules use the same gateway:

Bay	Description	Static IP Address	Enable External Ports	Enable External Control on Ports	Preserve IP Address on Reset
1	Ethernet SM	<input type="text" value="9.42.171.89"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	SAS Conn Mod	<input type="text" value="9.42.171.67"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	SAS Conn Mod	<input type="text" value="9.42.171.68"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 3-32 I/O Module Configuration for SAS Connectivity Module

The administrative interfaces, typically web-based or Telnet-based, of most I/O Expansion Modules offer detailed information about the performance of their module and extra configuration capabilities. Configuring the modules through their administration interface is optional, and is not required for normal operation.

10. If all I/O modules use the same subnet and gateway (preferred), select the two option boxes and then enter the IP address information for each module. If you want the external ports automatically enabled on the restart of the AMM, select **Enable External Ports** for each module. If this option is not selected, the external ports/uplinks on the Ethernet switch and the SAS module will not be functional after the management module restarts.

If all I/O modules will not use the same subnet and gateway, click to clear the two option boxes. Then, enter the additional network settings in the fields next to the module's IP address.

11. Leave **Enable External Control on Ports** cleared. Enable external control only if you have the I/O modules and the advanced management module on separate subnets or VLANs.
12. If you want the user-defined IP configuration settings to be preserved when the module's factory defaults are restored, or when a reset is initiated by a source other than the management module, select **Preserve IP Address on Reset**. If you do not, the factory default IP configuration settings become active when the I/O module factory defaults are restored, or when an I/O module reset is initiated by a source other than the management module.
13. After you enter the network settings and select the management options, click **Next**. You can modify I/O module information further after the initial AMM configuration is complete.

If you are using the advanced management module to configure a BladeCenter S chassis that has the SAS RAID Controller Module, you must configure two IP addresses for each controller: One for the SAS Switch and another for the RAID Controller, as shown in Figure 3-33.

I/O Module Configuration

The following I/O modules (e.g., switches, pass-through modules) were found in this chassis. Please specify the network configuration information for the

☒ All I/O Modules use the same subnet mask:

255.255.255.0

☒ All I/O Modules use the same gateway:

9.42.171.1

Bay	Description	Static IP Address	Enable External Ports	Enable External Control on Ports
1	Ethernet SM	9.42.171.89	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	SAS RAID Ctrl Mod		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SAS SW	9.42.171.67		
	RAID Ctrl	9.42.171.68		
4	SAS RAID Ctrl Mod		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SAS SW	9.42.171.37		
	RAID Ctrl	9.42.171.38		

Exit Wizard

Figure 3-33 I/O Module Configuration for SAS RAID Controller Module

14. On the Login Profile window (Figure 3-34), you can change the user ID and password of the AMM default login account. Change at least the password of the default USERID account. More accounts can be created after the initial AMM configuration is complete.

Login Profile

Default Profile

This is the default user ID. You can change both the user ID and the password here. It is **highly** recommended that you change at least the password.

Administrative (read/write access) Login ID (default is USERID):

USERID

New Password:

••••••••

Confirm New Password:

••••••••

Note: You can enter additional profiles and enable LDAP verification from the main Advanced Management Module UI after completing this wizard.

Exit Wizard < Back Next

Figure 3-34 Step 7 of the AMM Express Configuration Wizard

Important: The default user name and password for the AMM (USERID and PASSWORD) have been used for years. They are well known by anyone who has worked with BladeCenter or System x servers before. Change the user name and password to prevent unauthorized access to the management module.

15. After you change the login information, click **Next**.

16. If you want to enable SSL or SSH communication protocols (Figure 3-35), select **Enabled** for both protocols, select **Generate and install a new self-signed certificate**, and then click **Next**.

Security

The Advanced Management Module supports secure communication protocols for both its Web Interface, via secure socket layer (SSL) and its Command Line Interface, via secure shell (SSH). SSL protocol ensures secure transactions between web servers (the AMM) and browsers (your computer).

Secure Socket Layer (SSL)

SSL server: Enabled ▾

A certificate is already installed.

☐ Generate and install a new self-signed certificate. If you wish to use a third-party certificate, you may do so through the main user interface.

Secure Shell (SSH)

Secure Shell (SSH) is a protocol for remotely logging into a machine via a shell. It is very similar in functionality to telnet, however unlike telnet, all data between the server (the AMM) and client (your computer) is encrypted.

SSH server: Enabled ▾

Below is encryption information about your SSH Host Key

SSH host key status: SSH Host Key Present

1024-bit DSA, Fingerprint e7:8b:13:23:3b:d4:b4:4b:f4:c9:a3:a4:88:4f:5e:c6

2048-bit RSA, Fingerprint 58:0a:e4:f5:e2:46:6a:ad:db:c2:fd:13:17:e7:ab:27

Exit Wizard < Back Next >

Figure 3-35 Custom path Security window

17. If you elected to enable SSL and SSH protocols, the SSL Server Self-signed Certificate window is displayed as shown in Figure 3-36. Complete the required information, and if you want, complete the optional data fields that appear in the certificate. The email address that you provide in this section is not used for alert notification.



The image shows a window titled "SSL Server Self-signed Certificate". It contains two sections: "Required Certificate Data" and "Optional Certificate Data". Each section has several text input fields. At the bottom, there are three buttons: "Exit Wizard", "< Back", and "Next >".

Required Certificate Data	
Country (2 letter code)	US
State or Province	NC
City or Locality	Raleigh
Organization Name	IBM
MM Hostname	BC6MM

Optional Certificate Data	
Contact Person	John Smith
Email Address	js@example.com
Organizational Unit	IT Support
Surname	Smith
Given Name	John
Initials	US
DN Qualifier	
Years Valid	20

Exit Wizard < Back Next >

Figure 3-36 SSL Server Self-signed Certificate window

18. The certificate is presented to your web browser or SSH application when you log in to the AMM after the first restart. Verify the information on this window, then click **Next**.
19. On the Domain Name Server window (Figure 3-37), select whether the DNS for the AMM must be enabled or disabled. If you want to enable it, enter the IP address of the DNS in your environment and click **Next**.

Note: If you do not enable DNS, you must specify IP addresses for any other protocols you want to enable such as SMTP, SNMP, and NTP.

Domain Name Server

Domain Name Server

If you have a dynamic host configuration protocol (DHCP) server on your network, the field(s) below may be populated with the IP addresses of the domain name servers (DNS) on your network. If your network does not have a DHCP server, and you wish to enable DNS, you will need to enter the IP address of at least one DNS.

DNS

Enabled

DNS IP 1

168.244.1.3

DNS IP 2

168.244.1.4

DNS IP 3

168.244.1.5

Exit Wizard

< Back

Next >

Figure 3-37 Domain Name Server window

20. In the Event Notifications window (Figure 3-38), indicate the events that the AMM monitors and broadcasts to recipients. Select Informational, Warning, or Critical alerts, which have the following functions:

- Informational alerts are mostly event logs of user activity, AMM and blade restarts, and configuration changes.
- Warnings include temperature alerts, I/O module and storage events, and firmware flash failures that do not necessarily need intervention.
- Critical alerts include module failures, power faults, blade and AMM communication failures, and other chassis impacting outages that usually need user interaction.

Event Notifications

BladeCenter can notify you of various events including hardware errors and temperature problems. Below, indicate the events that the AMM should monitor and broadcast to recipients.

☒ Informational Alerts

☒ Warning Alerts

☒ Critical Alerts

Use the section below to configure the first event recipient for email notification. If this is the first time you are configuring the Advanced Management Module (AMM), you will not see any information entered below. However, if you have previously configured the first event recipient in the AMM to use a notification method other than e-mail (e.g., SNMP), this wizard will reconfigure the recipient to use e-mail notification instead.

☒ Configure an e-mail recipient

Recipient Name
John Smith

E-mail address
js@example.com

SMTP server fully qualified hostname or IP address
mailserver.example.com

Exit Wizard < Back Next >

Figure 3-38 Event Notifications window

21. Select **Configure an e-mail recipient** and enter the recipient information if you want to configure alerts to be sent through email.

Tip: If using email event notification, be sure to conduct a test event to ensure that the email and SMTP address are entered correctly. Conduct this test through the **Alerts** menu of the AMM.

22. In the Date and Time window of the wizard (Figure 3-39), enter the date and time. Select the appropriate GMT offset based on the location of the BladeCenter S, or select the option to enable NTP. The accuracy of this information is important when you review the event logs of the AMM.

After you set the date and time or configure NTP, click **Next**.

Date and Time

Setting the accurate date and time is important so that the events that occur are time stamped appropriately

☒ Use Network Time Protocol (NTP) to set the date and time

NTP server fully qualified hostname or IP address: 9.42.170.1

NTP update frequency (minutes): 3600

☒ Use NTPv3 Authentication

Key index: 5

Key type: M - MD5

Key: ••••••••

GMT Offset: -5:00 - Eastern Standard Time (Eastern USA, Ontario, Quebec) ▼

☒ Automatically adjust for daylight saving changes

Exit Wizard < Back Next >

Figure 3-39 Configuring NTP

23. If you selected **Automatically adjust for daylight saving changes**, you are asked to select an available daylight saving time scheme, as shown in Figure 3-40. Select the appropriate scheme based on your location and click **Next**.



Observe Daylight Saving Time

Unable to automatically determine the daylight saving time to use.
Please provide the DST scheme:

Selected GMT offset: -5:00

Available schemes: USA and Canada ▼

Exit Wizard < Back Next >

Figure 3-40 Daylight saving time

24. Configure SNMP hosts for gathering information about the chassis and delivering alerts to a remote server as shown in Figure 3-41. Enter the Community name, the type of access, and the host name or IP addresses for the SNMP server. For added security, you can also configure SNMPv3. Click **Next** to continue.

SNMP

SNMP is a set of protocols used for managing complex networks. It is used for retrieving information about your Advanced Management Module, changing settings, and receiving alerts about the current state of your MM and other BladeCenter chassis components.

SNMPv3 offers better security features than SNMPv1.

Simple Network Management Protocol version 1 (SNMPv1)

SNMPv1 agent: Enabled ▾

SNMPv1 Communities

Community name	Access type	Fully qualified hostnames / IP Addresses
<input type="text" value="public"/>	Get ▾	1. <input type="text" value="9.42.170.1"/> 2. <input type="text" value="0::0"/> 3. <input type="text"/>
<input type="text"/>	Get ▾	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
<input type="text"/>	Get ▾	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>

Simple Network Management Protocol version 3 (SNMPv3)

SNMPv3 agent: Disabled ▾

Exit Wizard< BackNext >

Figure 3-41 SNMP window

25. Select a storage configuration. You can select one of the predefined configurations by clicking the name of the configuration to see a visual representation of the disk allocation as shown in Figure 3-42. Then, click **Activate Selected Configuration**, which is shown at the bottom of the window.

Click **Next** to continue.

Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date
<input type="radio"/>	✓	Predefined Config 02	Pre-defined	6	2	1	6	04/24/2002:00:00
<input type="radio"/>		Predefined Config 03	Pre-defined	6	1	2	7	04/24/2002:00:00
<input type="radio"/>		Predefined Config 04	Pre-defined	1	2	6	8	04/24/2002:00:00
<input type="radio"/>		Predefined Config 05	Pre-defined	1	1	12	9	04/24/2002:00:00
<input type="radio"/>		Predefined Config 06	Pre-defined	3	2	2	10	04/24/2002:00:00
<input type="radio"/>		Predefined Config 07	Pre-defined	3	1	4	11	04/24/2002:00:00
<input type="radio"/>		Predefined Config 08	Pre-defined	2	2	3	12	04/24/2002:00:00
<input type="radio"/>		Predefined Config 09	Pre-defined	2	1	6	13	04/24/2002:00:00
Select	Active?	Name	Type	Description			Configuration Store	Date
<input type="radio"/>		User Defined Config 01	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.			1	00/00/0000:00:00
<input type="radio"/>		User Defined Config 02	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.			2	00/00/0000:00:00
<input type="radio"/>		User Defined Config 03	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.			3	00/00/0000:00:00
<input type="radio"/>		User Defined Config 04	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.			4	00/00/0000:00:00

Exit Wizard

Figure 3-42 Storage configuration

26. Figure 3-43 shows the details of a configuration that you see when you click the name of that configuration in Figure 3-42 on page 142.

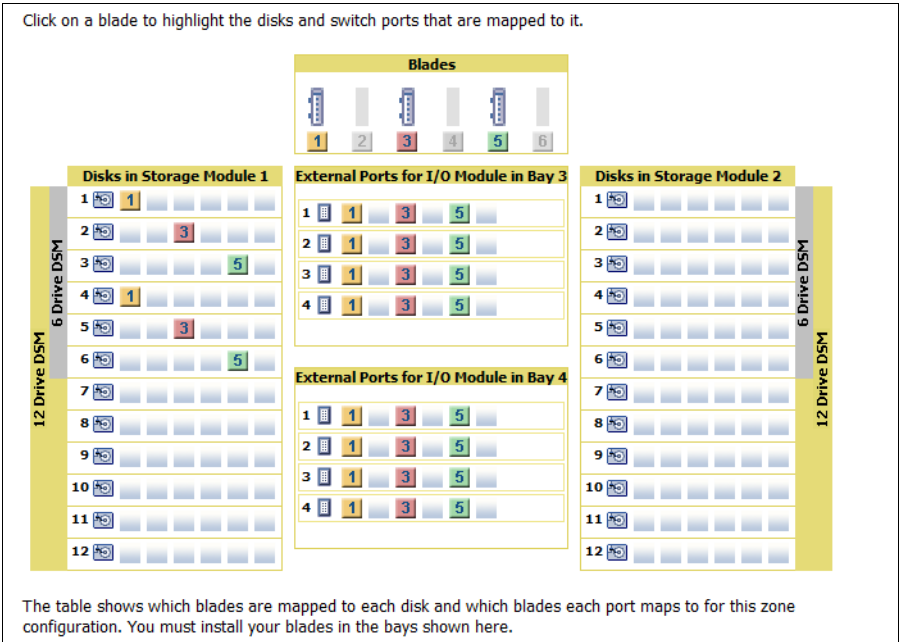


Figure 3-43 Visual representation of a configuration

27. If you are using the advanced management module to configure a BladeCenter S chassis with SAS RAID Controller Modules installed, you see only Predefined Configuration 10 as shown in Figure 3-44.

I/O Module 3 (SAS RAID Ctrl Mod) ?									
The table below lists zone configurations that is most appropriate for my current number of blades and SAS I/O Modules.									
Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date	
<input checked="" type="radio"/>	✓	Predefined Config 10	Pre-defined	6	2	12	14	04/24/2002:00:00	

I/O Module 4 (SAS RAID Ctrl Mod) ?									
The table below lists zone configurations that is most appropriate for my current number of blades and SAS I/O Modules.									
Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date	
<input checked="" type="radio"/>	✓	Predefined Config 10	Pre-defined	6	2	12	14	04/24/2002:00:00	

Figure 3-44 Configuration choices for SAS RAID Controller Module

Predefined Storage Configuration 10 for the SAS RAID Controller Module is designed so that all six blade servers have access to both SAS RAID Controller Modules in the chassis. The configuration consists of storage that is mapped to all six blade servers, two SAS RAID Controller Modules, and two fully populated disk storage modules.

Each blade server can access *all* hard disk drives in *all* disk storage module and all external ports on the SAS module, as shown in Figure 3-45.

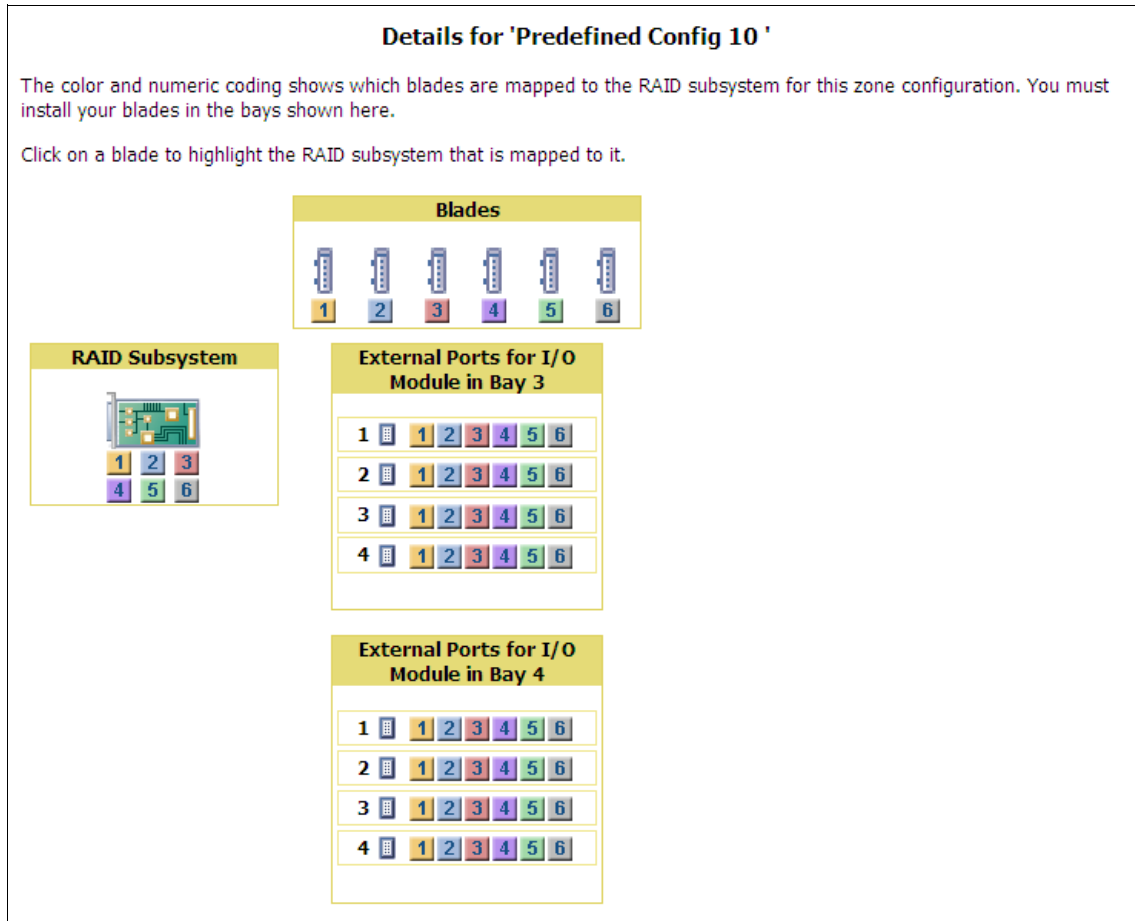


Figure 3-45 Visual representation for Predefined Configuration 10

Use Storage Configuration Manager: The SAS Connectivity Module uses the LSI Configuration Utility in each blade server to create arrays and establish RAID support for the assigned storage. However, to configure RAID levels and hot-spare disks in the SAS RAID Controller Module, you must access the controller web interface or use Storage Configuration Manager.

Click **Next** to continue.

28. After you complete the storage configuration for the BladeCenter S, you are presented with the Server Advisor Settings window shown in Figure 3-46. You can configure the AMM to monitor your chassis for hardware events and capture the error logs and service data. It then automatically reports the event to IBM.

Service Advisor Settings

Service Advisor resides on your Advanced Management Module (AMM) and monitors your BladeCenter Chassis for hardware events. Upon detecting a hardware event, Service Advisor captures the event, error logs, and service data, and can automatically report the event to IBM support. To send the serviceable event to IBM support, you must enable and configure Service Advisor. For each serviceable call home event IBM receives, a service ticket will be opened, and a follow-up call will be made.

☒ Enable IBM Support

Service Advisor Settings

IBM Service Support Center (Mandatory)

Enter the country code for the IBM Service Support Center. Please choose the appropriate center to satisfy your needs. A proper support center will make the handling of your Call Home request operate smoothly and easily.

IBM Support Center

US - United States

Contact Information (Mandatory)

Please make sure all the fields in this section are input correctly. These configurations are necessary for Service Advisor and only valid configurations can allow Service Advisor to be enabled.

Company Name	IBM
Contact Name	John Smith
Phone	919-555-1212
Email	js@example.com
Address	3 IBM Way
City	Raleigh
State	NC
Postal code	27017

Exit Wizard

< Back

Next >

Figure 3-46 Service Advisor Settings window

29. After you configure the Service Advisor settings, the Wizard Configuration Summary window shown in Figure 3-47 is displayed. Review all information on this window. If any changes must be made, use the **Back** option to revisit the appropriate configuration wizard section. If all settings are correct, click **Save All Settings**.

You have completed entry of all the information necessary to get your chassis running and communicating with your network. Press "Save All Settings" to commit changes.

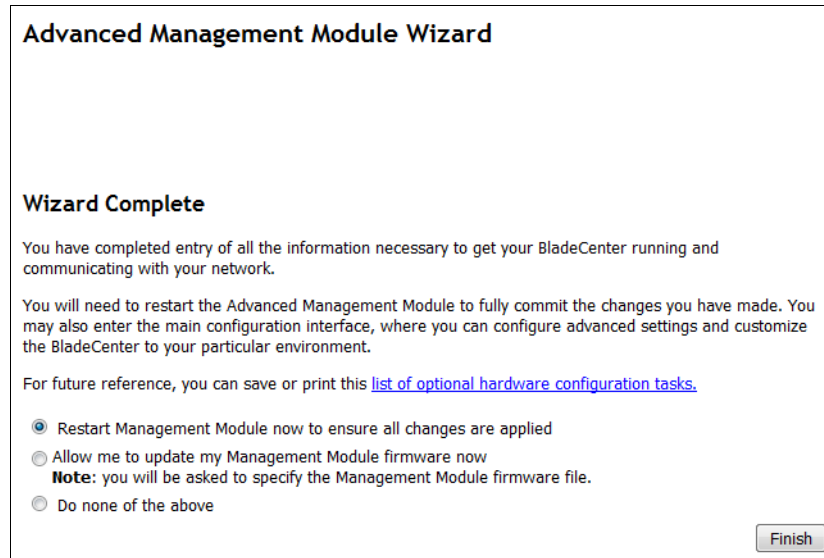
Wizard Configuration Summary

General Settings	
AMM Name:	bcamm6
Location:	RTP, NC
Administrator Contact:	ITSO
AMM Network Interface	
Hostname:	bcamm6
DHCP:	Disabled - Use static IP configuration
Static IP Configuration	
IP address:	9.42.171.1
Subnet mask:	255.255.254.0
Gateway address:	9.42.170.1
I/O Module Configuration	
Bay 1	
Static IP address:	9.42.171.89
Subnet mask:	255.255.255.0
Gateway address:	9.42.171.1
External ports:	Enabled
External control on ports:	Enabled
Preserve IP address on reset:	Enabled
Bay 3	
Static IP address:	9.42.171.67
Subnet mask:	255.255.255.0
Gateway address:	9.42.171.1
External ports:	Enabled
External control on ports:	Enabled
Preserve IP address on reset:	Enabled
Bay 4	
Static IP address:	9.42.171.68

Figure 3-47 Summary and confirmation of the AMM Express Configuration Wizard

30. The Custom path for the AMM Configuration Wizard is now complete. You are offered the option to reboot the management module, apply firmware, or do nothing. You must restart the AMM to commit and activate the settings that you entered in the wizard. Select **Restart Management Module now to ensure all changes applied** and click **Finish** (Figure 3-48).

Tip: Restarting the AMM does not affect the operation of the blade servers or the disk storage modules. The fans spin up to 100% for several seconds but then return to normal speeds (and sound volume).

The screenshot shows a web-based wizard titled "Advanced Management Module Wizard". Below the title, it says "Wizard Complete". The text explains that the user has completed the configuration and needs to restart the module. It provides a link to "list of optional hardware configuration tasks". There are three radio button options: "Restart Management Module now to ensure all changes are applied" (which is selected), "Allow me to update my Management Module firmware now" (with a note that the user will be asked to specify the firmware file), and "Do none of the above". A "Finish" button is located in the bottom right corner.

Advanced Management Module Wizard

Wizard Complete

You have completed entry of all the information necessary to get your BladeCenter running and communicating with your network.

You will need to restart the Advanced Management Module to fully commit the changes you have made. You may also enter the main configuration interface, where you can configure advanced settings and customize the BladeCenter to your particular environment.

For future reference, you can save or print this [list of optional hardware configuration tasks](#).

☒ Restart Management Module now to ensure all changes are applied

☐ Allow me to update my Management Module firmware now
Note: you will be asked to specify the Management Module firmware file.

☐ Do none of the above

Finish

Figure 3-48 Completion of the AMM Express Configuration Wizard

31. Upon clicking **Finish**, the AMM activates all changes made throughout the configuration wizard and reboots. Your session to the AMM is ended and the browser window prompts you to start a new session.

After the AMM finishes rebooting, it is accessible by using its new IP address. If you want to configure the management module further, log in to the new address and enter the revised user ID and password that you specified in the wizard.

Tip: To track the progress of an AMM reboot, ping its new IP address by using the **ping -t** option. This begins a continuous ICMP probe of the management module every second.

When you see replies being returned from the address of the AMM, you can log in.

3.3 ServerGuide Scripting Toolkit

The IBM ServerGuide Scripting Toolkit is a collection of system configuration tools and installation scripts. You can use to deploy your IBM System x or BladeCenter server in a repeatable, predictable manner. When used with IBM ServerGuide and IBM UpdateXpress, the ServerGuide Scripting Toolkit provides a total solution for deploying IBM System x or BladeCenter servers in an unattended mode.

This toolkit provides for automation of large server rollouts with substantial customer control and customization. It also provides a mechanism to integrate deployment of IBM System x and BladeCenter systems into your existing deployment processes.

The ServerGuide Scripting Toolkit supports deployment by using the following applications and devices:

- ▶ Altiris Deployment Solution for Windows and Linux
- ▶ Microsoft Automated Deployment Services (ADS)
- ▶ Create a bootable Windows PE CD or DVD
- ▶ DOS bootable diskette and network share or data CD
- ▶ DOS bootable CD
- ▶ BladeCenter and Remote Supervisor Adapter II virtual diskette and network share

3.3.1 Key features

You can use the ServerGuide Scripting Toolkit to run the following tasks automatically:

- ▶ Detect hardware
- ▶ Configure RAID adapters
- ▶ Delete any existing partitions and data from the drives of the target server

- ▶ Create a primary operating-system installation partition on the first drive of the target server
- ▶ Format the new partition as FAT32
- ▶ Install an operating system
- ▶ Install device drivers (Windows only)
- ▶ RSA II and BladeCenter MM/AMM remote disk scenarios
- ▶ UpdateXpress System Packs installation that is integrated with scripted NOS deployment
- ▶ IBM Director Agent installation that is integrated with scripted NOS deployment
- ▶ Dispose of servers by securely removing data

In addition, the ServerGuide Scripting Toolkit saves persistent-state information across system restarts so that it can monitor the deployment process.

3.3.2 Operating system support

The ServerGuide Scripting Toolkit offers Windows and Linux based support on x86-based blades, including the following operating systems:

- ▶ SUSE Linux Enterprise Server 9 32 bit SP4
- ▶ SUSE Linux Enterprise Server 9 x64 SP4
- ▶ SUSE Linux Enterprise Server 10 32 bit SP1-SP4
- ▶ SUSE Linux Enterprise Server 10 x64 SP1-SP4
- ▶ SUSE Linux Enterprise Server 11 32 bit Base, SP1, SP2
- ▶ SUSE Linux Enterprise Server 11 x64 Base, SP1, SP2
- ▶ Red Hat Enterprise Linux 4 AS and ES 32 bit U6-U8
- ▶ Red Hat Enterprise Linux 4 AS and ES x64 U6-U8
- ▶ Red Hat Enterprise Linux 5 32 bit U1-U8
- ▶ Red Hat Enterprise Linux 5 x64 U1-U8
- ▶ Red Hat Enterprise Linux 6 32 bit U1-U3
- ▶ Red Hat Enterprise Linux 6 x64 U1-U3
- ▶ VMware ESX Server 3.5 U4/U5
- ▶ VMware ESX Server 4.0, 4.0 U1, 4.0 U2
- ▶ VMware ESX Server 4.1, 4.1 U1, 4.1 U2, 4.1 U3
- ▶ Microsoft Windows Server 2003, Standard, Enterprise, and Web Editions

- ▶ Microsoft Windows Server 2003 R2, Standard and Enterprise Editions
- ▶ Microsoft Windows Server 2003, Standard and Enterprise x64 Editions
- ▶ Microsoft Windows Server 2003 R2, Standard and Enterprise x64 Editions
- ▶ Microsoft Windows Server 2008, Standard, Enterprise, Datacenter, and Web Editions
- ▶ Microsoft Windows Server 2008 x64, Standard, Enterprise, Datacenter, and Web Editions
- ▶ Microsoft Windows Server 2008, Standard, Enterprise, and Datacenter Editions without Hyper-V
- ▶ Microsoft Windows Server 2008 x64, Standard, Enterprise, and Datacenter Editions without Hyper-V
- ▶ Microsoft Windows Server 2008 R2 x64, Standard, Enterprise, Datacenter, and Web Editions
- ▶ Microsoft Windows Server 2012

For detailed instructions, downloads, requirements, features, installation, management, and support for the ServerGuide Scripting Toolkit, see the following links:

- ▶ IBM ServerGuide Overview, Documents, and Downloads:
<http://www-03.ibm.com/systems/be/management/sgstk/>
- ▶ IBM ServerGuide Scripting Toolkit, Windows Edition: User's Guide:
http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/userguide_wtk930.pdf
- ▶ IBM ServerGuide Scripting Toolkit, Linux Edition: User's Guide:
http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/userguide_ltk930.pdf

3.4 Using the command-line interfaces

In addition to the other tools described in this chapter, the Advanced Management Module, SAS Connectivity Module, and SAS RAID Controller Module offer powerful command-line interfaces. These CLIs can be used to configure, gather information about, and support your BladeCenter environment.

This book covers the CLIs in the following sections:

- ▶ Advanced management module: 5.2, “Command-line interface” on page 318
- ▶ SAS RAID Controller Module: 4.8, “Configuring the SAS RAID Controller Module using the CLI” on page 265
- ▶ SAS Connectivity Module: 4.9, “Configuring the SAS Connectivity Module using CLI” on page 269

3.5 IBM Fabric Manager

IBM Fabric Manager allows address virtualization, server pre-provisioning, and automatic failover of compute nodes to enable speed of deployment and high availability through dynamic provisioning of IT resources in a production environment. This application replaces both BladeCenter Open Fabric Manager Basic and Advanced applications, combining them into a single package.

Fabric Manager includes the following features:

- ▶ High availability with redundant Fabric Manager servers
- ▶ Option to run Fabric Manager server as a service
- ▶ Protection with unique addresses for newly defined profile
- ▶ Remote console
- ▶ Profile-based user interface
- ▶ Combination of both BladeCenter Open Fabric Manager Basic and Advanced applications in one easy-to-use package.

BladeCenter Open Fabric Manager: IBM Fabric Manager replaces BladeCenter Open Fabric Manager (BOFM). The functions of IBM Fabric Manager are the same as the combination of BOFM Basic and BOFM Advanced.

3.5.1 Overview

Fabric Manager is designed to easily manage I/O and network interconnects by virtualizing network parameters such as the worldwide name (WWN) and MAC addresses. When a compute node is replaced or failover occurs from one compute node to another, the LAN and SAN configurations are not affected.

After Fabric Manager is installed, you can preconfigure LAN and SAN connections. I/O connections are made automatically when compute nodes are

plugged into the chassis slots. No special tools or training are required. You just manage the program with an easy-to-use web-based user interface.

Fabric Manager offers these benefits:

- ▶ Save time: Preconfigure more than 1,400 LAN and SAN connections once for each blade server.
- ▶ Simplified management: Manage growth and complexity from a single Fabric Manager user interface.
- ▶ Flexibility: Fabric Manager works with Ethernet, Fibre Channel, and SAS switch modules.
- ▶ Ease of use: Profile-based user interface enables easy setup, deployment, and management.
- ▶ Reduced risk: Manage risk to keep business operations running with available I/O failover to standby compute nodes and redundant Fabric Manager servers.
- ▶ New Enterprise Licensing offering provides time-saving benefits in deploying multiple chassis.

3.5.2 Licensing

Features can be used on your chassis after you install a valid license key for the feature.

Use the following link to obtain license keys that enable features for your chassis. Install license keys that you get from this website on your chassis AMM to unlock and use the features.

<http://licensing.datacentertech.net>

Two types of keys are available:

- ▶ 60 Day Trial: This license type allows you to use the feature for sixty days. The trial starts when you install the sixty day trial license key on the AMM. The machine type or model and serial number of the chassis where you want to use the feature.
- ▶ Permanent: This is the standard license type for features that you purchase. A permanent license never expires. To obtain a permanent license key, provide the authorization code (or activation code) that was provided to you when you purchased the feature, and the machine type / model and serial number of the chassis where you want to use the feature.

Table 3-1 lists the part numbers for single chassis entitlement for the type of chassis with the Subscription and Support (maintenance) term listed.

Table 3-1 Ordering part numbers for IBM Fabric Manager

Description	Part number	
	EMEA and LA	US, Canada, AP, and Japan
IBM Fabric Manager for BladeCenter Per Managed Chassis with 1 Year SW S&S	00Y6198	00Y6192
IBM Fabric Manager for BladeCenter Per Managed Chassis with 3 Year SW S&S	00Y6199	00Y6193
IBM Fabric Manager for BCS Per Managed Chassis with 1 Year SW S&S	00Y6200	00Y6194
IBM Fabric Manager for BCS Per Managed Chassis with 3 Year SW S&S	00Y6201	00Y6195
IBM Fabric Manager for BladeCenter Upgrade from BOFM Per Managed Chassis with 1 Year SW S&S	00Y6202	00Y6196
IBM Fabric Manager for BCS Upgrade from BOFM Per Managed Chassis with 1 Year SW S&S	00Y6203	00Y6197

3.5.3 Enabling Fabric Manager

After you obtain your license, there are two ways to apply it:

- Using the AMM web interface: Click **Blade Tasks** → **Open Fabric Manager**. Then enter the seven digit unique key for your chassis as shown in Figure 3-49.

Bay 1: SN#YK1680856157

- Monitors
 - System Status
 - Event Log
 - LEDs
 - Power Management
 - Hardware VPD
 - Firmware VPD
 - Remote Chassis
- Blade Tasks
 - Power/Restart
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN
 - Open Fabric Manager**
- I/O Module Tasks

Enter License Information ?

Enter the new key and "Submit".

Feature	Status	License Key
IBM BladeCenter Open Fabric Manager ?	No License	<input type="text" value="hggfeb4"/>

License Keys are unique for each chassis. Only License Keys that are issued for Machine Type / Model 88861MU Serial Number 1003E1A are valid for this chassis.

Wed, 13 Mar 2013 19:33:31

Figure 3-49 License Information window

- Using the command-line interface: The **feature** command allows you to add, remove, and display the status of licensed features as shown in Example 3-1.

Example 3-1 Applying a Fabric Manager license from the command line

```
system> env -T mm[1]
OK
system:mm[1]> feature ?
feature {-[index] {-remove}|-add -key}}|-apply}|-retrieve {-filter}}
Add/Remove/Display Status of licensed features
-remove:  removes the license for the specified index
-add:     add a license: requires -key
-key:     license key of the feature ordered (7 characters)
-apply:   remote location of the license file to apply. Must specify the
          filename.
-retrieve: remote location to save the license file. Must specify the filename.
-filter:  remote location of the AMM IP filter file, used when retrieving the
          license file.

Note: For -apply, -retrieve, and -filter use one of the following protocols:
tftp, ftp, ftps, http, or https to specify the remote location. An example of a
qualified location can be: tftp://192.168.0.1/license.csv
system:mm[1]> feature -1 -add -key hggfeb4
```



```
License Status: Active
system:mm[1]> feature
1. IBM BladeCenter-S Open Fabric Manager
   -serial 1003E1A
   -key hggfeb4
License Status: Active
2. IBM BladeCenter Advanced Open Fabric Manager
License Status: No License
3. IBM BladeCenter Advanced Open Fabric Manager Plug-in
License Status: No License
4. <no license description>
```

3.5.4 Opening Fabric Manager components

The Fabric Manager configuration file and AMM web interface are essential for Fabric Manager functions.

The Fabric Manager configuration file is the central tool for managing the Fabric Manager domain. It contains the definitions that you need for a domain of up to 100 BladeCenter chassis or 1400 blade servers. You can generate it automatically, save it, and edit it to conform to the needs of a specific domain, and then apply it to the domain. You also have the option of creating your own configuration file.

The configuration file is a comma-separated value (CSV) file. Each non-blank and non-comment line defines a single entity within a domain of BladeCenter chassis. The entities defined are chassis, slots (that is, blade server bays), and ports (that is, ports on network cards). There is one for each interface type.

The file is organized hierarchically by chassis, slots, and ports, with ample comment lines included to act as a guide to editing the file if needed. Generally, maintain the original structure as much as possible to retain the readability of the file. For certain purposes, it might be appropriate to extract a smaller section of the domain into a new file. This allows you to update a particular BladeCenter chassis or a particular blade server individually.

For more information about using the Fabric Manager configuration file, see the *IBM Open Fabric Manager Installation and Users Guide* at:

http://pic.dhe.ibm.com/infocenter/director/v5r2/topic/bofm_1.00/btp0_bofm_users_doc.pdf

3.5.5 Creating a BOFM configuration file

When you use Fabric Manager for the first time, you must create a configuration file in which you assign virtual addresses to each slot in each chassis.

The following example outlines the kind of steps you might follow when creating a configuration file automatically. It does not apply to all BladeCenter environments. These example steps assume that you have a single domain (no addresses are duplicated):

1. Log in to the AMM web interface and select **Open Fabric Manager** in the left pane, under Blade Tasks. The Open Fabric Manager Configuration Management page opens in the right pane as shown in Figure 3-50.

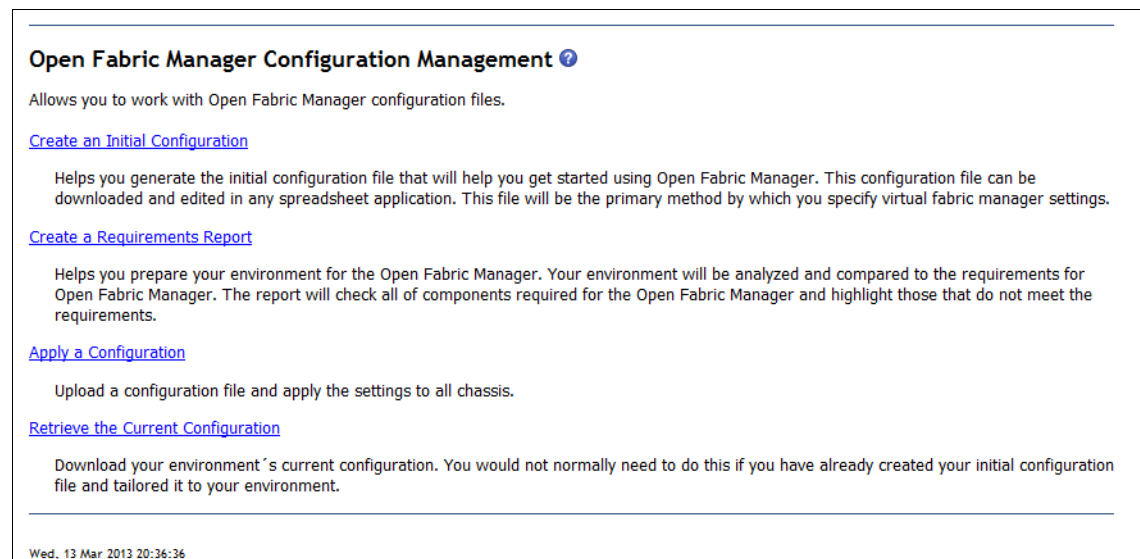


Figure 3-50 Open Fabric Manager Configuration Management window

2. Click **Create an Initial Configuration**. This opens the Specify Virtual Addresses page in the right pane as shown in Figure 3-51.

Specify Virtual Addresses

This allows you to create an initial Open Fabric Manager configuration for all chassis on the network. Virtual addresses can be automatically assigned to blades that are present on the network and support the Open Fabric Manager feature.

Address Type	Vendor	Automatically assign addresses	Port	Addresses Range	
				From	To
Ethernet	User Defined	<input type="checkbox"/>	-	00:00:00:00:01:00	00:00:00:00:01:50
		<input type="checkbox"/>	WWNN A	00:00:00:00:00:00:01	00:00:00:00:00:00:06
FC	User Defined	<input type="checkbox"/>	WWNN B	00:00:00:00:00:00:07	00:00:00:00:00:00:12
		<input type="checkbox"/>	WWPN A	00:00:00:00:00:00:13	00:00:00:00:00:00:18
		<input type="checkbox"/>	WWPN B	00:00:00:00:00:00:19	00:00:00:00:00:00:24
		<input type="checkbox"/>	WWPN	00:00:00:00:00:00:25	00:00:00:00:00:00:30
SAS	User Defined	<input type="checkbox"/>	WWPN	00:00:00:00:00:00:25	00:00:00:00:00:00:30

The following section allows you to configure the Advanced Options for Open Fabric Manager.

Show Advanced Options

Next >Cancel

Figure 3-51 Specify Virtual Addresses window

3. For the Ethernet Address Type, click the menu under Vendor and select **IBM**.

Note: Another option for Vendor is **User Defined**.

4. For the FC Address Type, click the menu under Vendor and select **Emulex** or **QLogic**.
5. For the SAS Address Type, click the menu under Vendor and select **LSI** or **IBM**.

6. Click **Show Advanced Options** and select **Generate an FC target place holder** or **SAS target place holder** as shown in Figure 3-52.

The following section allows you to configure the Advanced Options for Open Fabric Manager.

Hide Advanced options

Enable Ports
This allows you to enable/disable specific port types for each blade offset. When a port type is enabled, all related ports will be active for Open Fabric Manager.

Ethernet	<input checked="" type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>
SAS	<input checked="" type="checkbox"/>
Virtual NIC	<input checked="" type="checkbox"/>

Enable Blade Offsets
This allows you to choose the maximum number of blade offsets for mulit-wide blade scenarios. Each blade offset will inherit the port configuration defined in "Enable Ports".

Enable Offset 0 ▾

Ethernet

MAC Address Step	<input type="text" value="1"/>
Ethernet VLAN	<input type="text" value="0"/>
Generate range of MAC addresses per port	<input type="checkbox"/>

FC

FC WWNN Address Step	<input type="text" value="1"/>
FC WWPN Address Step	<input type="text" value="1"/>
Generate a FC target place holder	<input type="checkbox"/>

SAS

SAS WWPN Address Step	<input type="text" value="1"/>
Generate a SAS target place holder	<input type="checkbox"/>

Next > **Cancel**

Figure 3-52 Configuration management advanced options

7. In the WWN field, enter the storage system WWPN.

Note: You also have the option to specify a value in the LUN field.

- Click **Next** to open the Chassis to include page in the right pane as shown in Figure 3-53.

Chassis to include

Please specify which chassis to include in initial configuration file. You can supply your own text file containing the IP addresses of desired chassis, or if your AMM is connected to a management network along with other chassis, the discovered chassis will automatically be included in configuration file.

Note that when choosing to use the discovered IP addresses option below, you must ensure that the discovery task has been previously run. You can [view discovered chassis](#) to see what chassis will be included.

Use AMM IP addresses

☒ discovered by the AMM

☐ in a file that I specify

Next > Cancel

Figure 3-53 Chassis to include

- Click **Next** to open the window shown in Figure 3-54. You can optionally add to existing Fabric Manager configuration. You can specify an existing Fabric Manager configuration file (CSV file) by clicking **Browse**. This file is prepended to the newly generated Fabric Manager configuration file that contains addresses that continue those in the existing specified file. This process extends the existing Fabric Manager domain. If you do not want the new Fabric Manager configuration prepended to an existing configuration, do not specify any file name. Click **Next**.

Optionally add to existing OFM configuration

You can optionally add this new configuration to existing OFM configuration data. Specify the existing OFM data file (.csv file) using the control below. If you do not wish to add to an existing configuration data, simply leave the file name blank.

Configuration file name:

Browse...

Next > Cancel

Figure 3-54 Add existing Fabric Manager configuration

- On the Chassis to include page, there are two methods for providing the list of chassis to be included in the configuration file.

You can either create a file with the list of AMM IP addresses, or use the chassis that were discovered by the AMM through Service Location Protocol (SLP). When using the Use AMM IP Addresses that were discovered on the AMM management network, first operate the Remote Chassis page using the

SLP method. Verify that all chassis that show up there are those you want to configure Fabric Manager on. Otherwise, explicitly specify the chassis address list in a file as explained in the next step.

If you elect to use an explicit list of AMM IP addresses, create a text file in which each line contains a single IP address or the host name of a single chassis. If you use host names in this file, enable DNS and define at least one DNS server on the AMM web interface Network Protocols page. When the text file is complete, select **Use AMM IP Addresses in a file that I specify** on the Chassis to include page.

Click **Browse** to locate the file that you created.

Note: You can also use a valid existing Fabric Manager configuration file to define the list of chassis.

11. Click **Next**. The AMM generates the configuration file and displays the Configuration File Has Been Created window as shown in Figure 3-55.

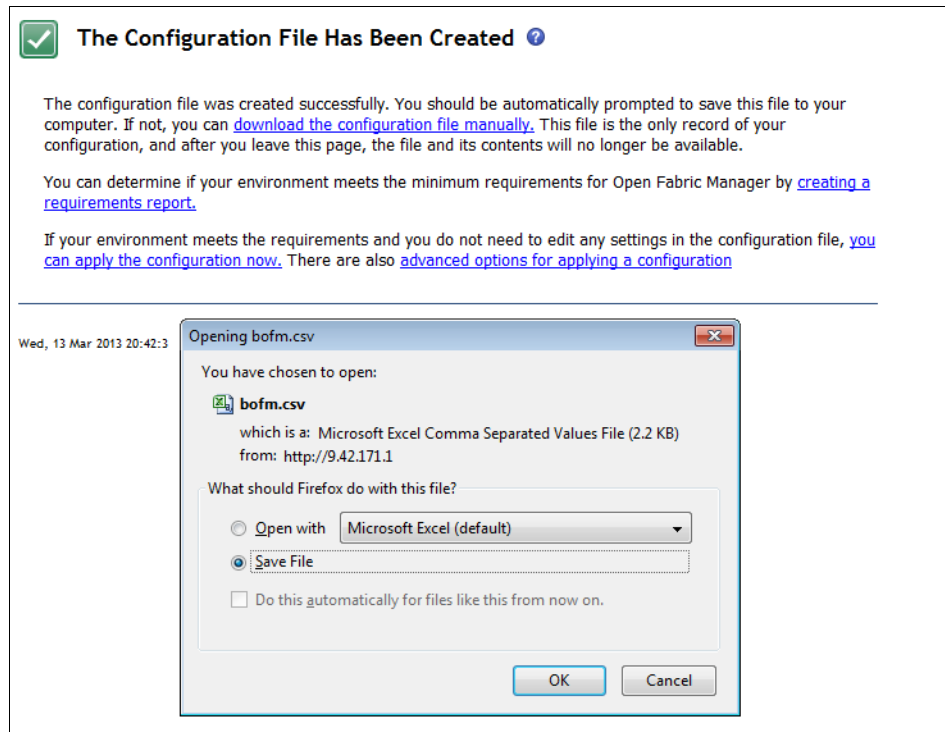


Figure 3-55 Configuration File Has Been Created window

12. The browser launches the File Save window that allows you to save the generated configuration file. If the File Save window is not displayed, click **Download the configuration file manually** on the Configuration File Has Been Created window.

Generally, store the configuration file locally, and validate the new configuration. Store the configuration file in a safe location because this is your original copy of the Fabric Manager configuration. If an AMM has a hardware failure and you do not have a standby AMM, then this is your single source to reproduce the Fabric Manager configuration.

If you want to apply the configuration directly or create a Requirements Report, you can do it directly from this page as shown in Figure 3-56.

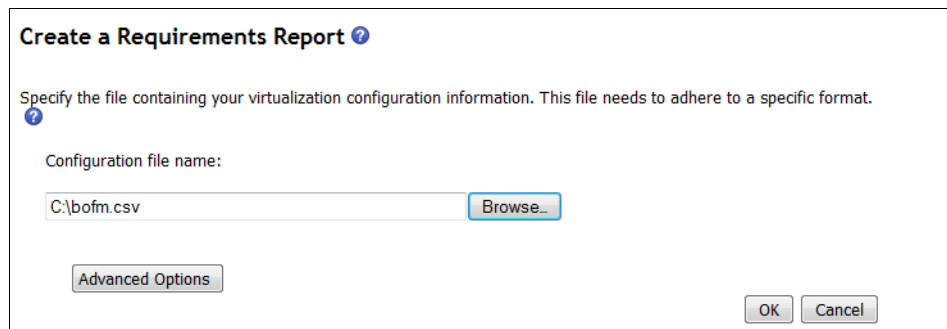


Figure 3-56 BOFM Create a Requirements Report window

For more information about editing the configuration file, applying, reviewing, or retrieving a new configuration, or advanced BOFM functions, see the *IBM Open Fabric Manager Installation and Users Guide* at:

http://pic.dhe.ibm.com/infocenter/director/v5r2/topic/bofm_1.00/btp0_bofm_users_doc.pdf

3.6 BladeCenter S tips and guidelines

When purchasing, installing, or deploying the BladeCenter S chassis, there are several important items to consider to ensure that you maximize your return on investment. This section provides tips and recommendations when you are planning the environment, deploying the chassis in your infrastructure, and supporting the BladeCenter S chassis.

3.6.1 Before you buy

When planning your BladeCenter S purchase, consider the following concerns:

- ▶ Define the networking and SAN requirements for your BladeCenter environment based on your existing infrastructure, including fault tolerance, throughput, and interoperability.
- ▶ Review the power requirements and thermal output to ensure that your environment can support BladeCenter S. Examine your electrical circuits, power distribution units, rack space, and chassis location. Verify that you can provide redundant power sources and adequate cooling. Also, determine whether you plan to place the BladeCenter in an existing location or if you require a new one.

For more information about space requirements, see 2.14, “BladeCenter S Office Enablement Kit” on page 78, and 2.15, “Extra rack options” on page 80. For more information about power redundancy based on the Power Management Policy that you implement, see 2.16, “Power supply modules and redundancy” on page 82. Ensure that you order the type of power cables that match your electrical outlets.

- ▶ Review 2.5.3, “Comparison table of the two SAS module types” on page 48 and decide whether you will deploy the SAS Connectivity Module or the SAS RAID Controller Module. To determine drive size and whether you plan to use SAS or SATA drives, see 2.3, “Drives” on page 37. Ensure that your available disk space meets the growth that you expect for the entire hardware lifecycle.
- ▶ Decide on the type of blades that you are going to install in the chassis. For more information about all supported blades, see 1.5, “Blade servers” on page 11. Size the environment to support the hardware lifecycle.
- ▶ Consider whether your business requires the use of the IBM BladeCenter Airborne Contaminant Filter to passively remove dirt and debris from the environment. More information about the filter can be found at:

http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.chassisop.filter.doc/dw1hh_r_product_overview.html

3.6.2 Deploying the BladeCenter S chassis

Consider the following concerns before you deploy your new chassis:

- ▶ After moving or shipping the BladeCenter S chassis, ensure that all chassis components are properly seated inside the chassis. The best method to ensure that all components are detected without errors during the first power-on of the chassis is to remove and reseal each component.

- ▶ During power-on and discovery, if any module displays the amber fault light, reseal the component before you continue.
- ▶ Depending on your environment, generally connect the BladeCenter AMM on a subnet with a valid DHCP server. This configuration saves time and ensures that the AMM comes online in a correct and timely manner.
- ▶ Determine the best method of ensuring critical firmware updates of all chassis components and how you plan to deploy the BladeCenter S chassis in your environment.

Depending on the size of your deployment, you can use UpdateXpress, the ServerGuide Scripting Toolkit, the AMM or SAS web interface, the command-line interfaces, or a custom deployment method. Maintaining a current revision of firmware on at least the AMM and the I/O Modules ensures that known problems do not affect your environment. Review this chapter to determine the best solution for your deployment.

- ▶ The AMM module provides robust management, monitoring, and alerting on all chassis components. Enabling a proactive alerting system and the Service Advisor feature within the AMM ensures that you maximize the uptime of your chassis. For information about implementing monitoring in your environment, see 3.2.2, “Using the AMM Wizard Custom path” on page 126 or 5.7.3, “Alerts” on page 394.
- ▶ Where possible and practical, place the AMM and I/O Module management interfaces in a separate subnet from the blade environment. Only users in that subnet (typically the administrators group) should have access to it. No normal user should be able to get to the web interface of your systems management hardware by accident.
- ▶ For each management interface, change the password of the default user USERID. When practical, secure the environment by creating a new supervisor user with a different ID and password, and delete USERID.
- ▶ When an LDAP server is available, configure LDAP for user authentication on the AMM. Activate SSL for the LDAP communication. Have at least one supervisor user that is defined locally on every AMM just in case you have LDAP problems.
- ▶ Disable Telnet access and enable SSH connectivity to the command-line interface. Consider generating a unique SSH host key.
- ▶ Enable SSL communication, and either generate a self-signed certificate or import your SSL certificate for the web interface on the AMM.
- ▶ After you finish configuring the BladeCenter advanced management module, back up the configuration to the chassis, and in a file you store remotely in case you must restore it.

- ▶ If a firmware upgrade fails, check the appropriate logs and alerts. Sometimes the firmware has installed successfully but the process still reported an error.
- ▶ For StartNow Advisor and generally other networking functionality on a BladeCenter S, the requirement is for a network module to be installed in bay 1 and configured on the same subnet as the AMM and SAS modules.



Configuring storage

The BladeCenter S chassis offers internal storage that can be easily assigned to any blade server in the chassis. You can install one or two disk storage modules that, in total, can contain 12 hot-swap 3.5-inch disk drives.

The paths to these disks are managed by either the SAS Connectivity Module or the SAS RAID Controller Module.

This chapter covers the following topics:

- ▶ 4.1, “Features of each storage management interface” on page 166
- ▶ 4.2, “Understanding storage zones” on page 168
- ▶ 4.3, “Predefined configuration summary” on page 172
- ▶ 4.4, “Predefined storage configuration schematics” on page 176
- ▶ 4.5, “Storage Configuration Manager” on page 187
- ▶ 4.6, “Using the AMM Storage Configuration task” on page 250
- ▶ 4.7, “Using the SAS module web browser interface” on page 253
- ▶ 4.8, “Configuring the SAS RAID Controller Module using the CLI” on page 265
- ▶ 4.9, “Configuring the SAS Connectivity Module using CLI” on page 269
- ▶ 4.10, “Configuring external SAS ports for SAS tape” on page 280
- ▶ 4.11, “Firmware updating” on page 289
- ▶ 4.12, “Firmware update for disk drives” on page 307
- ▶ 4.13, “IBM System Storage multipath driver” on page 313

4.1 Features of each storage management interface

The BladeCenter S chassis can accommodate up to two disk storage modules as shown in Figure 4-1. Each storage module can house up to six 3.5-inch hard disk drives. These disks can then be assigned directly to blade servers by using either predefined or user definable customer configurations. The two disk storage modules can support up to a total of 24 TB of share storage using 2 TB drives.

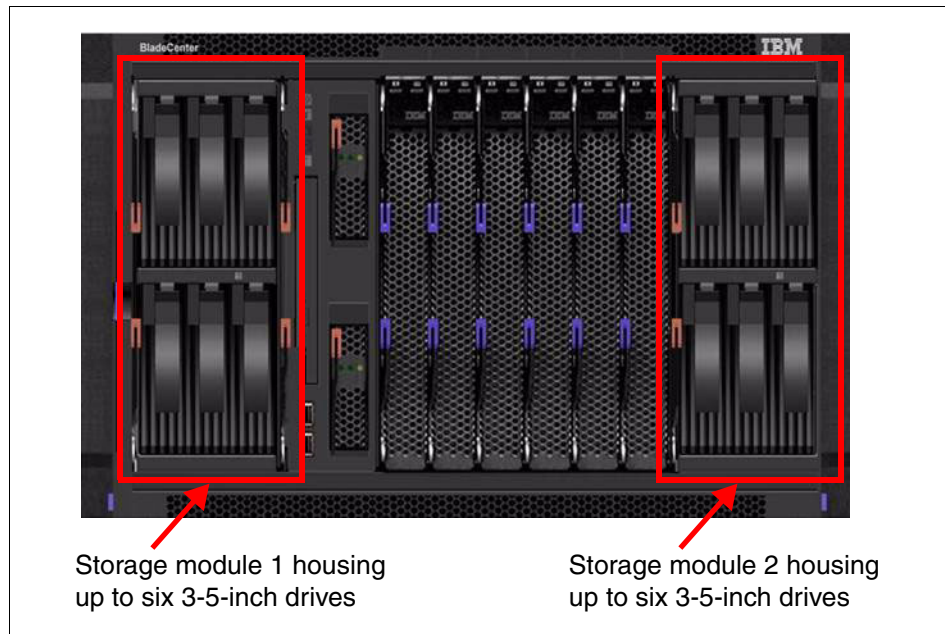


Figure 4-1 The front of the BladeCenter S chassis

BladeCenter S uses a SAS I/O module to enable access from the blade servers to the drives in the disk storage modules. Each provides a different solution and configuration. These SAS I/O modules are available:

- ▶ SAS Connectivity Module
- ▶ SAS RAID Controller Module

The SAS Connectivity Module can be managed by three graphic user interface-based tools, plus a command-line interface that allows you to configure the storage zone configurations:

- ▶ Advanced management module (AMM) Storage Configuration task
- ▶ Storage Configuration Manager
- ▶ SAS Connectivity Module Web browser interface
- ▶ Command-line interface using Telnet

The SAS RAID Controller Module can be managed by using a graphic user interface or a command-line interface:

- ▶ Storage Configuration Manager
- ▶ SAS RAID Controller Module Web browser interface
- ▶ Command-line interface using Telnet

These management tools are addressed in this chapter.

The task that you want to run on the SAS Connectivity Module or SAS RAID Controller Module determines which tool to use. Storage Configuration Manager is the most comprehensive and easy-to-use graphic user interface. It also allows for centralized management of all SAS Connectivity and SAS RAID Controller Modules. SCM also can connect and configure storage on multiple BladeCenter S chassis.

Table 4-1 provides a summary of the tasks and the features of each storage management tool as a quick reference guide.

Table 4-1 Summary of the available features of each storage management tool

Tasks available	SAS Connectivity Module				SAS RAID Controller Module			
	Storage Configuration Manager	SAS Connectivity Module browser UI	AMM storage task	CLI through Telnet	Storage Configuration Manager	SAS RAID Controller Module Browser UI	AMM storage task	CLI through Telnet
N/A = Not Applicable								
Control multiple SAS modules from a single interface	Yes	No	No	No	Yes	No	No	No
Choose and activate a zone configuration	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Create a user-defined configuration	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Create Storage Pools and Volumes	Not applicable				Yes	No	No	Yes
Update SAS Module firmware	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Update Storage Module firmware	Yes	Yes	No	Yes	Yes	No	No	Yes
Back up and restore zone configurations	Yes	No	No	Yes	Yes	No	No	Yes
View system logs	Yes	Yes	No	Yes	Yes	Yes	No	Yes

Tasks available	SAS Connectivity Module				SAS RAID Controller Module			
	Storage Configuration Manager	SAS Connectivity Module browser UI	AMM storage task	CLI through Telnet	Storage Configuration Manager	SAS RAID Controller Module Browser UI	AMM storage task	CLI through Telnet
N/A = Not Applicable								
View error counters	Yes	Yes	No	Yes	Yes	Yes	No	Yes
View audit log	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Enable/disable SAS port access	Yes	No	No	Yes	Yes	No	No	Yes
Modify SAS module user account passwords	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Collect support data	Yes	No	No	Yes	Yes	No	No	Yes

Tip: Most of these tasks are available directly by using a command-line interface through Telnet to the SAS Connectivity Module or the SAS RAID Controller Module.

4.2 Understanding storage zones

Assigning storage within a BladeCenter S chassis involves four criteria:

- ▶ Drive location
- ▶ Storage module number
- ▶ Number of SAS modules
- ▶ External SAS port access

These criteria are linked together to form a configuration that is then assigned to a blade server. The configuration is basically a set of rules that describe the permissions and provisioning of the four criteria. A collection of all six blade server configurations is referred to as a *zone*, and the process of applying the configurations to SAS modules is called *zoning*.

Zoning allows you to decide how to map hard disk drives in storage modules 1 and 2, if present, to the blade servers. It also maps the blade servers to the external ports on the Connectivity Module. When you configure the zoning for the

BladeCenter S, you must determine which hard disk drives are accessible by each of the blade servers. In addition, you must determine which external ports on the SAS Connectivity Module are accessible by each of the blade servers.

To assist with the initial setup of drives and SAS modules, 13 zones have been created. The zones were designed to provide maximum flexibility while remaining simple to use and apply.

Be sure that you fully understand each zone's definition and its impact on blade placement before you begin zoning the chassis. Zoning can be modified later, but there is a risk of data loss. If you rezone and those disks are no longer in your new zone, the stripe or mirror might be broken and the data are lost.

The 13 zones are divided into two types that can be used for storage configuration:

- User-defined configurations

These zones (User Defined Config 1 - 4) are empty so that you can create your own zone configurations.

Replacing a SAS module: The AMM will not restore a user-defined configuration of a replaced SAS module. The user-defined configuration must be manually reapplied to the replaced SAS module. The AMM will, however, restore a predefined zone configuration automatically to a replaced SAS module.

- Predefined configurations

These zones (Predefined Storage Config 6 - 13) are preset zone configurations that cannot be modified. Zone 5 is reserved and therefore not a valid configuration for the BladeCenter S.

Two SAS modules: When a SAS module is installed in a BladeCenter S, a predefined or user-defined configuration must be selected and activated. You must select identical zone configurations if you have two SAS modules installed. This can be done by using the AMM, SAS module web browser interface, or Storage Configuration Manager.

4.2.1 User-defined zones

You can specify up to four user-defined zones (User Defined Config 1 - 4) for the storage that is installed in the chassis. There are these ways to specify your own zoning configuration:

- ▶ Using the Storage Configuration Manager application
- ▶ Using the SAS module web interface
- ▶ Using the SAS module command-line interface

Important: If you use a User Defined Config option, save or export the custom zone configuration. In a SAS module failure, the configuration can be restored to a new module without data loss.

When you design a user-defined zone configuration, determine the following settings in advance:

- ▶ Which hard disk drives in storage module 1 are mapped to each of the blade servers in the BladeCenter unit
- ▶ Which hard disk drives in storage module 2 (if installed) are mapped to each of the blade servers in the BladeCenter unit
- ▶ Which blade server are mapped to the external ports on the SAS module in I/O Expansion Bay 3
- ▶ Which blade server is mapped to the external ports on the SAS module in I/O Expansion Bay 4 (if installed)

Consider the following when mapping blade server storage:

- ▶ Map a blade server to one or more hard disk drives in each storage module for redundancy.
- ▶ Map the blade server to the same hard disk drives in each storage module to reduce management complexity. For example, if you choose to map the blade server in the blade server bay 1 to the hard disk drive in bay 1 of storage module 1, map the same blade server to the hard disk drive in bay 1 of storage module 2.
- ▶ In addition to mapping the hard disk drives, you must use server-side tools, such as the LSI Configuration Utility, to set up hardware redundancy or software mirroring.
- ▶ By default, each disk drive is not allocated to any zones. Each external port belongs to its own zone, and no external port can access any other external port.

4.2.2 Predefined zones

Predefined Storage Config 6- 13 are preset zones that cannot be modified:

- ▶ Even-numbered zones (6, 8, 10, and 12) assume that two SAS modules are installed in the chassis.
- ▶ Odd-numbered zones (7, 9, 11, and 13) assume that only one SAS module is installed.

If you implement a predefined zone and then modify the BladeCenter configuration (such as adding a blade server or storage module), you might have to choose a new zone that matches the BladeCenter's new configuration.

Predefined config 10: There are two Predefined Configuration 10 configurations available: One for the SAS Connectivity Module and another for the SAS RAID Controller Module:

- ▶ Predefined Configuration *10a* is the configuration available if you have the SAS Connectivity Module installed.
- ▶ Predefined Configuration *10b* is the configuration if you have the SAS RAID Controller Module installed.

Each zone defines a predetermined combination of drive location, storage module number, path to SAS modules, and external SAS port access. To view or apply a predefined zone, locate the zone by using the AMM Storage Tasks, the command-line interface, or the Storage Configuration Manager application. The zone's description field provides configuration summary details.

Configuration numbering: Predefined configurations begin with Configuration 6.

Predefined configurations are available to support most typical environments. There are several ways to select a predefined configuration:

- ▶ AMM configuration wizard
- ▶ AMM web-based user interface
- ▶ SAS module command line
- ▶ Storage Configuration Manager application

Tip: You can use Storage Configuration Manager to modify a predefined configuration. However, you must save any changes that you make as one of the four user-defined configurations.

4.3 Predefined configuration summary

A high-level summary of all of the predefined zones is listed in Table 4-2. Detailed descriptions of each zone can be found in 4.4, “Predefined storage configuration schematics” on page 176.

Table 4-2 Predefined configuration summary table (SM1 = storage module 1, SM2 = storage module 2)

	Number of disks assigned	SAS Controller in I/O Expansion Bay 3	SAS Controller in I/O Expansion Bay 4	Access to external SAS ports
Predefined Configuration 6 (see page 176 for disk mappings)				
Blade server 1	2	Disk 1 - SM1	Disk 1 - SM2	All
Blade server 2	2	Disk 2 - SM1	Disk 2 - SM2	All
Blade server 3	2	Disk 3 - SM1	Disk 3 - SM2	All
Blade server 4	2	Disk 4 - SM1	Disk 4 - SM2	All
Blade server 5	2	Disk 5 - SM1	Disk 5 - SM2	All
Blade server 6	2	Disk 6 - SM1	Disk 6 - SM2	All
Predefined Configuration 7 (see page 177 for disk mappings)				
Blade server 1	2	Disk 1 - SM1 Disk 1 - SM2	Not applicable	All
Blade server 2	2	Disk 2 - SM1 Disk 2 - SM2	Not applicable	All
Blade server 3	2	Disk 3 - SM1 Disk 3 - SM2	Not applicable	All
Blade server 4	2	Disk 4 - SM1 Disk 4 - SM2	Not applicable	All
Blade server 5	2	Disk 5 - SM1 Disk 5 - SM2	Not applicable	All
Blade server 6	2	Disk 6 - SM1 Disk 6 - SM2	Not applicable	All
Predefined Configuration 8 (see page 178 for disk mappings)				
Blade server 1	12	Disk 1,2,3,4,5,6 - SM1	Disk 1,2,3,4,5,6 - SM2	All
Blade server 2	0	None	None	All
Blade server 3	0	None	None	All

	Number of disks assigned	SAS Controller in I/O Expansion Bay 3	SAS Controller in I/O Expansion Bay 4	Access to external SAS ports
Blade server 4	0	None	None	All
Blade server 5	0	None	None	All
Blade server 6	0	None	None	All
Predefined Configuration 9 (see page 179 for disk mappings)				
Blade server 1	12	Disk 1,2,3,4,5,6 - SM1 Disk 1,2,3,4,5,6 - SM2	Not applicable	All
Blade server 2	0	None	Not applicable	All
Blade server 3	0	None	Not applicable	All
Blade server 4	0	None	Not applicable	All
Blade server 5	0	None	Not applicable	All
Blade server 6	0	None	Not applicable	All
Predefined Configuration 10a - SAS Connectivity Module (see page 180 for disk mappings)				
Blade server 1	4	Disk 1 - SM1 Disk 4 - SM1	Disk 1 - SM2 Disk 4 - SM2	All
Blade server 2	0	None	None	All
Blade server 3	4	Disk 2 - SM1 Disk 5 - SM1	Disk 2 - SM2 Disk 5 - SM2	All
Blade server 4	0	None	None	All
Blade server 5	4	Disk 3 - SM1 Disk 6 - SM1	Disk 3 - SM2 Disk 6 - SM2	All
Blade server 6	0	None	None	All

	Number of disks assigned	SAS Controller in I/O Expansion Bay 3	SAS Controller in I/O Expansion Bay 4	Access to external SAS ports
Predefined Configuration 10b - SAS RAID Controller Module (see page 142 for disk mappings)				
Blade server 1	All	RAID Pool	RAID Pool	All
Blade server 2	All	RAID Pool	RAID Pool	All
Blade server 3	All	RAID Pool	RAID Pool	All
Blade server 4	All	RAID Pool	RAID Pool	All
Blade server 5	All	RAID Pool	RAID Pool	All
Blade server 6	All	RAID Pool	RAID Pool	All
Predefined Configuration 11 (see page 183 for disk mappings)				
Blade server 1	4	Disk 1, 4 - SM1 Disk 1, 4 - SM2	Not applicable	All
Blade server 2	0	None	Not applicable	All
Blade server 3	4	Disk 2, 5 - SM1 Disk 2, 5 - SM2	Not applicable	All
Blade server 4	0	None	Not applicable	All
Blade server 5	4	Disk 3, 6 - SM1 Disk 3, 6 - SM2	Not applicable	All
Blade server 6	0	None	Not applicable	All
Predefined Configuration 12 (see page 184 for disk mappings)				
Blade server 1	6	Disk 1, 3, 5 - SM1	Disk 1, 3, 5 - SM2	All
Blade server 2	0	None	None	All
Blade server 3	0	None	None	All
Blade server 4	6	Disk 2, 4, 6 - SM1	Disk 2, 4, 6 - SM2	All
Blade server 5	0	None	None	All
Blade server 6	0	None	None	All

	Number of disks assigned	SAS Controller in I/O Expansion Bay 3	SAS Controller in I/O Expansion Bay 4	Access to external SAS ports
Predefined Configuration 13 (see page 185 for disk mappings)				
Blade server 1	6	Disk 1, 3, 5 - SM1 Disk 1, 3, 5 - SM2	Not applicable	All
Blade server 2	0	None	Not applicable	All
Blade server 3	0	None	Not applicable	All
Blade server 4	6	Disk 2, 4, 6 - SM1 Disk 2, 4, 6 - SM2	Not applicable	All
Blade server 5	0	None	Not applicable	All
Blade server 6	0	None	Not applicable	All

4.4 Predefined storage configuration schematics

This section describes the details of the predefined storage configurations.

4.4.1 Predefined Storage Configuration 6

Predefined Storage Configuration 6 is designed so that all six blade servers have access to the onboard storage of the BladeCenter S. The configuration consists of storage that is mapped to all six blade servers, two SAS modules, and two fully populated disk storage modules. Each blade server can access one hard disk drive in each disk storage module and all external ports on both SAS modules.

This configuration, which is shown in Figure 4-2, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Use the LSI Configuration Utility, which is available during the boot sequence of each blade server, to create arrays and establish RAID support for the assigned storage.

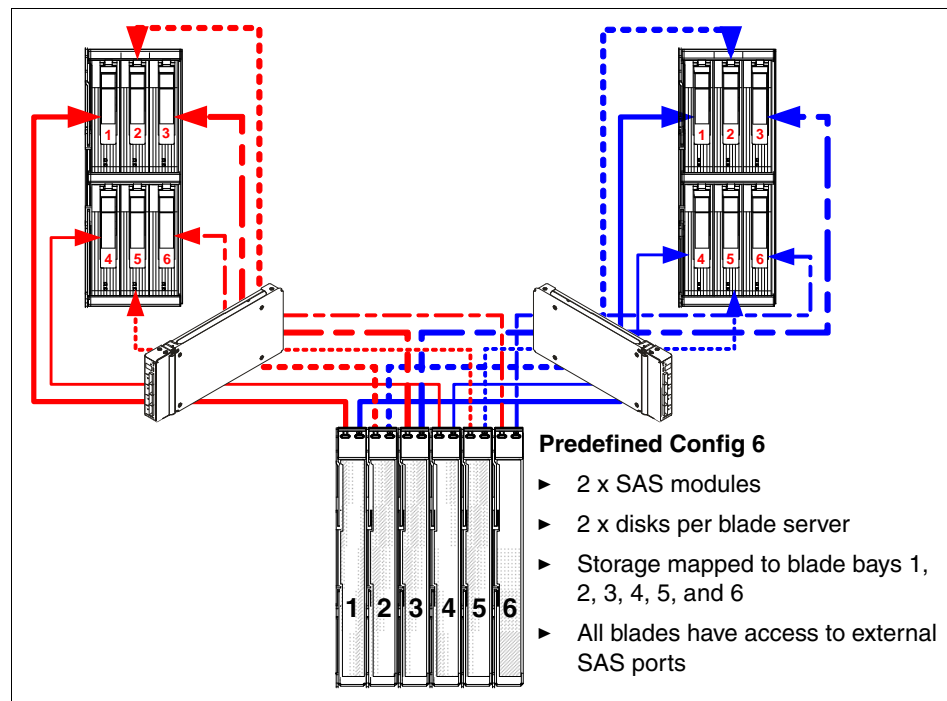


Figure 4-2 Predefined Storage Configuration 6

4.4.2 Predefined Storage Configuration 7

Predefined Storage Configuration 7 is designed so that all six blade servers have access to the onboard storage of the chassis. The configuration consists of storage that is mapped to all six blade servers, one SAS module, and two fully populated disk storage modules. Each blade server can access one hard disk drive in each disk storage module and all external ports on the SAS module.

This configuration, which is shown in Figure 4-3, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Use the LSI Configuration Utility, which is available during the boot sequence of each blade server, to create arrays and establish RAID support for the assigned storage.

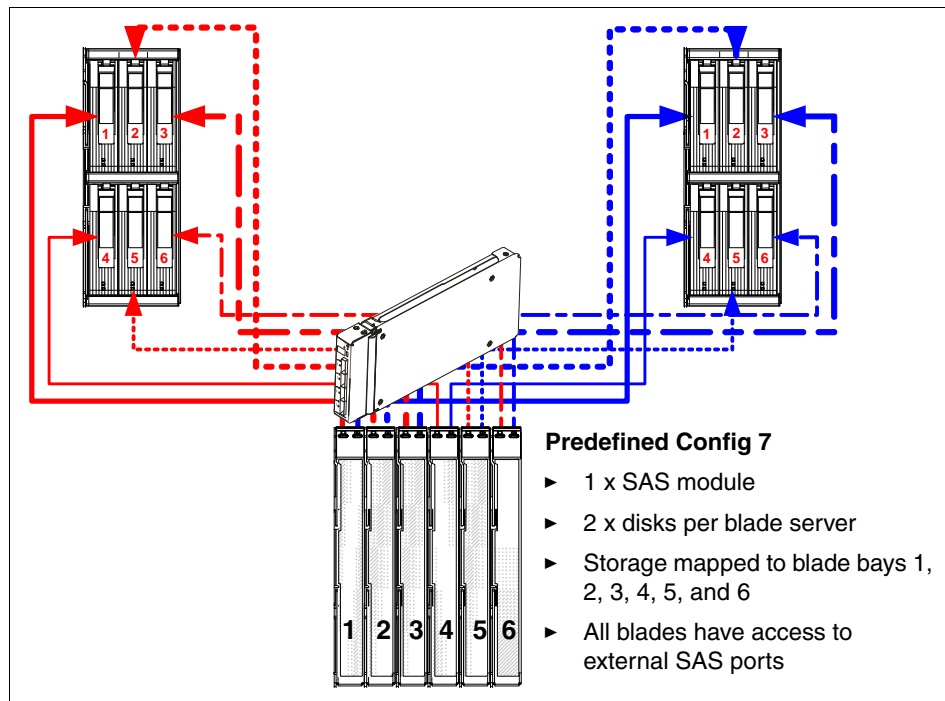


Figure 4-3 Predefined Storage Configuration 7

4.4.3 Predefined Storage Configuration 8

Predefined Storage Configuration 8 is designed so that only the blade server in blade bay 1 has access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to a single blade server, two SAS modules, and two fully populated disk storage modules. The blade server can access all hard disk drives in both disk storage modules and all external ports on both SAS modules.

This configuration, which is shown in Figure 4-4, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Use the LSI Configuration Utility, which is available during the boot sequence of each blade server, to create arrays and establish RAID support for the assigned storage.

Important: The blade server must be in blade bay 1 to access the zoned storage of this configuration.

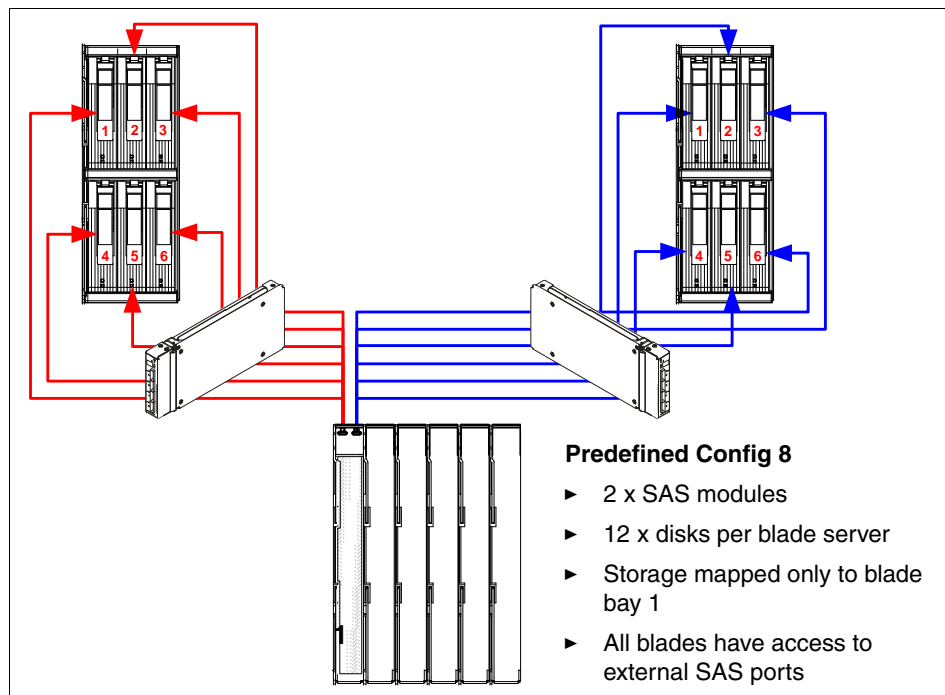


Figure 4-4 Predefined Storage Configuration 8

4.4.4 Predefined Storage Configuration 9

Predefined Storage Configuration 9 is designed so that only the blade server in blade bay 1 has access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to a single blade server, one SAS module, and two fully populated disk storage modules. The blade server can access all hard disk drives in both disk storage modules and all external ports on the SAS module.

This configuration (Figure 4-5) maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Use the LSI Configuration Utility, which is available during the boot sequence of each blade server, to create arrays and establish RAID support for the assigned storage.

Important: The blade server must be in blade bay 1 to access the zoned storage of this configuration.

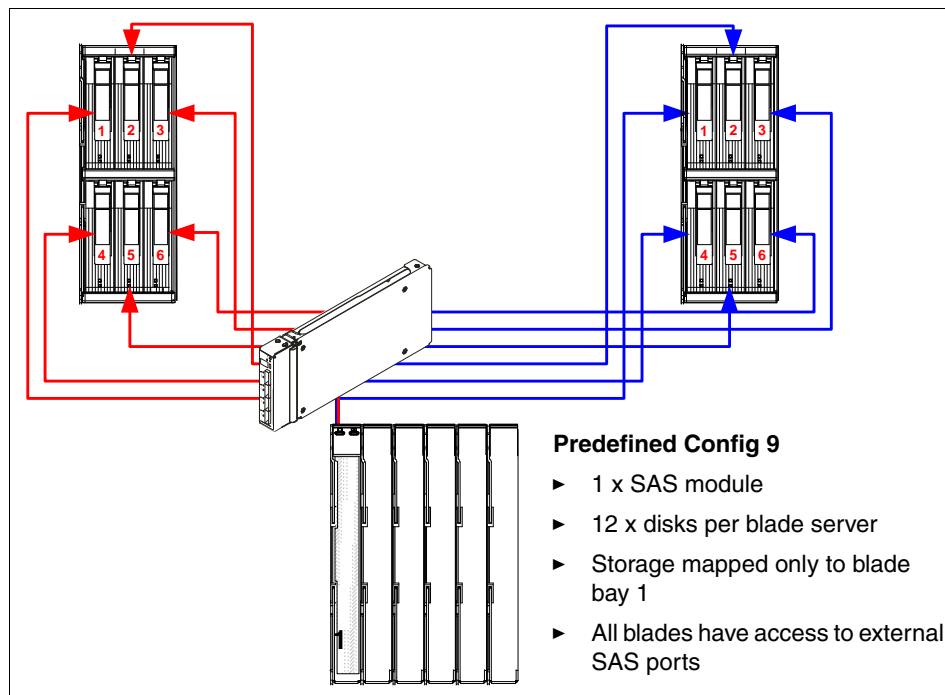


Figure 4-5 Predefined Storage Configuration 9

4.4.5 Predefined Storage Configuration 10a

Note: Predefined Storage Configuration 10a is valid only for the SAS Connectivity Module. If you have the SAS RAID Connectivity Module, refer to 4.4.6, “Predefined Storage Configuration 10b” on page 181.

Predefined Storage Configuration 10 is designed so that only three blade servers (which must be in blade bays 1, 3, and 5 to access the zoned storage of the configuration) have access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to three blade servers, two SAS modules, and two fully populated disk storage modules. Each blade server can access two hard disk drives in each disk storage module and all external ports on both SAS modules.

This configuration, which is shown in Figure 4-6 on page 181, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Server-side tools like the LSI Configuration Utility, which is available during the boot sequence of the HS23 server, can be used to create arrays and establish RAID support for the assigned storage.

Important: The blade servers must be in blade bays 1, 3, and 5 to access the zoned storage of this configuration.

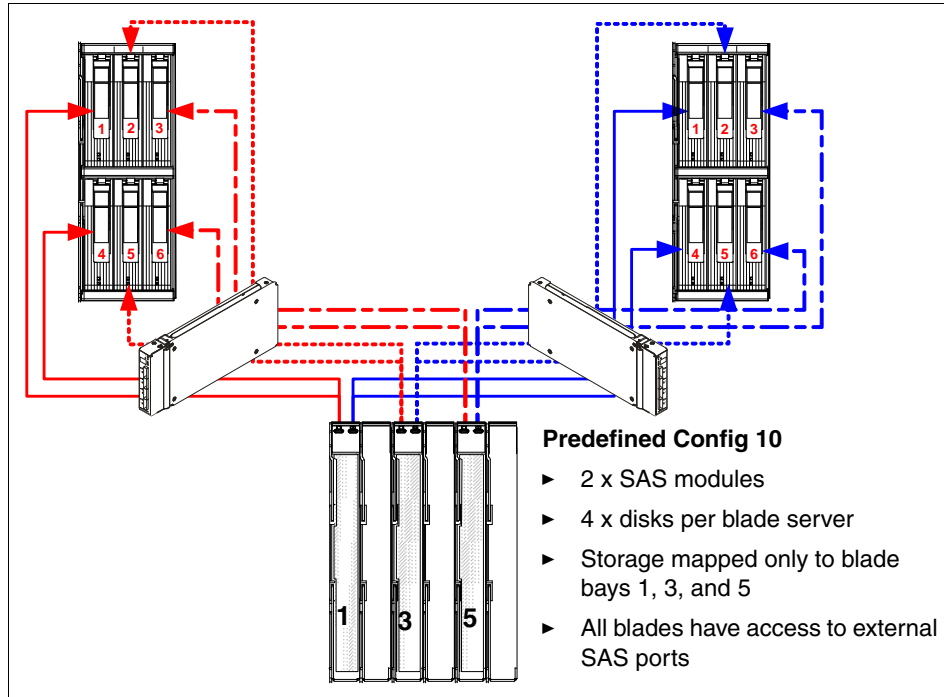


Figure 4-6 Predefined Storage Configuration 10

4.4.6 Predefined Storage Configuration 10b

Note: Predefined Storage Configuration 10b is valid only for the SAS RAID Connectivity Module. If you have the SAS Connectivity Module, refer to 4.4.5, “Predefined Storage Configuration 10a” on page 180.

Predefined Storage Configuration 10b is designed so that all blade servers to have access to the onboard storage of the BladeCenter S.

The configuration consists of all hard disk drives in both storage modules to be mapped to all blade servers, using both SAS RAID modules. Each blade server can access the storage pool in each disk storage module and all external ports on both SAS modules.

This configuration, which is shown in Figure 4-7, maps the hard disk pool to the blade server and all blade servers to the external ports on the SAS module. To create RAID levels and define hot-spare drives, connect the SAS RAID Controller Module by using Storage Configuration Manager. You can also configure volumes, raid levels, and pools by using the command-line interface of the RAID module.

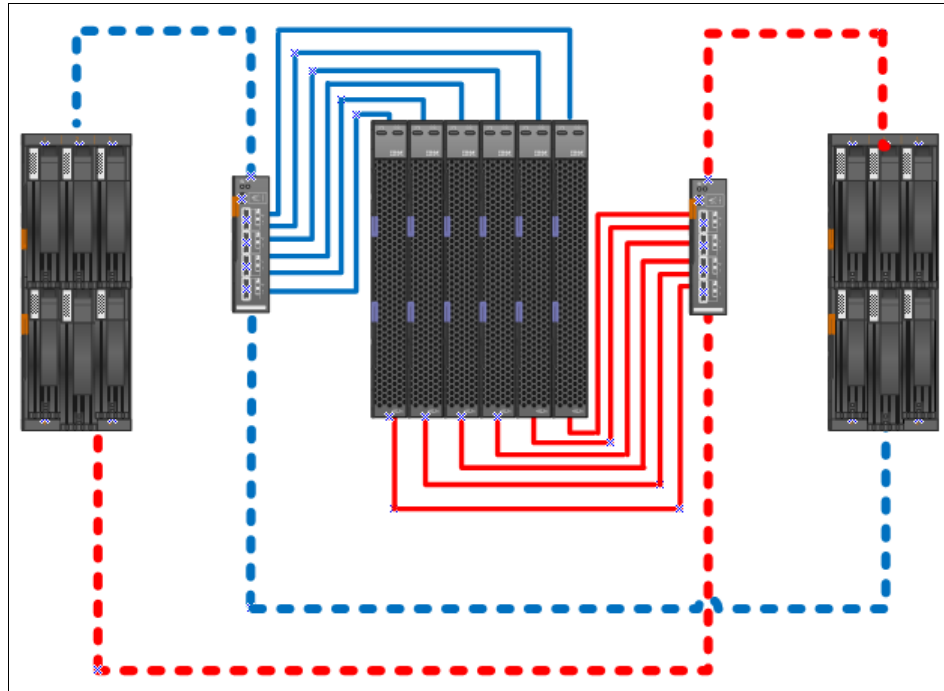


Figure 4-7 All blade servers with access to all disks

The SAS CIOv daughter card that is installed in each blade server connects to the two SAS RAID Controller Modules present in the BladeCenter S chassis. The two SAS modules have access to both Storage Modules. More levels of redundancy can be achieved by configuring RAID levels and hot-spare drives with the disks.

4.4.7 Predefined Storage Configuration 11

Predefined Storage Configuration 11 is designed so that three blade servers (which must be in blade bays 1, 3, and 5 to access the zoned storage of the configuration) have access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to three blade servers, one SAS module, and two fully populated disk storage modules. Each blade server can access two hard disk drives in each disk storage module and all external ports on the SAS module.

This configuration, which is shown in Figure 4-8 on page 184, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Server-side tools like the LSI Configuration Utility, which is available during the boot sequence of the HS23 server, can be used to create arrays and establish RAID support for the assigned storage.

Important: The blade servers must be in blade bays 1, 3, and 5 to access the zoned storage of this configuration.

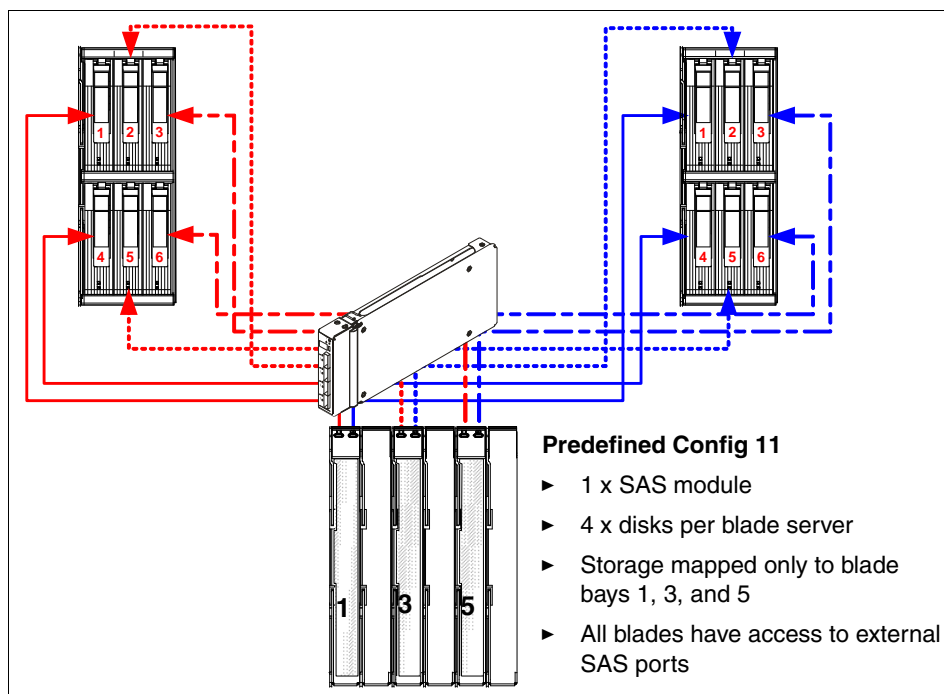


Figure 4-8 Predefined Storage Configuration 11

4.4.8 Predefined Storage Configuration 12

Predefined Storage Configuration 12 is designed so that two blade servers (which must be in blade bays 1 and 4 to access the zoned storage of the configuration) have access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to two blade servers, two SAS modules, and two fully populated disk storage modules. Each blade server can access three hard disk drives in each disk storage module and all external ports on both SAS modules.

This configuration, which is shown in Figure 4-9, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. Server-side tools like the LSI Configuration Utility, which is available during the boot sequence of the HS23 server, can be used to create arrays and establish RAID support for the assigned storage.

Important: The blade servers must be in blade bays 1 and 4 to access the zoned storage of this configuration.

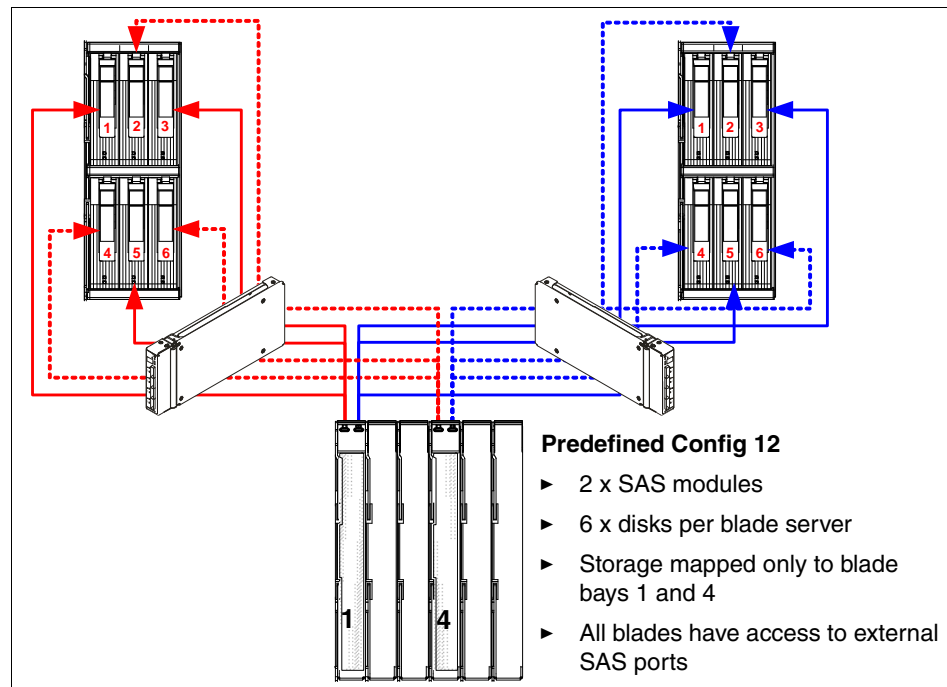


Figure 4-9 Predefined Storage Configuration 12

4.4.9 Predefined Storage Configuration 13

Predefined Storage Configuration 13 is designed so that two blade servers (which must be in blade bays 1 and 4 to access the zoned storage of the configuration) have access to the onboard storage of the BladeCenter S. Blade servers that are installed in any other blade bays do not have access to the zoned storage of this configuration, but function normally otherwise.

The configuration consists of storage that is mapped to two blade servers, one SAS module, and two fully populated disk storage modules. Each blade server can access three hard disk drives in each disk storage module and all external ports on the SAS module.

This configuration, which is shown in Figure 4-10, maps the hard disks to the blade server and the blade server to the external ports on the SAS module. The LSI Configuration Utility, which is available during the boot sequence of each blade server, must be used to create arrays and establish RAID support for the assigned storage.

Important: Blade servers must be in blade bays 1 and 4 to access the zoned storage of this configuration.

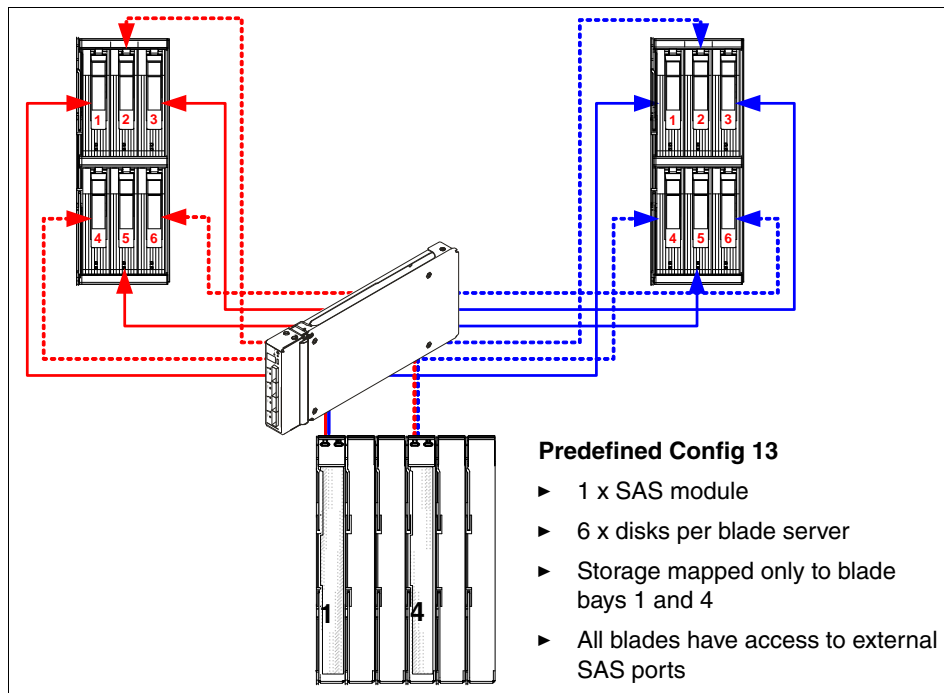


Figure 4-10 Predefined Storage Configuration 13

4.5 Storage Configuration Manager

The Storage Configuration Manager (SCM) tool is used to administrator the SAS modules and other storage controllers. It allows for centralized administration of multiple SAS modules that might be installed in multiple BladeCenter chassis. This sections we looks specifically at the BladeCenter S component within SCM and its available management features.

The following tasks are addressed in this section:

- ▶ 4.5.1, “Installing SCM with the BladeCenter S component” on page 187
- ▶ 4.5.2, “Starting Storage Configuration Manager” on page 194
- ▶ 4.5.3, “Initial Setup Wizard for the SAS RAID Controller Module” on page 197
- ▶ 4.5.4, “Initial Configuration Wizard for the SAS Connectivity Module” on page 213

The following sections cover the SAS Connectivity Module:

- ▶ 4.5.5, “User-defined and zone configurations” on page 219

The following sections cover the SAS RAID Controller Module:

- ▶ 4.5.6, “All Resources window” on page 229
- ▶ 4.5.7, “Physical View window” on page 230
- ▶ 4.5.9, “Active Alerts window” on page 233
- ▶ 4.5.10, “Long Running Tasks window” on page 234
- ▶ Figure 4.5.11 on page 235

The following sections cover common tasks:

- ▶ 4.5.12, “SAS Zoning task” on page 236
- ▶ 4.5.13, “Ports and SAS ports” on page 237
- ▶ 4.5.14, “Audit log” on page 242
- ▶ 4.5.15, “Update firmware for the SAS Connectivity Module” on page 243
- ▶ 4.5.16, “Updating firmware for the SAS RAID Controller Module” on page 243
- ▶ 4.5.17, “Device log” on page 244
- ▶ 4.5.18, “Error counters” on page 246
- ▶ 4.5.19, “Collecting support data” on page 248
- ▶ 4.5.20, “User management” on page 249

4.5.1 Installing SCM with the BladeCenter S component

Before SCM can be used, the product must be installed onto either a workstation or server that is running either Windows or Linux. Read the documentation that is supplied with the Storage Configuration Manager software for hardware and

software installation requirements. The example installs SCM Version 2.20.0 onto a Windows workstation. SCM can be downloaded from:

<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5081393>

To begin the installation, complete these steps:

1. Extract **ibm_sw_scm-2.20.0_windows_i386.zip** files into your assigned folder and then view the extracted files. There are two folders, called FILES and META-INF.
2. Click the **FILES** folder and then double-click **scminstall.exe**. This starts the installation process for SCM.
3. The SCM Introduction window is displayed as shown in Figure 4-11. Click **Next**.

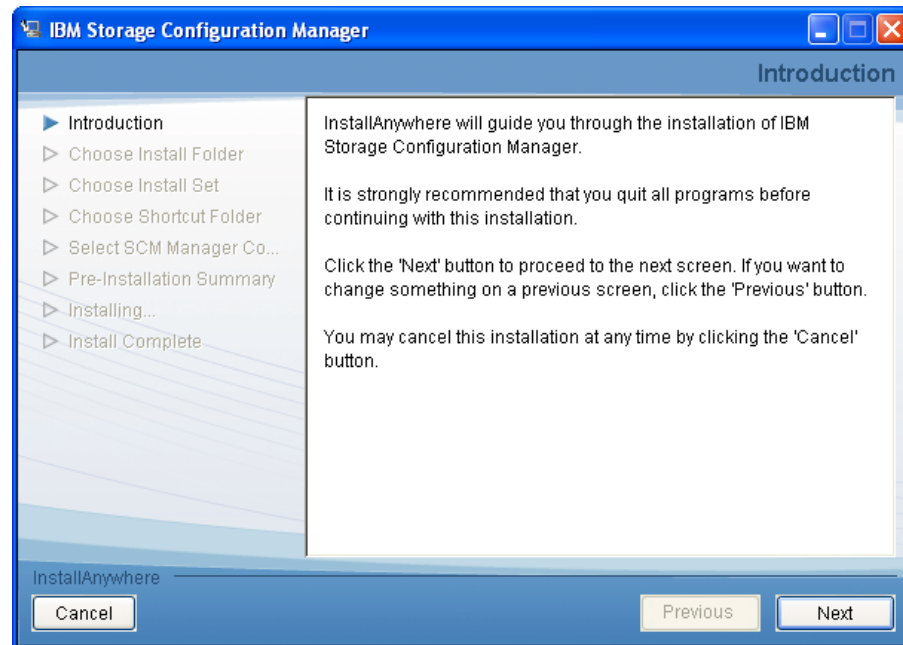


Figure 4-11 SCM Introduction window

4. Accept the license agreement and then click **Next**.

5. The SCM then prompts for the installation folder location. The example used the defaults as shown in Figure 4-12. Click **Next**.

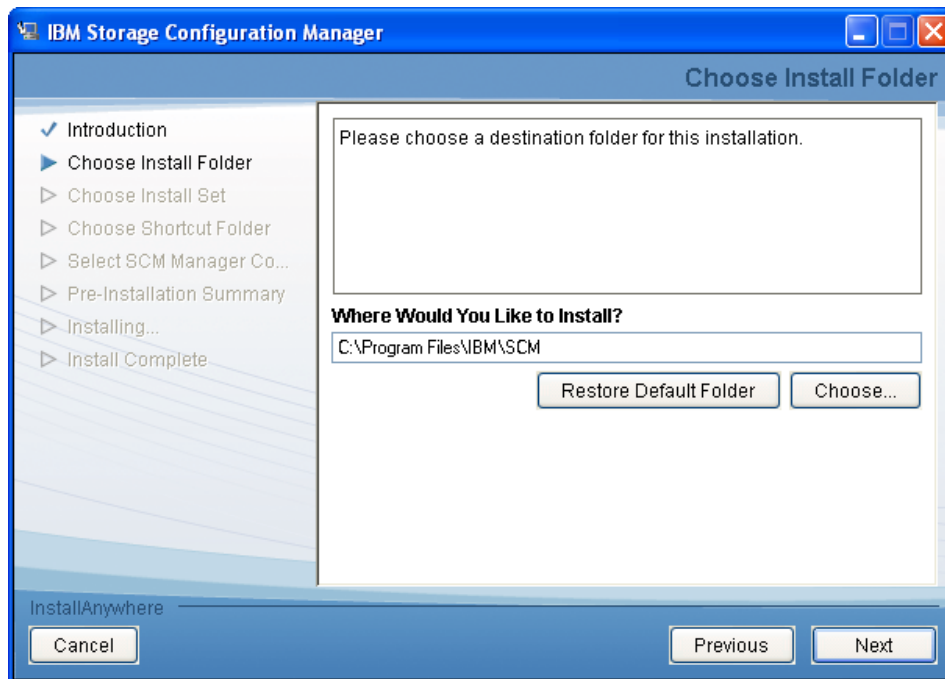


Figure 4-12 SCM folder installation location

6. SCM 2.2.0 only provides **SCM Full Install for all devices** as shown in Figure 4-13. Click **Next**.

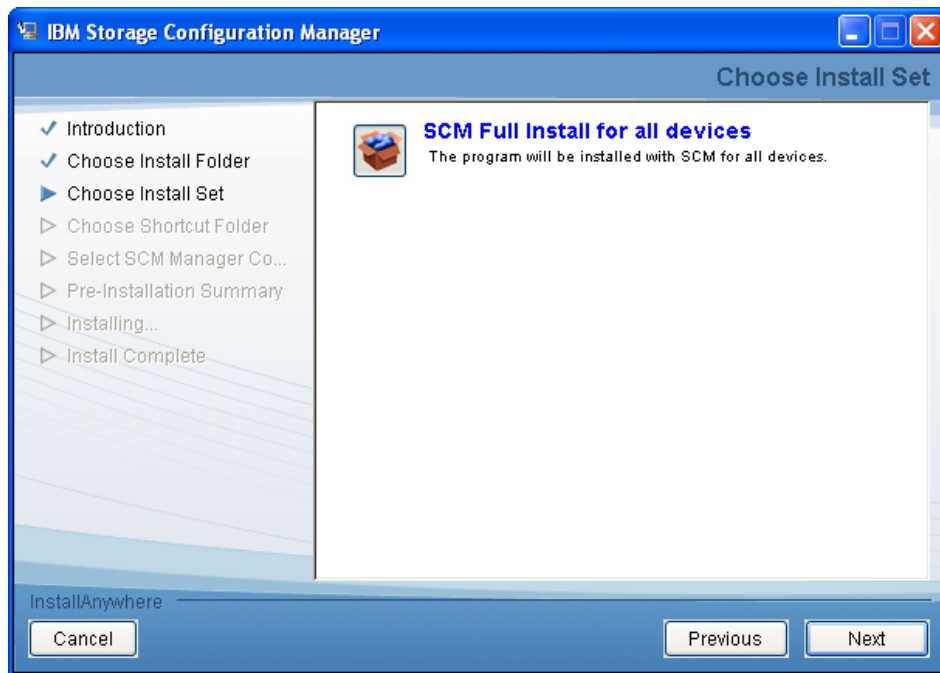


Figure 4-13 SCM full installation option

7. Figure 4-14 prompts you to select where to place the program icons for SCM. Generally, use the default ports unless they are already assigned. Click **Next**.

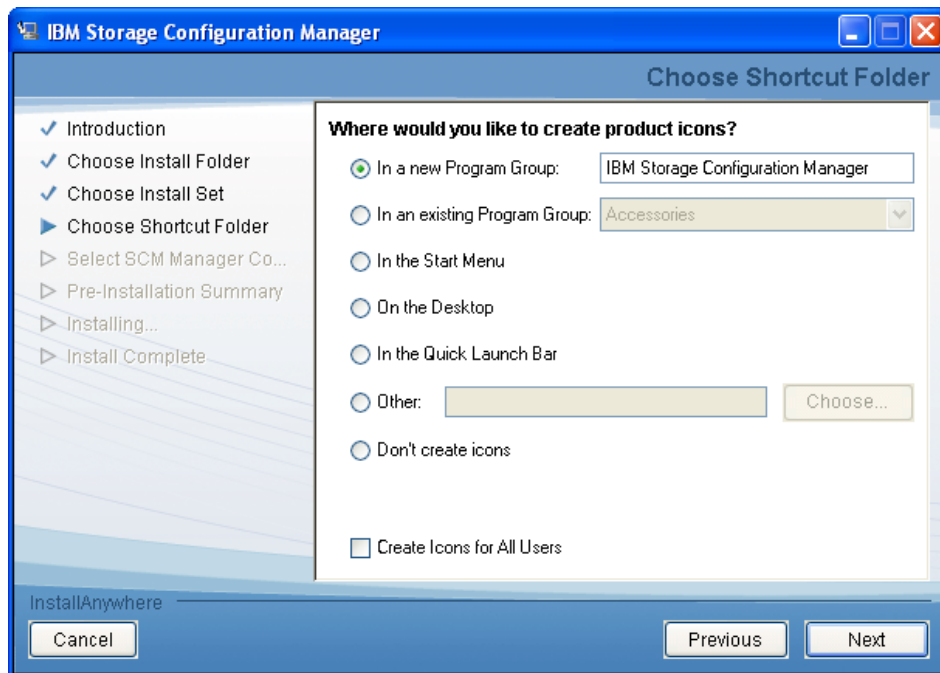


Figure 4-14 SCM shortcut locations window

8. Figure 4-15 allows you to either accept the default ports that SCM will use or select your own. Generally, use the default ports unless they are already assigned. Click **Next**.

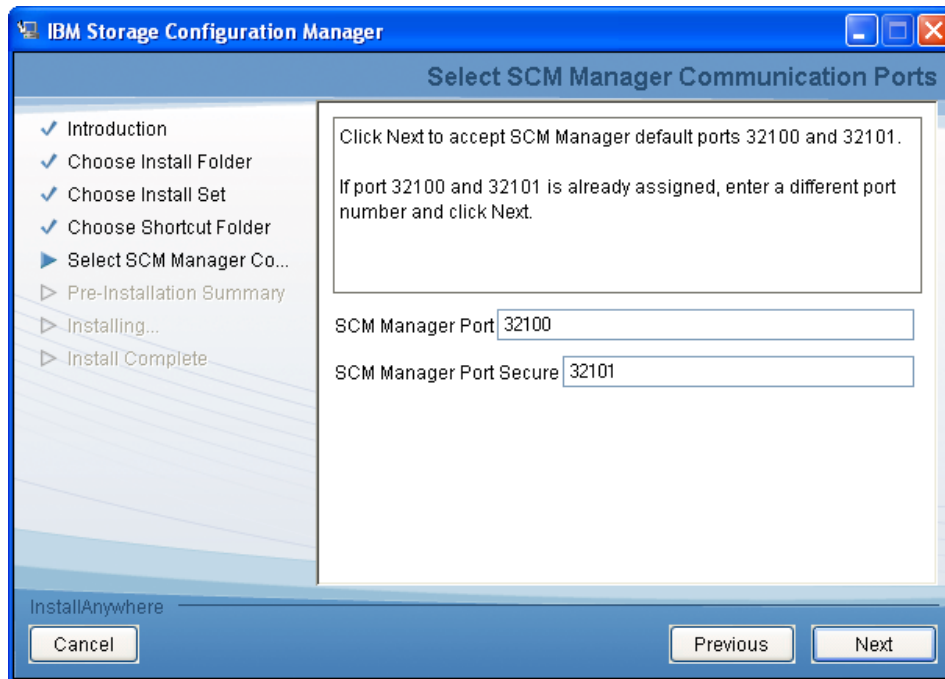


Figure 4-15 SCM communication port assignment

9. SCM displays a summary of the selected options before installation as shown in Figure 4-16. Click **Install** when ready.

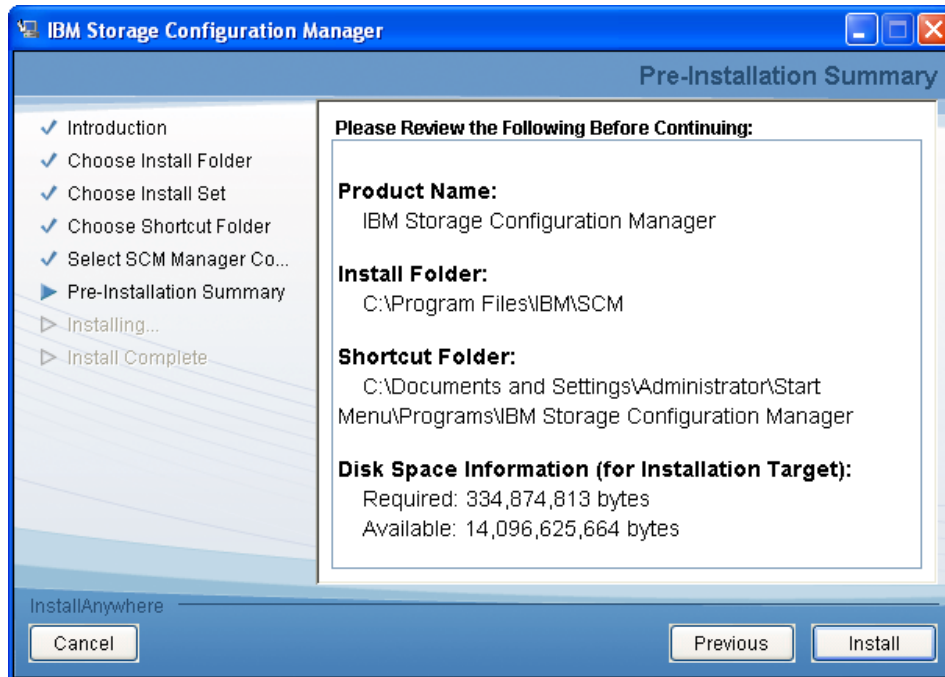


Figure 4-16 SCM preinstallion summary

10. SCM installs multiple components. After the installation is successful, an Install Complete window is displayed as shown in Figure 4-17. Click **Done**.

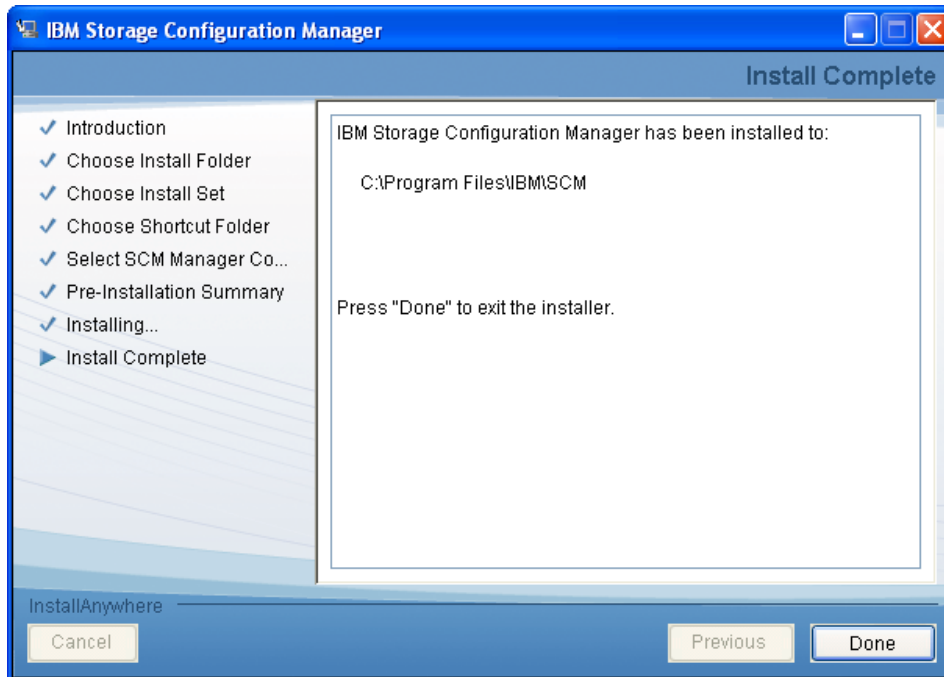


Figure 4-17 SCM successful installation window

11. Ensure that you reboot the system after the installation completes to allow proper operation of Storage Configuration Manager.

4.5.2 Starting Storage Configuration Manager

You can start Storage Configuration Manager either locally or remotely. A local launch can be done by using one of these methods:

- ▶ Click **Start** → **Programs** → **IBM Storage Configuration Manager** → **IBM Storage Configuration Manager**.
- ▶ Open a web browser and browse to:
`https://localhost:32101/ibm/console/logon.jsp`

To log in from a remote workstation, substitute `localhost` in the preceding URL with the remote server's fully qualified domain name or IP address; for example:

`https://servername-or-ipaddress:32101/ibm/console/Login.jsp`

Figure 4-18 displays the SCM login window as started by the application

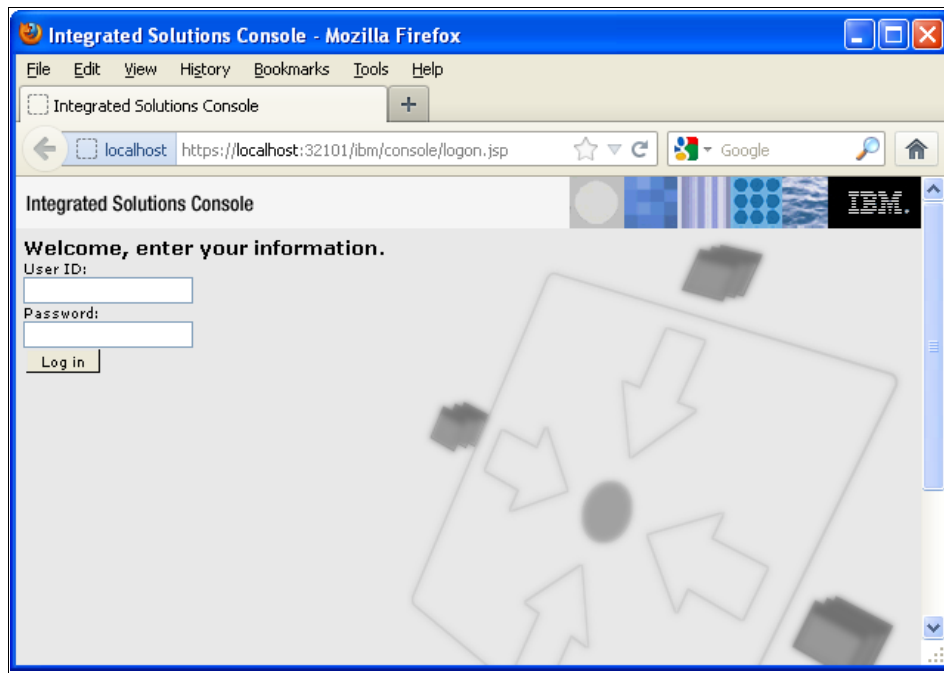


Figure 4-18 SCM Login Portlet window

After connecting your web browser to Storage Configuration Manager, log in by entering the user name and password. The account credentials that you supply can be the account with which you installed the product, or a user account that has administrative permissions to access the server or workstation where SCM is installed.

If Storage Configuration Manager is installed on a Windows server that is configured with multiple domains, specify the domain by entering the user name in the following format:

user@domain

After you log in to Storage Configuration Manager, the Welcome window is displayed as seen in Figure 4-19.

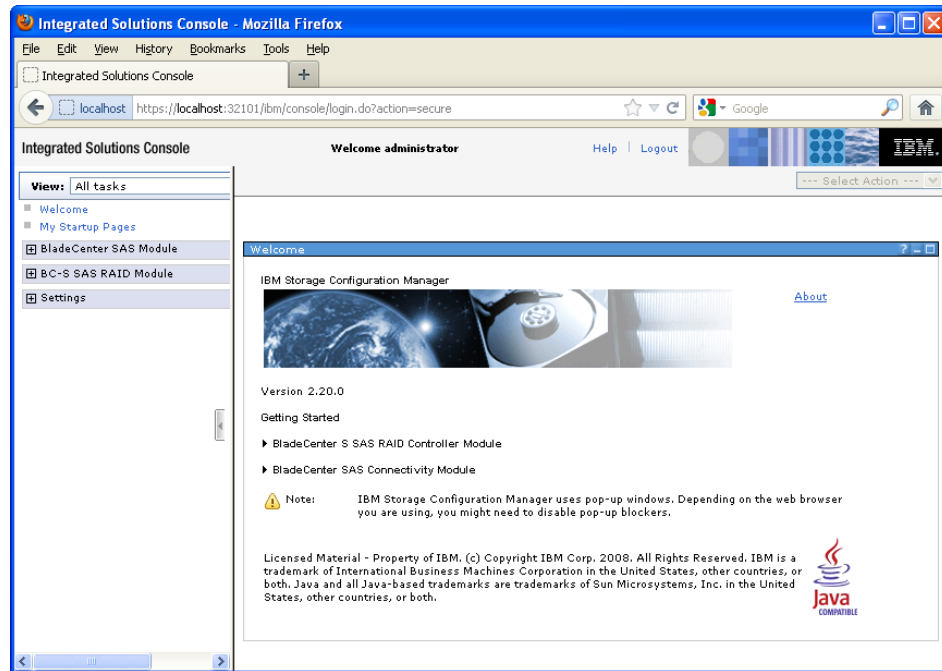


Figure 4-19 SCM Welcome window

The next two sections describe the wizards use for initial configuration:

- ▶ 4.5.3, "Initial Setup Wizard for the SAS RAID Controller Module" on page 197
- ▶ 4.5.4, "Initial Configuration Wizard for the SAS Connectivity Module" on page 213

4.5.3 Initial Setup Wizard for the SAS RAID Controller Module

You can use the Initial Setup Wizard to perform basic operations to add the SAS RAID Controller Modules into the console. To begin the configuration process, complete these steps:

1. Click **BladeCenter S SAS RAID Controller Module** on the Getting Started page and select the **Initial Setup Wizard** as seen in Figure 4-20.

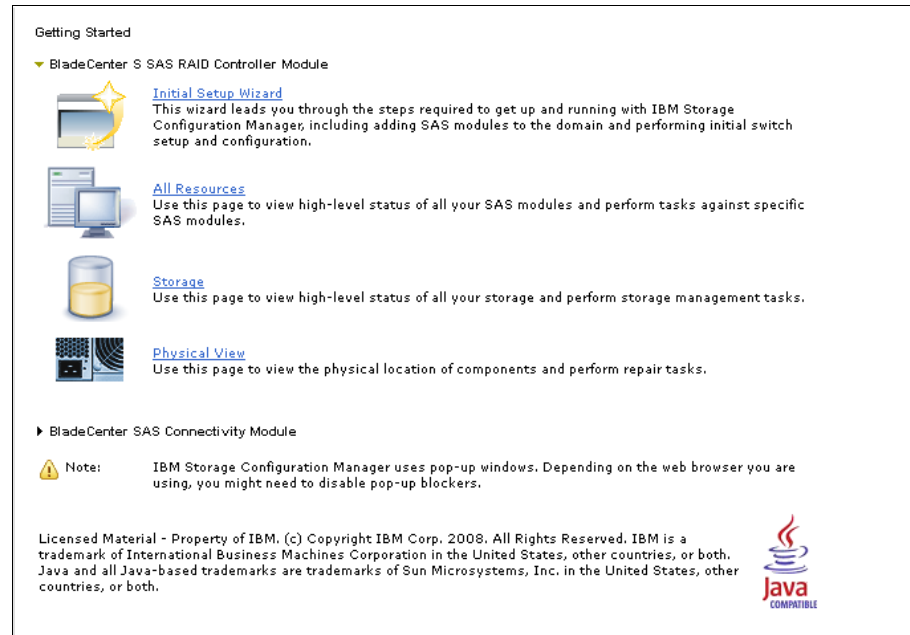


Figure 4-20 SAS RAID Controller Module initial wizard setup

2. A Welcome window to add the SAS RAID Controller Module is displayed as seen in Figure 4-21. Add the IP address of the built-in SAS Switch of the SAS RAID Controller Module installed in bay 3. In addition, provide the user ID and password for both the SAS switch and the RAID Controller and click **Next**.

The initial SAS RAID Controller IP address, user ID, and password are configured initially by using the AMM interface. For more information, see 5.5.2, “Configuration” on page 376.

Notes:

- ▶ Generally, use a SAS Switch Name that is shared for both SAS RAID Controller Modules. The I/O bay numbers are added as a suffix to this name when viewed through Storage Configuration Manager.
- ▶ You must add the IP address of the SAS RAID Controller Module’s built-in SAS switch, *not* the IP address that is assigned to the RAID Controller subsystem itself. Also, unlike the SAS Connectivity Module, you only need to add the IP address of the RAID Controller’s built-in SAS switch in bay 3. The SAS RAID Controller Module in bay 4 is added automatically if it is configured correctly.

Add SAS RAID Module in I/O Bay

Register your SAS RAID Module installed in I/O Bay 3 with SCM. Each SAS RAID Module has an embedded SAS Switch and RAID controller packaged together.

SAS Switch Identifier

* SAS switch IP address:

This is the IP address set up initially using the Advanced Management Module.

SAS Switch Name:

SAS RAID Module Login

This is either the default user ID and password, or one that was set up initially using the Advanced Management Module.

SAS Switch

* User ID: * Password:

RAID Controller

* User ID: * Password:

< Back Next > Finish Cancel

Figure 4-21 Adding a SAS RAID Controller Module

Single SAS RAID Controller Module: As of firmware 1.2.4.011, the SAS RAID Controller Module is now supported in single controller configuration. The example configuration uses a single SAS RAID Controller Module.

3. Set the date and time for the SAS switch subsystem to connect to an NTP time server, or specify the date and time manually as shown in Figure 4-22. Click **Next** when done.

The screenshot shows a configuration window titled "Set SAS Switches Date and Time". The window has a left sidebar with a list of configuration steps: "Add SAS RAID Modules", "SAS Date And Time" (highlighted), "RAID Date And Time", "SAS Passwords", "RAID Passwords", "Configure Storage", "Apply saved configuration", "Apply backed up configuration", "Spare Coverage", "Create Storage Pool", "Define Volumes", "Map Volumes", and "Summary". The main content area has a header "Set SAS Switches Date and Time" and a sub-header "If you use NTP, set the SAS Switches to use your NTP server". Below this, it states "The current time (UTC) on SAS Switches is: 3/6/13 4:25 PM". There are two radio button options: "Set SAS Switches time now" (which is selected) and "Set up SAS Switches to use NTP server:". The "Set up SAS Switches to use NTP server:" option has two input fields for "Primary server:" and "Secondary server:". Below these is another radio button option: "Set SAS Switches current date and time now". This option has a description: "Enter your local date/time. The date/time will be saved as the UTC value displayed below." It includes input fields for "Date:" (showing "3/7/13") and "Time:" (showing "3:27 AM"). At the bottom of the main content area, it displays "Date/Time(UTC): 3/6/13 4:27 PM UTC". At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 4-22 SAS Switch time source

4. Set the date and time for the RAID subsystem. Unlike the SAS switch subsystem, the RAID Subsystem does *not* support an NTP server. You must either set its time according to the SAS switch as shown in Figure 4-23, or manually specify its time. Click **Next** when done.

Tip: Generally, set the RAID controller's time according to the SAS Switch.

Set RAID Subsystem Date and Time
Set the RAID Subsystem current time using one of the options below.

The current date/time (UTC) on the RAID Subsystem is: 3/6/13 11:15 AM

☒ **Set RAID Controller current date and time now**

☐ Set with current SAS Switch time

☐ Manually set date and time:
Enter your local date/time. The date/time will be saved as the UTC value displayed below

Date:

Time:

Date/Time(UTC):

< Back Next > Finish Cancel

Figure 4-23 Setting the SAS RAID Controller time source


5. The Modify SAS Switches Passwords pane (Figure 4-24) allows you to change the default password for the built-in USERID accounts. It is advisable to do so.

If two modules are present, select **Change passwords on both modules** and click **Change Password**. Click **Next** to proceed.

Multiple user IDs are used for redundancy. If the password for the primary account is lost, the additional user IDs provide a fall back. Otherwise, the controller must be reset to factory defaults, which erases the current configuration. At the time of writing, there is no way to disable the additional user IDs.

Modify SAS Switches Passwords

This step is optional, but it is important that you change the default passwords for all user IDs.

 Passwords must be 8 to 16 characters and must contain at least one number and one letter. Enter the current password to change a lower level password.

Current Password:

	New Password	Confirm Password
USERID	<input type="password" value="....."/>	<input type="password" value="....."/>
USERID1	<input type="password" value="....."/>	<input type="password" value="....."/>
USERID2	<input type="password" value="....."/>	<input type="password" value="....."/>
USERID3	<input type="password" value="....."/>	<input type="password" value="....."/>

Apply Changes

☒ Change passwords on the module in I/O Bay 3

☐ Change passwords on the module in I/O Bay 4


☐ Change passwords on both modules

Figure 4-24 Modify SAS Switch Passwords pane

6. The Modify RAID Subsystem Passwords pane (Figure 4-25) allows you to change the default USERID account password of the RAID Subsystem. The password change applies to both RAID Subsystems if two modules are installed. Click **Change Password** and **Next** to proceed.

Modify RAID Subsystem Passwords

This step is optional, but it is important that you change the default password.

 The password must be 8 to 16 characters and must contain at least one number and one letter.

	Current Password	New Password	Confirm Password
USERID	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 4-25 Modify RAID Subsystem Passwords pane

7. The Configure Storage pane (Figure 4-26) provides a number of options to begin the storage configuration process:
- Use an existing configuration on the SAS RAID Controller Module.
 - Use a backup configuration file that was previously saved with Storage Configuration Manager. Use this option to restore a previous SAS RAID Controller Module backed-up state.
 - Create a custom configuration in which you either allow Storage Configuration Manager to select the appropriate drives in the Disk Storage Modules, or manually select the drives yourself.

The example uses a custom configuration that allows the SAS RAID Controller Module to select the disks. Click **Next**.

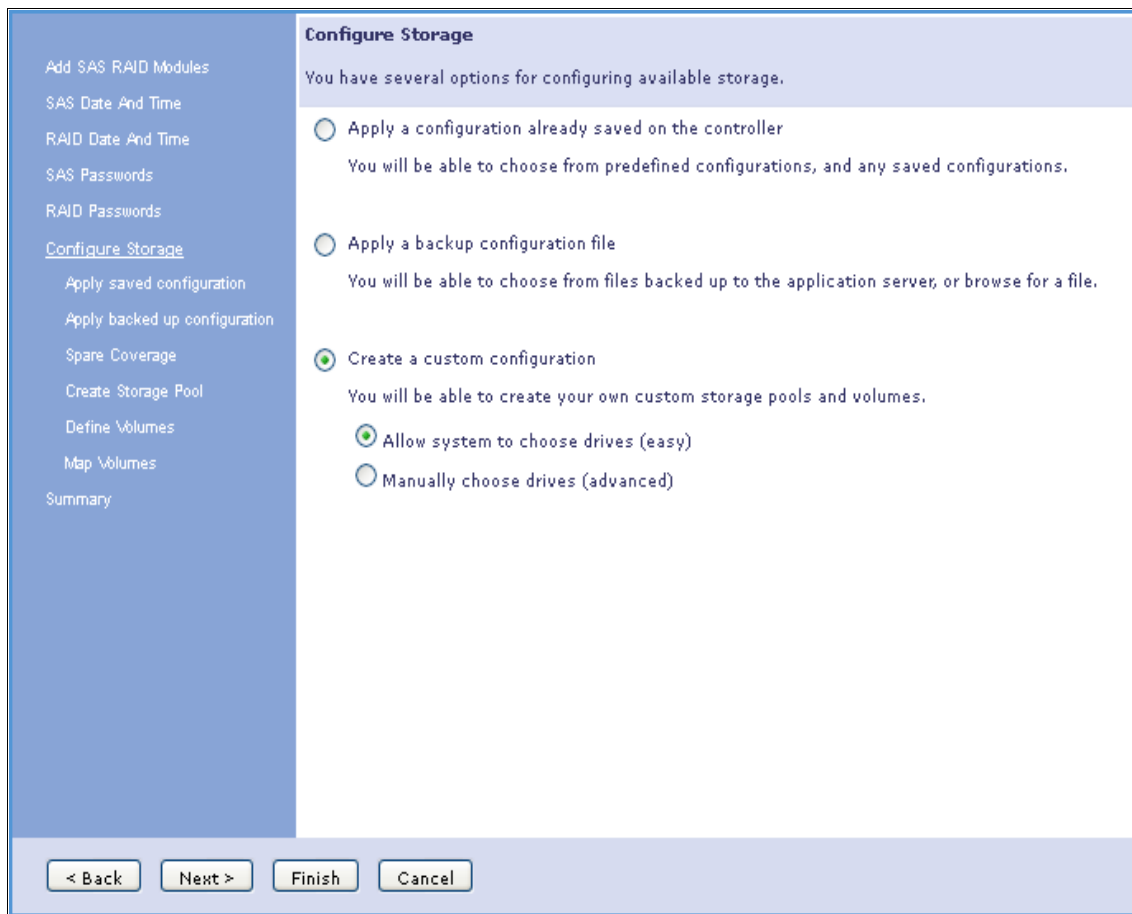


Figure 4-26 Configure Storage pane

8. The Spare Disk Drive Coverage pane (Figure 4-27) allows you to allocate a redundant global hot spare in the case of drive failure. Available disk drive capacity is reduced, but this configuration provides greater fault tolerance.

You can use the Initial Setup Wizard to select up to two global spare disks per drive type, providing you have sufficient capacity. You can change the number of global spare disks at a later stage, if required. The example selects **No** global spare disks.

Global spare: A larger global spare drive can provide fault tolerance for drives of a lower capacity, if required. It is also worth noting that a global spare provides protection across both Disk Storage Modules.

Spare Disk Drive Coverage

Select the amount of required spare disk drive coverage. Choosing the number of spare disk drives is a balance between redundancy and usable capacity.

Global spare drives can help retain redundancy in the event of multiple drive failures, but the amount of usable capacity for data storage is reduced.

Select the required number of global spare disk drives for each drive type:

Drive Type	Global Hot Spares	Enable Auto Copyback
136.732 GB 15 K SAS	0	<input type="checkbox"/>
279.396 GB 15 K SAS	0	<input type="checkbox"/>

< Back Next > Finish Cancel

Figure 4-27 Spare Disk Coverage pane

Bug with Next and Back buttons: During testing, clicking **Next** and then **Back** from the Spare Drive Coverage Page assigned a new global spare each time. Although this is a default setting, clicking **Back** did not free the previous assigned spare.

9. The Storage Pool creation pane (Figure 4-28) allows you to create a single storage pool to get you started. You can create more storage pools at a later stage. To create a storage pool, complete these steps:
 - a. Select a name to assign to the storage pool
 - b. Select the disk type that you want to use to create the storage pool.
 - c. Select the required RAID level. You have a choice of RAID 0,1,5, or 10.
 - d. The minimum and maximum storage pool capacity is based on the RAID level selected. Select the number of disks from the **Available Disk Drives**, then click **Add**. The drives are displayed in the added Disk Drives section. The example uses RAID 5 and all three available 136 GB drives.
 - e. Click **Next**.

Create Storage Pool
Based on RAID level, select drives and add to the new storage pool until the required capacity is reached. Click Next to create the storage pool.

* Storage pool name: Minimum number of disks: 3
Required disk type: Added number of disks: 4
Required RAID level: Total new pool capacity: 358.495 GB
Remaining system capacity: 1,956.072 GB

Available Disk Drives:

Capacity (GB)	Module	Bay
---------------	--------	-----

Added Disk Drives:

Capacity (GB)	Module	Bay
<input type="checkbox"/> 136.732	1	5
<input type="checkbox"/> 136.732	1	6
<input type="checkbox"/> 136.732	2	5
<input type="checkbox"/> 136.732	2	6

Add >> << Remove

Selected: 0

< Back Next > Finish Cancel

Figure 4-28 Storage Pool creation pane

10. Figure 4-29 summarizes the storage pool that is about to be created. Click **OK** to create the pool.

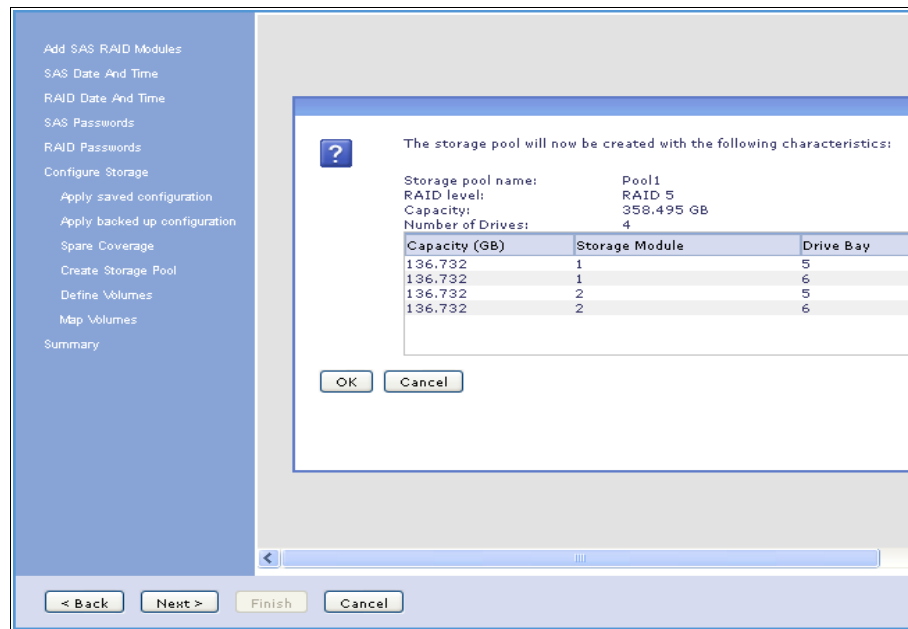


Figure 4-29 Storage Pool summary

11. After the pool is successfully created, a success status window is displayed as shown in Figure 4-30. Click **Next**.

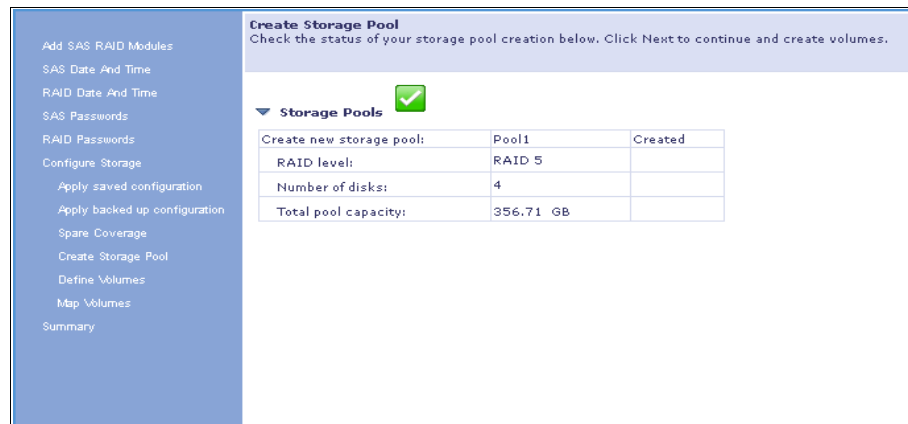


Figure 4-30 Storage Pool creation success

12. The Define Volumes pane (Figure 4-31) allows you to create single or multiple volumes from the storage pool created in the previous step. Specify a volume name, capacity for the volume to be created, and the quantity of volumes if you want to create identically sized volumes.

When you create multiples of the same volume, a suffix is added to the end of the volume name. In the example, three volumes are created, each being 111 GB in size. Click **Next** after you create the necessary volumes.

Tip: Do not attempt to select the exact available amount in the Define Volumes pane, as the volume creation will fail. This is because the volume writes its configuration data onto the Storage Pool. Without this space, the volume creation cannot complete successfully.

If you want to create a single volume from the entire storage pool, select an amount marginally less than the specified available amount.

Define Volumes
Define volumes and add them to the list of volumes to create. The volumes can be for the same or different hosts. You can map the volumes to the correct host in the next step.

Storage pool: Pool1 Capacity: 356.71 GB

RAID level: RAID 5

Volume Definition

*Name:

*Capacity (GB):

*Quantity:

Name suffix:

Example volume name (name + suffix):

New Volumes

	Capacity (GB)	Name
<input checked="" type="checkbox"/>	111	Volume011
<input type="checkbox"/>	111	Volume012
<input type="checkbox"/>	111	Volume013

Navigation: < Back Next > Finish Cancel

Figure 4-31 Volume definition pane with assigned volumes

13. To use the volumes, they need must be mapped to blade server. In Figure 4-32, the three example volumes are present but they are not mapped to any hosts. In fact, no hosts are present yet. SCM must find valid hosts to assign to a volume. Click **Discover Hosts**.

Discovery prerequisites: For Storage Configuration Manager to discover a valid host, the following must be true about the blade servers:

- ▶ A SAS Connectivity Card that is installed in the CIOv slot of the server.
- ▶ The server must be powered on.

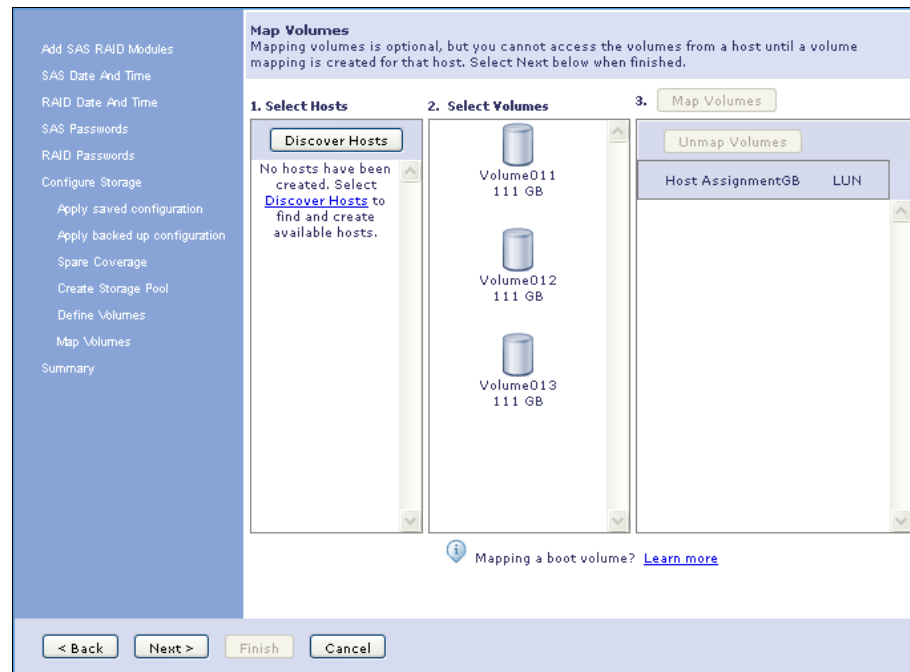


Figure 4-32 Unassigned volumes in SCM.

14. Figure 4-33 shows a summary of the discovered hosts available hosts. Click **Close**.

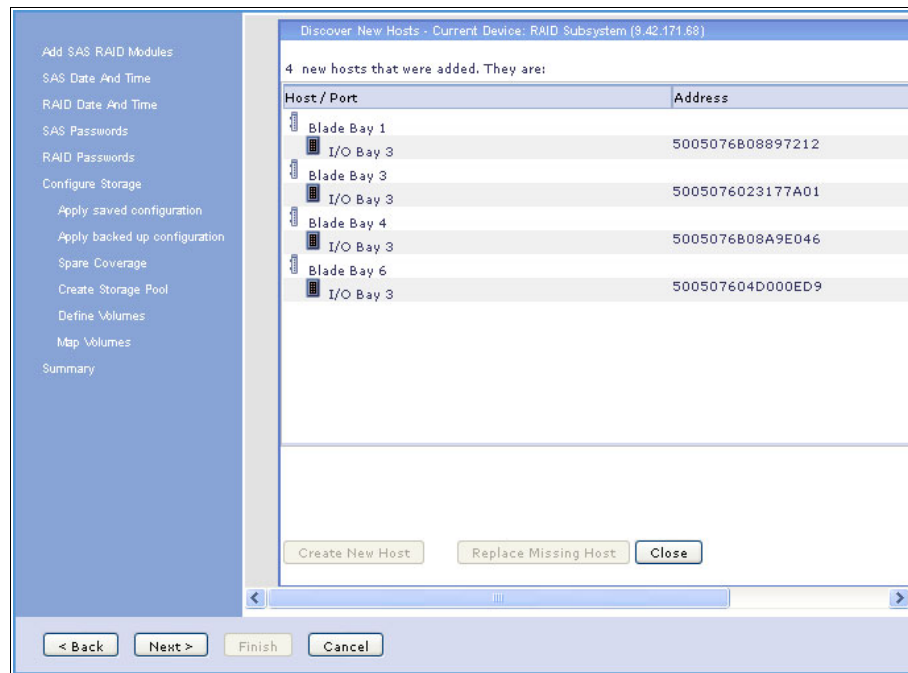


Figure 4-33 Discovered hosts available for volume assignment

- To map a volume, select the required blade and volume, then click **Map Volumes**. It is possible to map a volume to a blade after the wizard has completed.

Figure 4-34 shows the assigned blade and volume for the example configuration. Click **Next** to proceed.

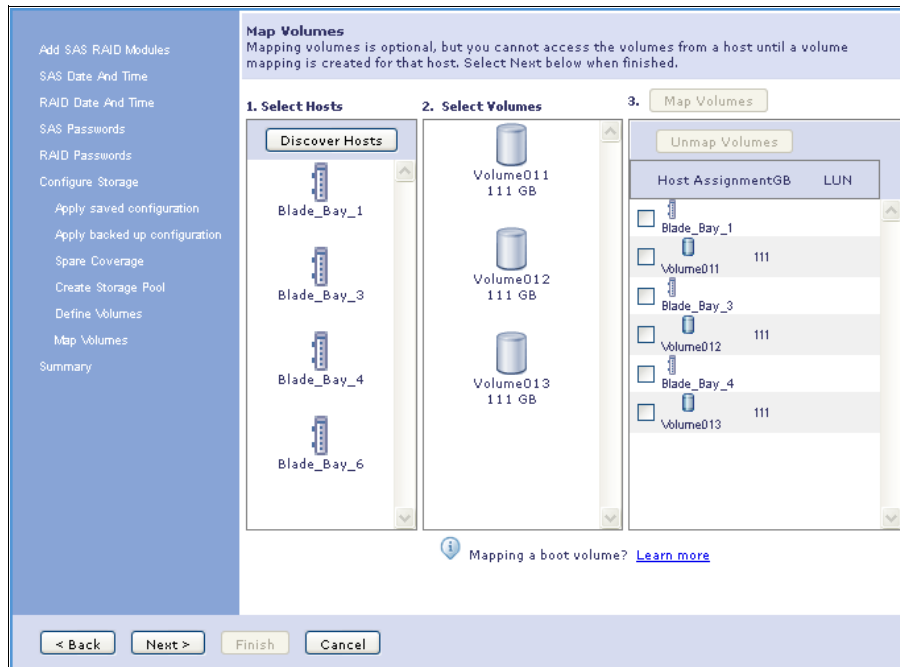


Figure 4-34 Mapped volumes to blade servers

15. The Summary pane (Figure 4-35) allows you to review your selections. When ready, click **Finish**. This runs the necessary tasks to finalize the volumes and mappings.

The screenshot shows a software configuration window with a left-hand navigation pane and a main summary area. The navigation pane lists the following steps: Add SAS RAID Modules, SAS Date And Time, RAID Date And Time, SAS Passwords, RAID Passwords, Configure Storage, Apply saved configuration, Apply backed up configuration, Spare Coverage, Create Storage Pool, Define Volumes, Map Volumes, and Summary (which is currently selected). The main area is titled 'Summary' and contains the instruction 'Verify configuration and then select Finish to start, or go back to make any required changes.' Below this, there are four items, each with a right-pointing triangle icon and a green checkmark: 'SAS RAID Modules Added', 'SAS Switch Date and Time', 'Spare Reserved', and 'Storage Pools'. A section titled 'Define Volumes' is expanded, showing a table with the following data:

Capacity (GB)	Name	Status
111	Volume011	Pending
111	Volume012	Pending
111	Volume013	Pending

Below the table, there is a section titled 'Volume to Host Mapping' which is currently collapsed. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 4-35 Configuration summary

16. A final window is displayed when all the tasks are complete as shown in Figure 4-36. This concludes the Initial Setup Wizard for the SAS RAID Controller Module(s).

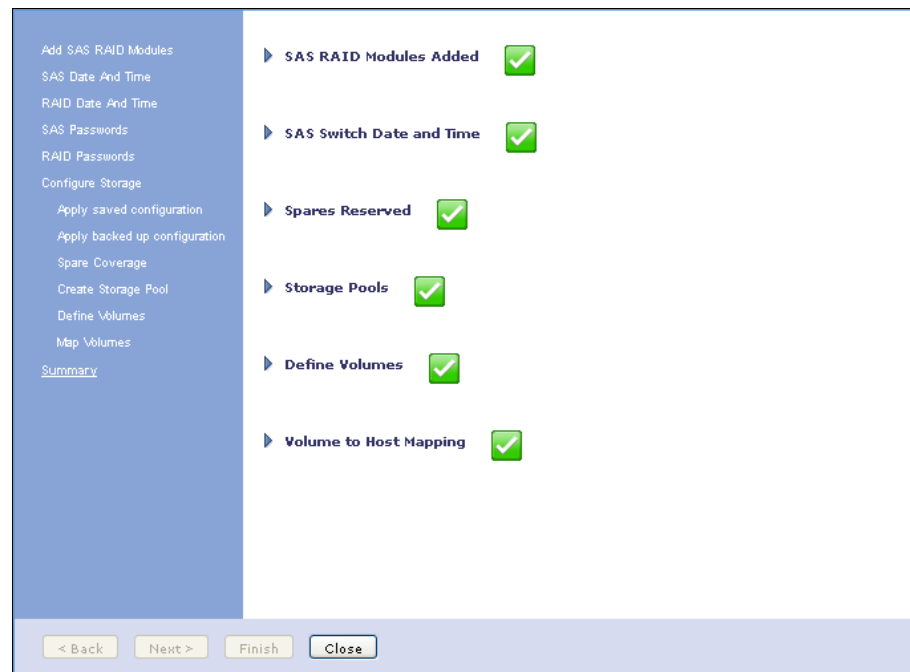


Figure 4-36 SCM wizard completion for SAS RAID Controller

4.5.4 Initial Configuration Wizard for the SAS Connectivity Module

You can use the Initial Configuration Wizard to perform basic operations that are required to add the SAS Connectivity Module into the Storage Configuration Manager console. To begin the configuration process, complete these steps:

1. Click **BladeCenter SAS Connectivity Module** on the **Getting Started** window, and select the **Initial Configuration Wizard**, as seen in Figure 4-37.

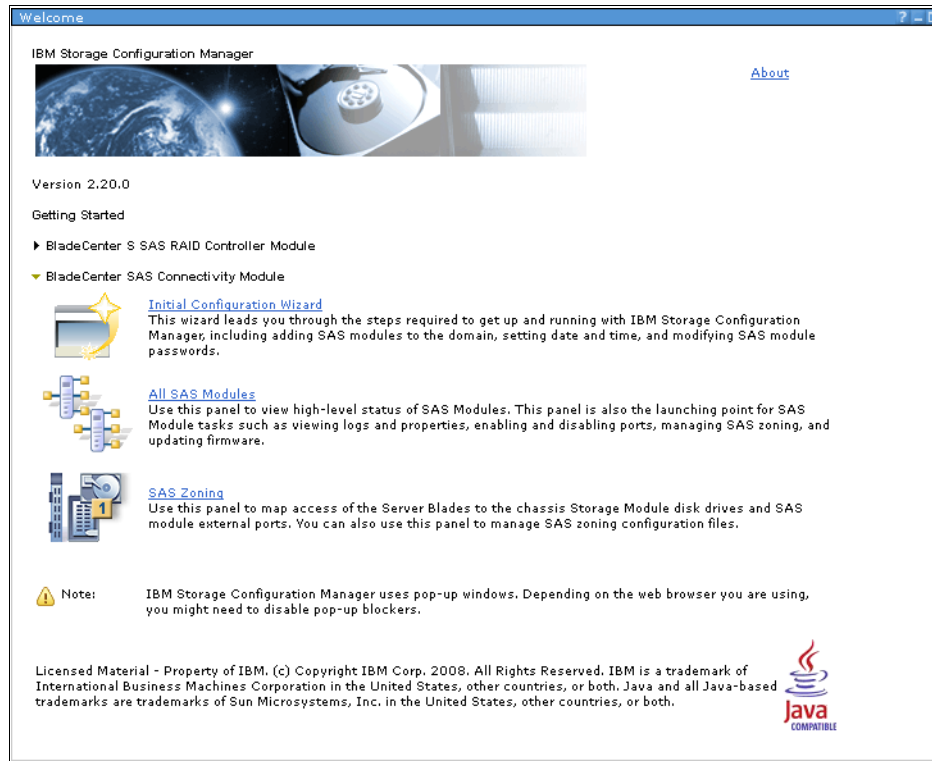


Figure 4-37 SAS Connectivity Module Initial Configuration Wizard

2. The pane shown in Figure 4-38 is displayed, informing you of the tasks that are available by using this wizard. Click **Next**.

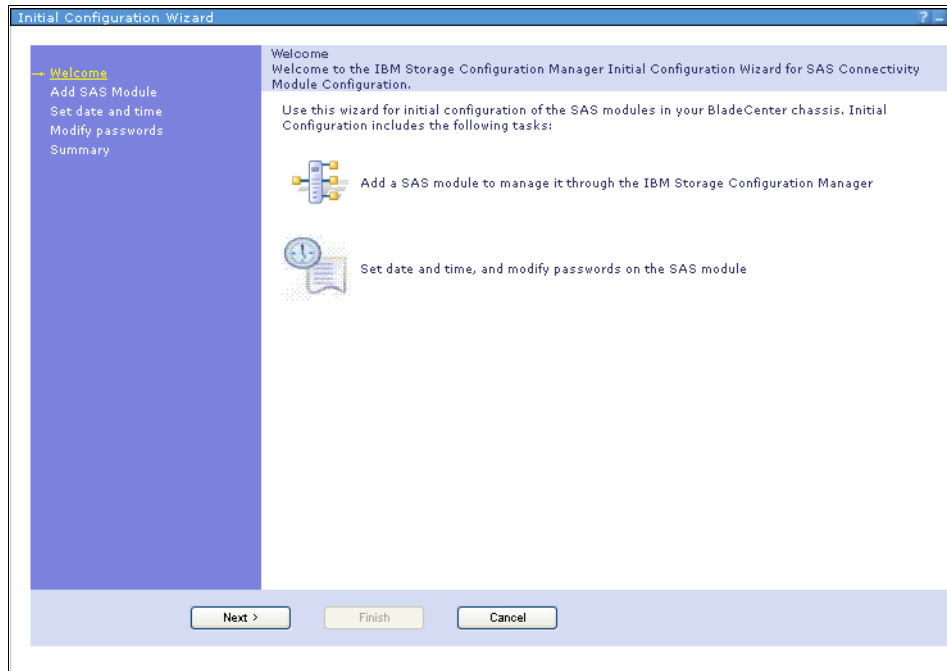


Figure 4-38 SAS Connectivity Module Welcome pane

3. The Add SAS Module window is displayed. Here you add the SAS modules to SCM. You need the IP addresses of your SAS modules, and the user account and password to authenticate to them. To add the SAS modules, complete these steps:
 - a. Enter the IP address, nickname, user account, and password of the first SAS module in the relevant fields and click **Add SAS Module** as shown in Figure 4-39.

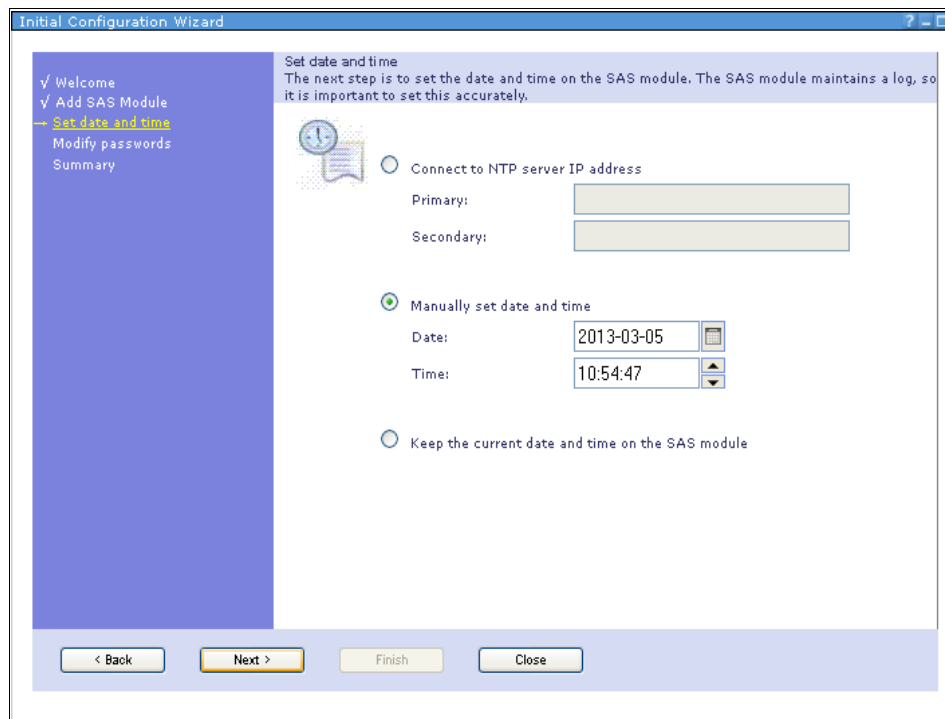
Note: Nickname must not exceed 16 characters.

The screenshot shows a window titled "Initial Configuration Wizard" with a sidebar on the left containing a tree view with the following items: "Welcome", "Add SAS Module" (highlighted with a yellow arrow), "Set date and time", "Modify passwords", and "Summary". The main area of the window is titled "Add SAS Module" and contains the following text: "The first step is to register your SAS module with IBM Storage Configuration Manager. Enter this information only once. If two SAS modules are installed in your chassis, enter the information for the first SAS module, click Add SAS Module, then enter the information for the second SAS module and click Add SAS Module again." Below this text are several input fields: "Identifier" (with a help icon), "* SAS Module IP Address:" (containing "9.42.171.67"), "Nickname:" (containing "SAS 3"), "Login" (with a help icon), "User ID:" (containing "USERID"), and "* Password:" (containing "*****"). An "Add SAS Module" button is located below the password field. At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Close".

Figure 4-39 Add SAS Connectivity Module pane

- b. If you have a second SAS module, enter its IP address, nickname, user account, and password in the relevant fields and click **Add SAS Module**.
 - c. Click **Next** when done.

4. On the Set date and time pane (Figure 4-40), enter a Network Time Protocol (NTP) time server if you have one on your network, and enter the date and time to be applied to both switches. Click **Next** when done.



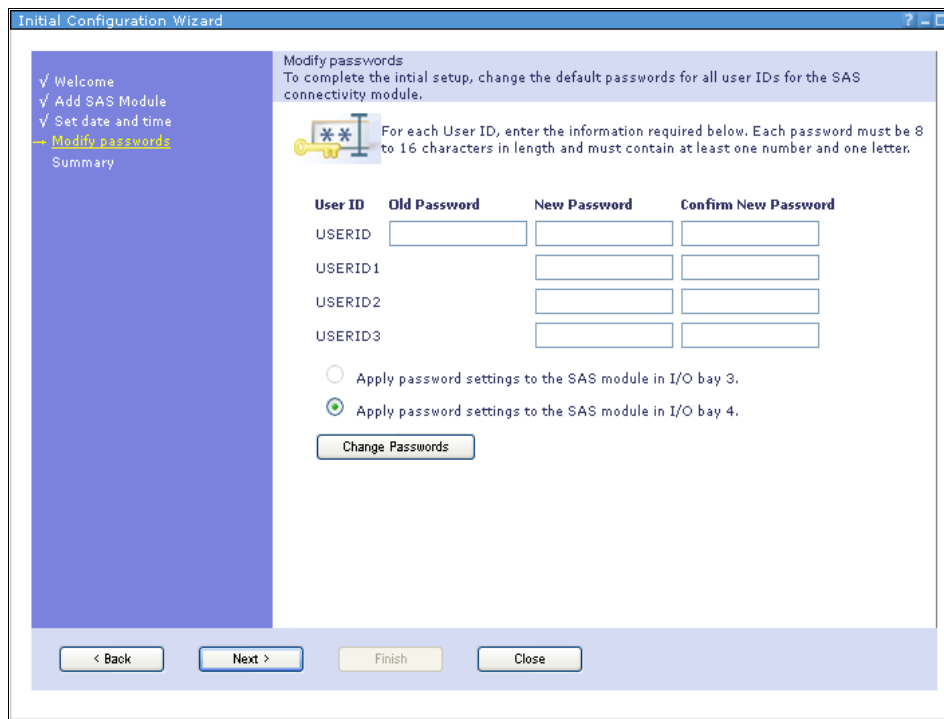
The screenshot shows the 'Initial Configuration Wizard' window. On the left is a blue sidebar with a list of steps: 'Welcome', 'Add SAS Module', 'Set date and time' (highlighted with a yellow arrow), 'Modify passwords', and 'Summary'. The main area has a title 'Set date and time' and a subtitle 'The next step is to set the date and time on the SAS module. The SAS module maintains a log, so it is important to set this accurately.' Below this is a clock icon. There are three radio button options: 'Connect to NTP server IP address' (with 'Primary:' and 'Secondary:' text boxes), 'Manually set date and time' (selected, with 'Date:' and 'Time:' text boxes), and 'Keep the current date and time on the SAS module'. The 'Date' box contains '2013-03-05' and the 'Time' box contains '10:54:47'. At the bottom are four buttons: '< Back', 'Next >' (highlighted with a yellow border), 'Finish', and 'Close'.

Figure 4-40 Setting the date and time

5. On the Modify passwords pane (Figure 4-41), modify the default USERID account password. You can also create more accounts. Specify on which switch you want the password changes to take place. Click **Next**.

Notes:

- ▶ The user names are USERID, USERID1, USERID2, and USERID3. These are fixed and cannot be changed.
- ▶ To ensure consistency, change the passwords on both SAS modules.



The screenshot shows the 'Initial Configuration Wizard' window. On the left is a blue sidebar with a list of steps: 'Welcome', 'Add SAS Module', 'Set date and time', 'Modify passwords' (highlighted with a yellow arrow), and 'Summary'. The main area has a title 'Modify passwords' and a subtitle 'To complete the initial setup, change the default passwords for all user IDs for the SAS connectivity module.' Below this is a yellow key icon and a text box stating: 'For each User ID, enter the information required below. Each password must be 8 to 16 characters in length and must contain at least one number and one letter.' A table with four columns follows: 'User ID', 'Old Password', 'New Password', and 'Confirm New Password'. The rows are for 'USERID', 'USERID1', 'USERID2', and 'USERID3'. Each row has input fields for the 'New Password' and 'Confirm New Password' columns. Below the table are two radio buttons: 'Apply password settings to the SAS module in I/O bay 3.' (unselected) and 'Apply password settings to the SAS module in I/O bay 4.' (selected). A 'Change Passwords' button is below the radio buttons. At the bottom of the window are four buttons: '< Back', 'Next >', 'Finish', and 'Close'.

User ID	Old Password	New Password	Confirm New Password
USERID			
USERID1			
USERID2			
USERID3			

Figure 4-41 Modifying the default passwords

6. Review your selections on the Summary window as shown in Figure 4-42. If required, you can go back to change a setting. Click **Finish** when done.

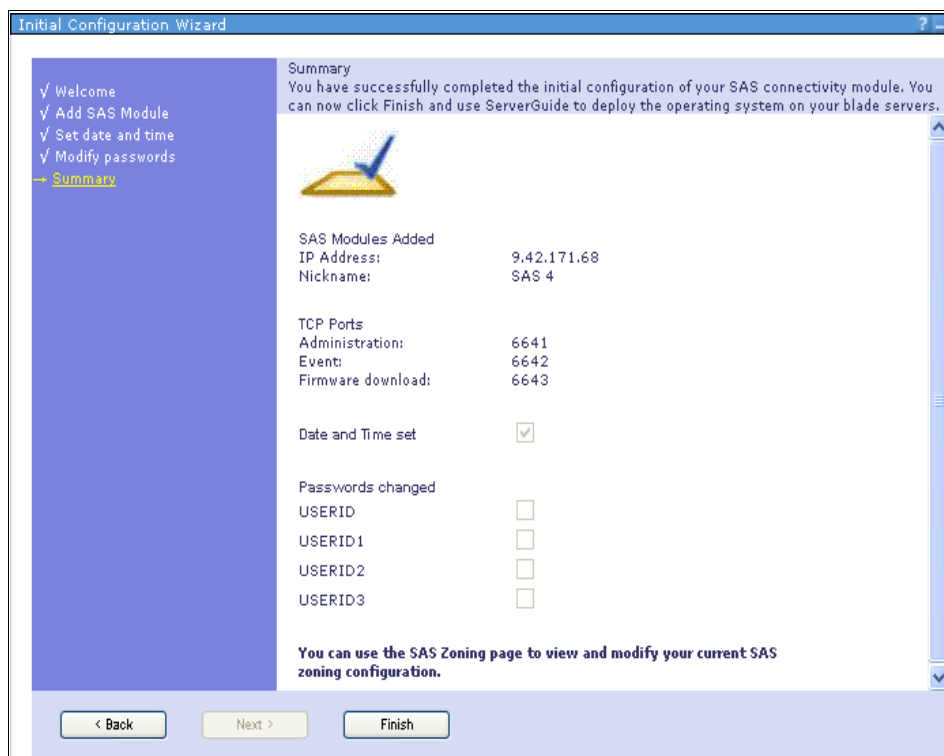


Figure 4-42 Information summary window

7. After you complete the Initial Configuration Wizard, click **BladeCenter SAS Module** → **Health** → **All SAS Modules** to see a quick overview of the SAS module health, as seen in Figure 4-43.

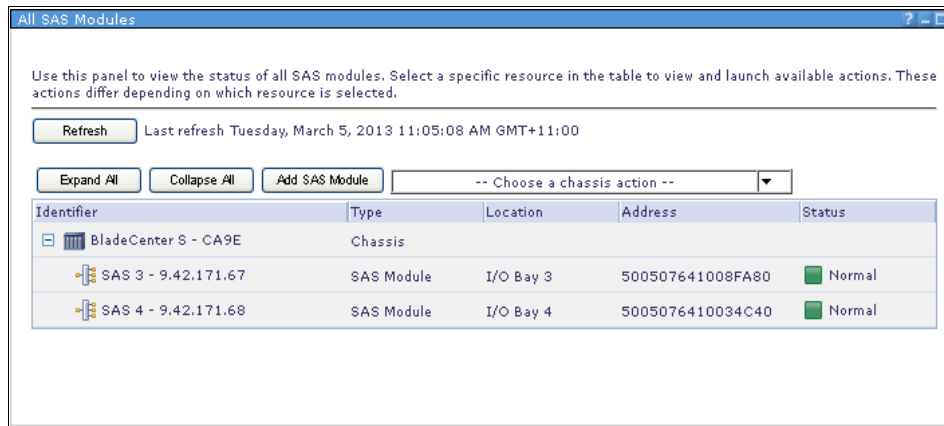


Figure 4-43 SAS module health status window

4.5.5 User-defined and zone configurations

This section applies to the SAS Connectivity Module only.

SCM provides the simplest method of creating user-defined zone configurations for the SAS Connectivity Module. User-defined configurations allow you to go beyond the confines of the predefined configurations and create your own access structure to disks and external ports.

Creating a user-defined zone configuration

To create a user-defined zone configuration, complete these steps:

1. Click **BladeCenter SAS Module** → **Configuration** → **SAS Zoning** for the SAS Connectivity Module. The window shown in Figure 4-44 is displayed.

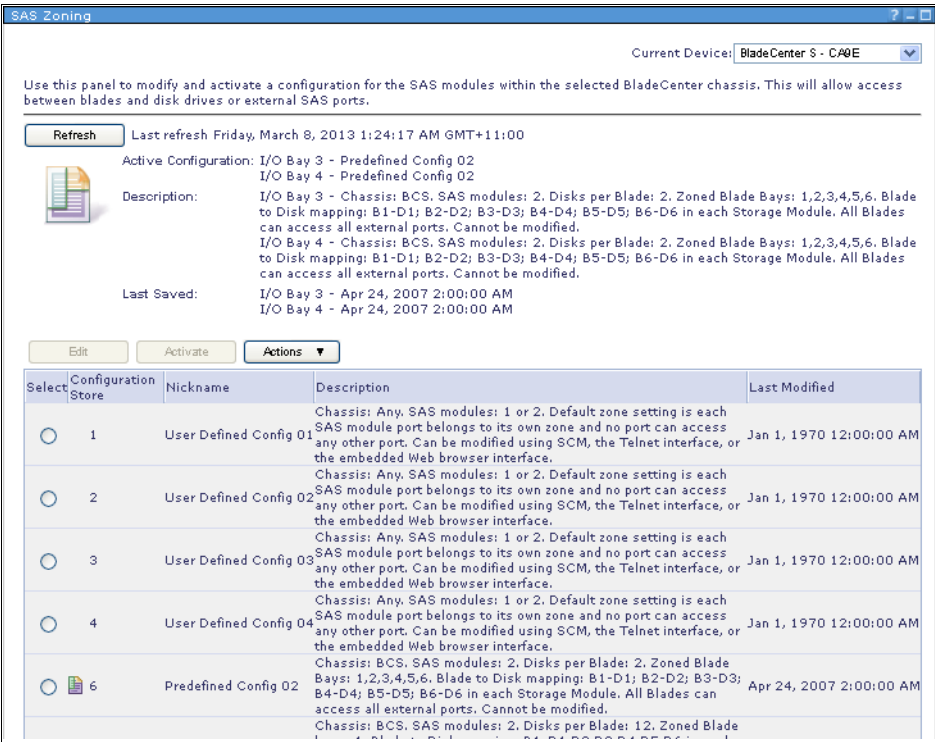


Figure 4-44 SAS Access zone configuration selection window

2. Select one of the User Defined Configs, which are User Defined Config 1, 2, 3, or 4, and then click **Edit**. The SAS Zoning - Edit window is displayed as seen in Figure 4-45.

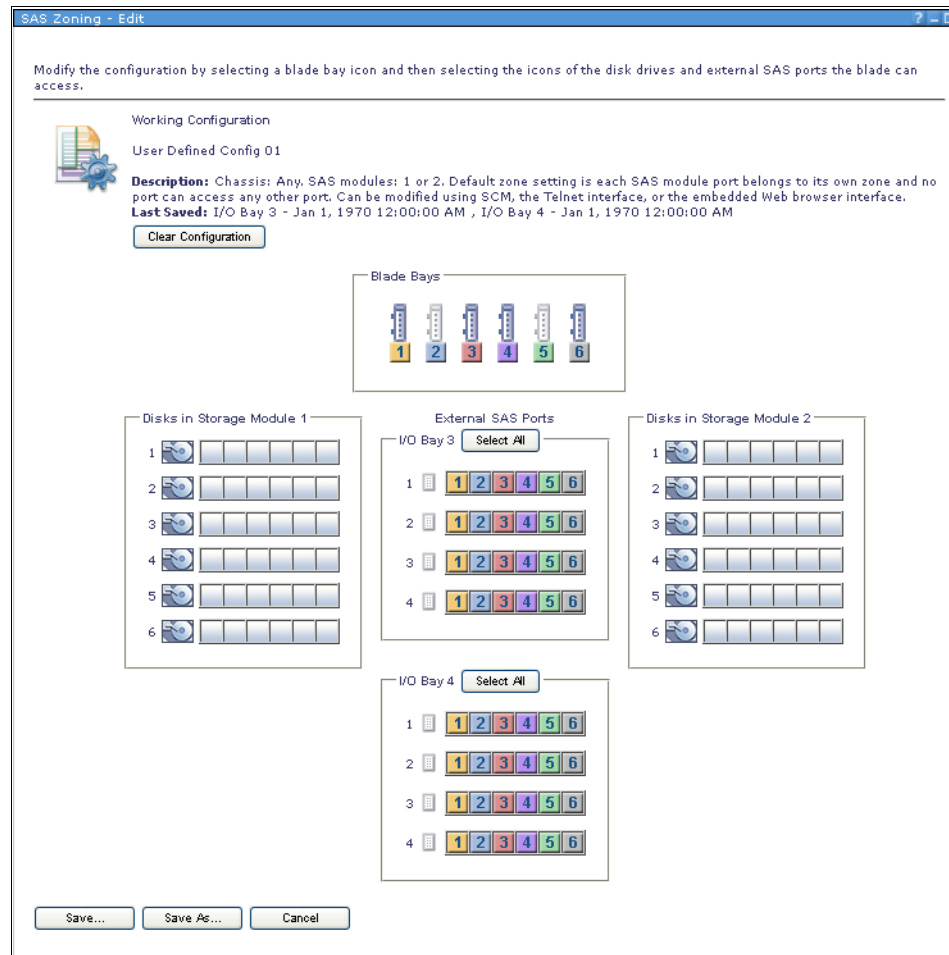


Figure 4-45 SAS Zoning - Edit window

3. Each Blade bay is assigned a color and number. You then assign these to whatever resource you want to define to each blade. The example in Figure 4-45 uses these assignments:
 - Blade 4 is configured to access all external ports on SAS Connectivity Module 3 and 4 and has no access to any disk.
 - Blade 1 has access to all external ports on SAS Connectivity Module 3 and 4, and has no access to any disk.

4. You can clear the previous settings by clicking **Clear Configuration**. This allows you to begin with a clean configuration for User Defined Config 1, as shown in Figure 4-46.

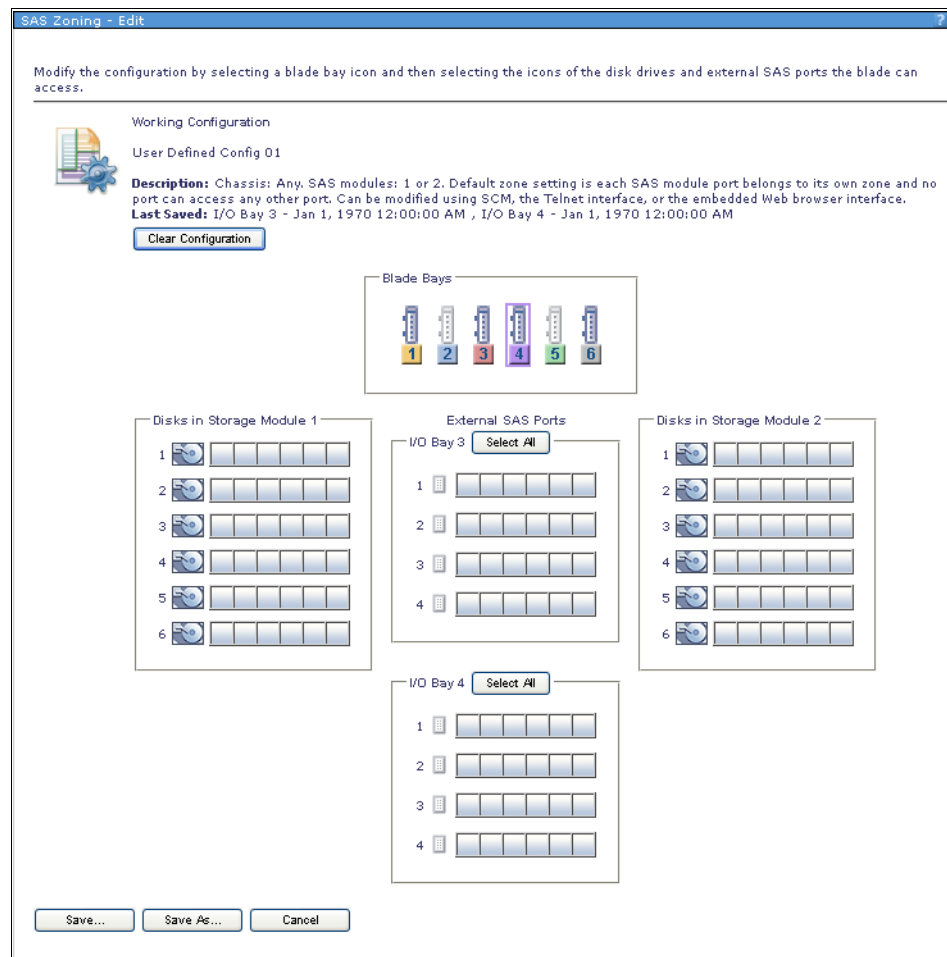


Figure 4-46 A cleared configuration

5. All of the blades are numbered in the order that they appear in the BladeCenter S chassis.

To allow a blade access to a disk in either Storage Module 1 or 2, complete these steps:

- a. Click the required blade number in the Blade Bays box and ensure it is highlighted.
- b. Select the required disk that you want to allow the blade to access by clicking the **Disk** icon next to the number of the disk in the required storage module.

To allow a blade access to an External Port in either I/O Bay 3 or 4:

- a. Click the required blade number in the Blade Bays box.
- b. Select the external port that you require the blade to have access to by clicking the **External Port** icon next to the number of the external port in the required I/O Bay.

- c. In the example configuration shown in Figure 4-47, the blades are assigned as follows:
- i. Blade 1 has access to Disk 1 in both storage units, and also exclusive access to the external SAS port 1 on both SAS connectivity cards.
 - ii. Blades 2 - 3 are assigned the same way, but to their corresponding blade number.
 - iii. As there are only four external ports on a SAS Connectivity card, Blades 5 and 6 do not have an assigned external SAS Port.

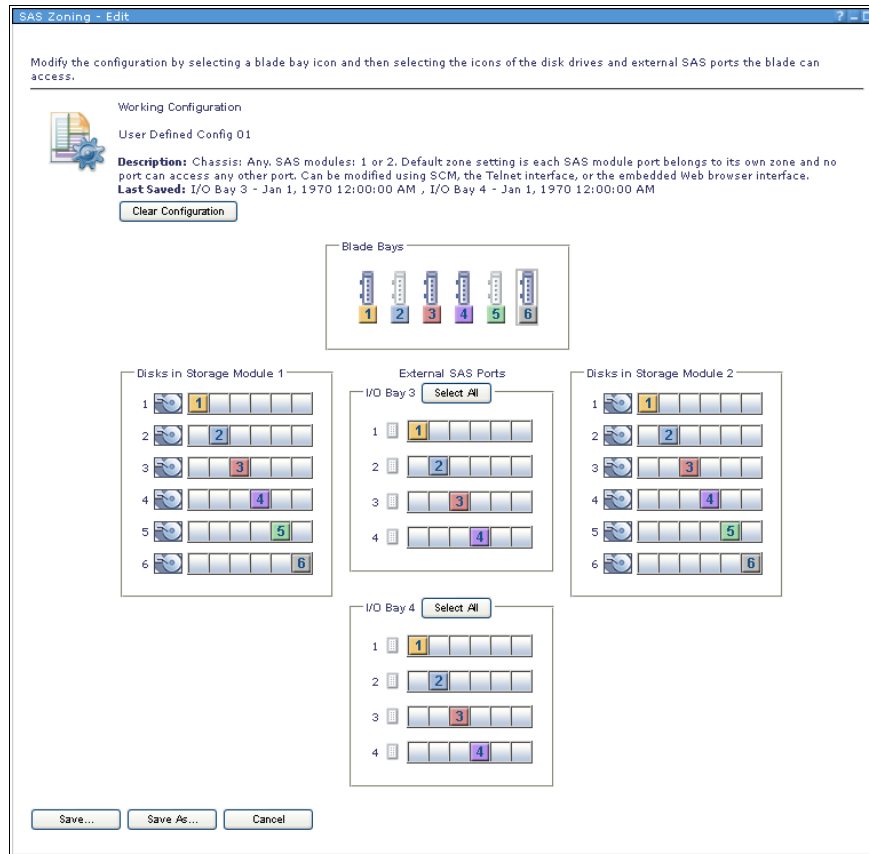


Figure 4-47 Example user defined configuration

6. After your drive allocation and external SAS ports are assigned, click **Save**. A dialog pane is displayed as shown in Figure 4-48 that asks if you want to confirm. Click **OK**.

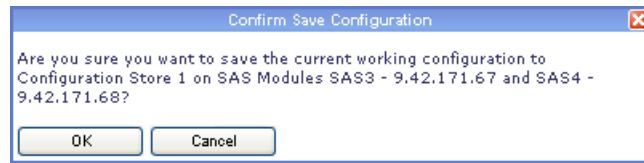


Figure 4-48 Saving a configuration

7. A summary page is displayed as shown in Figure 4-49 prompting you to give the configuration a meaningful name and description. After you are done, click **OK**.

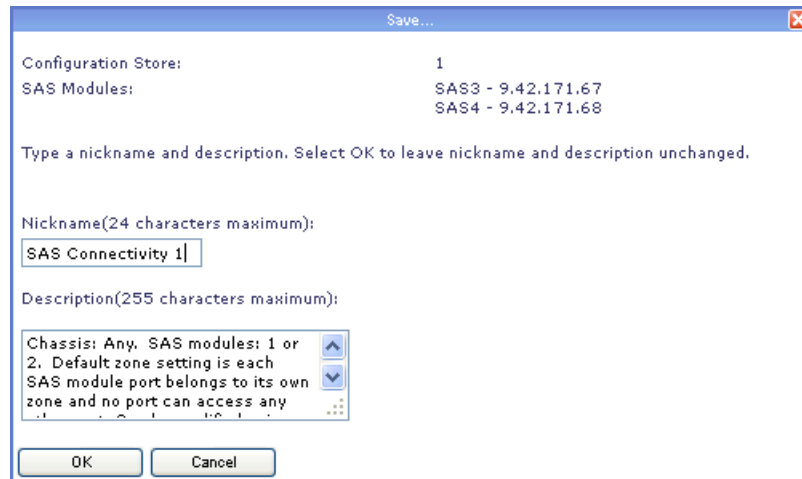


Figure 4-49 SAS Connectivity summary and save page

8. After it is saved, the SAS zoning window will display the new saved configuration. Figure 4-50 shows the saved configuration. The last step is to activate the zoning profile. Select a zone, and the **Activation** icon becomes active. Select it and click **OK**.

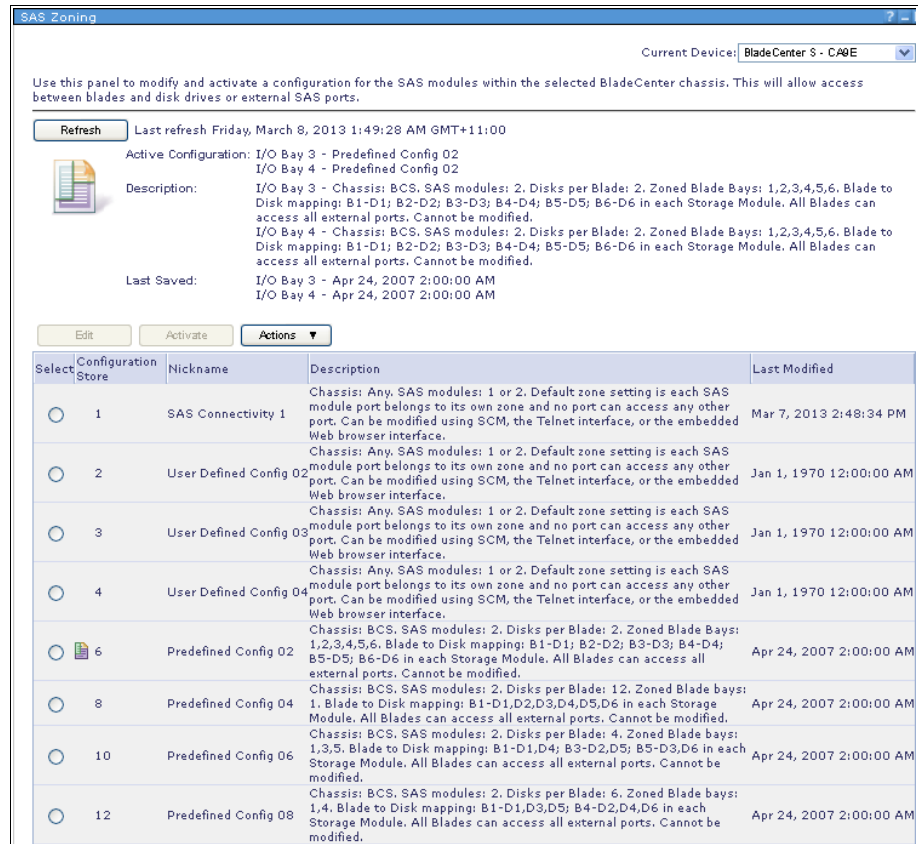


Figure 4-50 Saved configuration displayed in SAS Zoning

Note: The configuration is automatically applied to *both* SAS Connectivity Modules. This behavior is unlike the SAS Connectivity Module browser interface, where a configuration must be applied separately to each switch.

You must select an identical zone configuration for both SAS Connectivity Modules if you have two modules installed. Dissimilar zone configuration between the SAS Connectivity Modules is not supported.

SCM warns you if you have a zone configuration mismatch between the SAS Connectivity Modules when you attempt to alter zone configurations in the SAS

Zoning window. Zone mismatching is not possible using Storage Configuration Manager because it applies your selected zone configurations to each switch at the same time. You can, however, configure different zone configurations by using the SAS Connectivity Module browser interface or through the Storage Configuration of the AMM.

Backing up and restoring the configuration

Good business practice is to back up the BladeCenter SAS zoning. This is especially useful if you have a deployment program to roll out multiple BladeCenter S chassis with the same configuration.

Unlike the activation process, where the selected SAS Zone profile is applied to both SAS Connectivity Modules, a manual backup and restore is required for each card. This means that there will be two backup files: One for each SAS connectivity module.

Dual module configuration: For the SAS RAID Controller Module in a dual configuration, only one file must be backed up and restored because it is replicated between the two modules.

From the SAS Zoning page, select the configuration that you want to back up. Click **Actions** → **Backup**. In the example shown in Figure 4-51, the configuration file to be saved is for the SAS Connectivity Module in bay 3, with IP address 9.42.171.67. Repeat this step for the second SAS module.

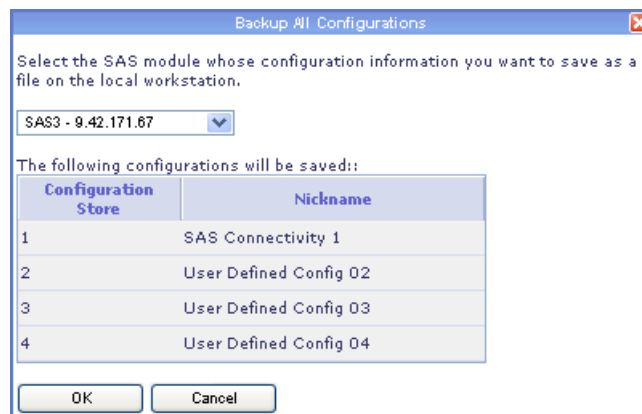


Figure 4-51 Confirmation that SAS Connectivity Module 3 configuration to be saved

To restore, click **Actions** → **Restore Configuration**. The window shown in Figure 4-52 is displayed. Select the backup file, then select the matching SAS Connectivity Module IP address for that backup. When done, click **Next**.

Restore Configuration

These two panels step through the process for restoring a previously saved zoning configuration to a configuration store on the selected SAS module.

Step 1

Specify the file path of the configuration file to be restored:

C:\Backups\sasconbay3.cfg

Step 2

Select the SAS module to which you want the configuration file restored:

SAS3 - 9.42.171.67

Figure 4-52 Restore file selection for SAS connectivity module in bay 3

The restore configuration is displayed in the next window where two selections must be made in steps 3 and 4. See Figure 4-53.

- ▶ Step 3. This lists configurations that were saved in the file. In the example, #1, SAS Connectivity 1 is selected
- ▶ Step 4. This lists the current configurations on the SAS Module in bay3 where the configuration will be restored to. In the example, #1, User defined Config 01 is selected.

The Restored configuration overwrites the configuration on the SAS Module. Select **Finish** when done.

Restore Configuration

These two panels step through the process for restoring a previously saved zoning configuration to a configuration store on the selected SAS module.

Step 3
Select the configuration in file sasconbay3.cfg to be restored to the SAS module.

Select	Configuration Store	Nickname
<input checked="" type="radio"/>	1	SAS Connectivity 1
<input type="radio"/>	2	User Defined Config 02
<input type="radio"/>	3	User Defined Config 03
<input type="radio"/>	4	User Defined Config 04

Step 4
Select the configuration store into which the restored configuration will be saved on SAS Module SAS3 - 9.42.171.67.

Select	Configuration Store	Nickname
<input checked="" type="radio"/>	1	User Defined Config 01
<input type="radio"/>	2	User Defined Config 02
<input type="radio"/>	3	User Defined Config 03
<input type="radio"/>	4	User Defined Config 04

Back Finish Cancel

Figure 4-53 Restore configuration location for SAS Connectivity Module

4.5.6 All Resources window

This section applies to the SAS RAID Controller Module only.

You can use the All Resources window to view all SAS RAID Controller Modules currently managed by Storage Configuration Manager. Depending on the item that is selected, it also provides you with links to most tasks available within the Storage Configuration Manager console. You can, for example, add SAS RAID Controller Modules without having to use the Initial Setup Wizard detailed in 4.5.3, “Initial Setup Wizard for the SAS RAID Controller Module” on page 197.

You can also remove SAS RAID Controller Modules from Storage Configuration Manager by using this window.

To view All Resources, click the BC-S SAS RAID Module → **Health** → **All Resources**, as shown in Figure 4-54.

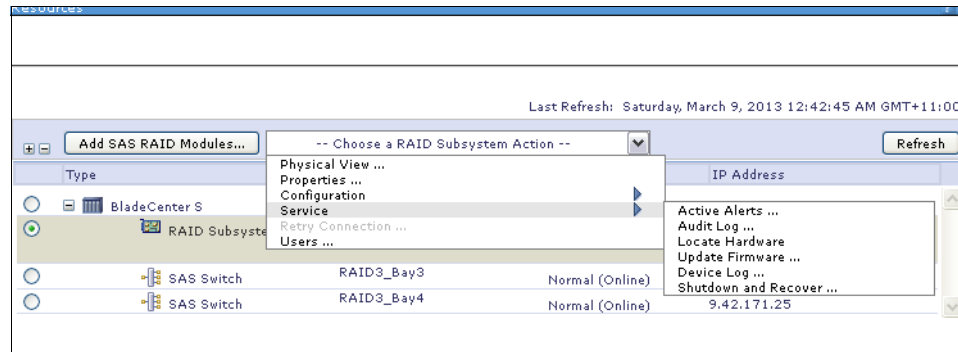


Figure 4-54 All Resources window

4.5.7 Physical View window

This section applies to the SAS RAID Controller Module only.

The Physical View window provides you with a physical view of a number of storage-related components that are installed in the BladeCenter S chassis. Like the All Resources window, the hardware component that you select determines the tasks available to you within the window.

To view the Physical View windows, click the BC-S SAS RAID Module → **Health** → **Physical View**.

As an example (Figure 4-55), select hard disk drive 6 in Disk Storage Module 1 by clicking the Drives tab and then clicking Disk 6. This disk is part of Pool1 that you configured earlier. To see the available actions you can perform against this disk, click **Select a Disk Action** → **Configuration**. The only task available is **Copyback to Replacement Drive**. You can locate this disk with its disk location light by clicking the **Select a Disk Action** → **Service** → **Locate Hardware**. These are just some of the many tasks available within this view.

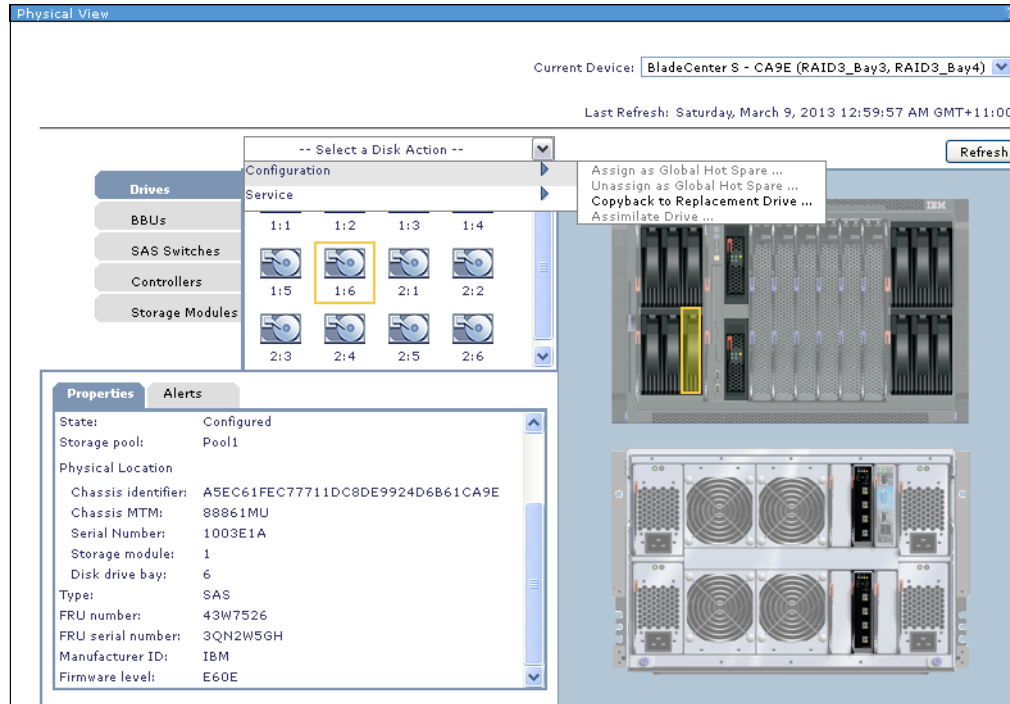


Figure 4-55 Physical View showing tasks available for the selected disk

4.5.8 Battery backup unit status and management

This section applies to the SAS RAID Controller Module only.

The battery backup units provide reserve power to the cache memory of the SAS RAID Controller Modules. This ensures that data still held in cache memory, which has not yet been committed to disk, is not lost in the event of a power failure to the chassis. There are two batteries, one for each SAS module.

Under normal operation or in the event of a power failure, you can view the reserve power of the battery backup units. To do this, open Storage Configuration Manager and click **BC-S SAS RAID Module** → **Physical View**. Click the BBUs

tab and click a battery backup unit (BBU) to view its status, as shown in Figure 4-56.

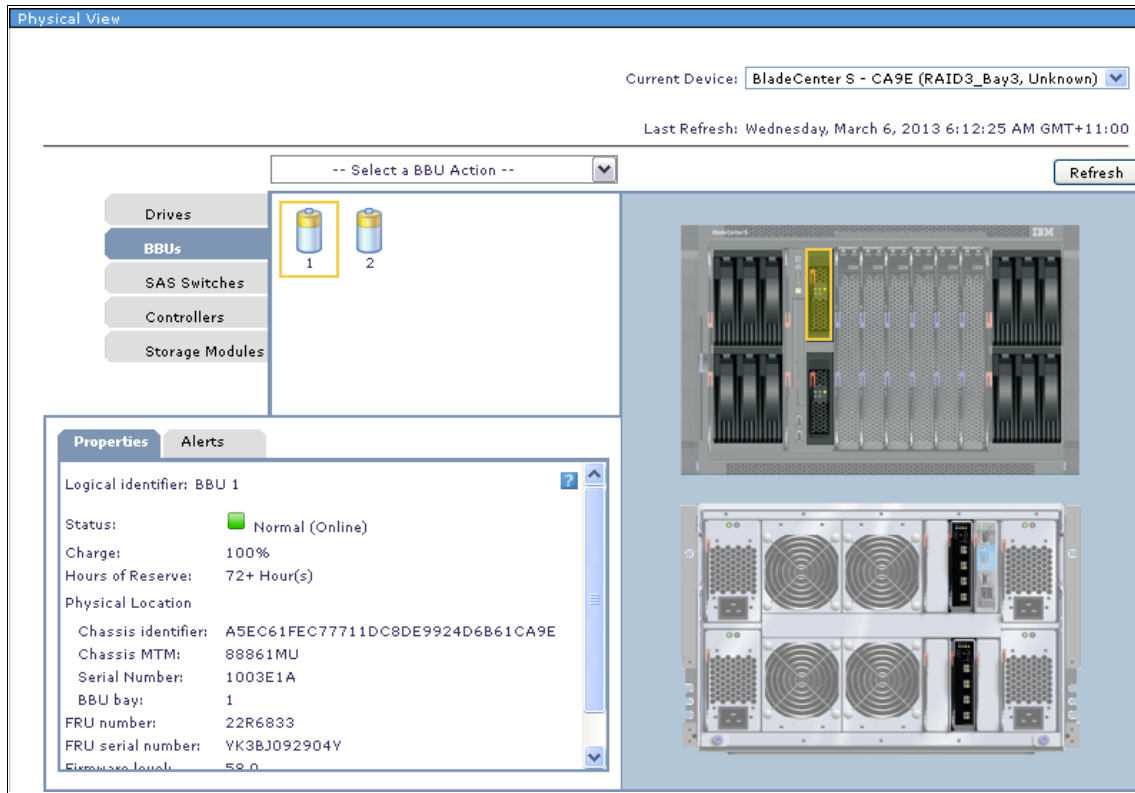


Figure 4-56 Battery Backup Unit properties

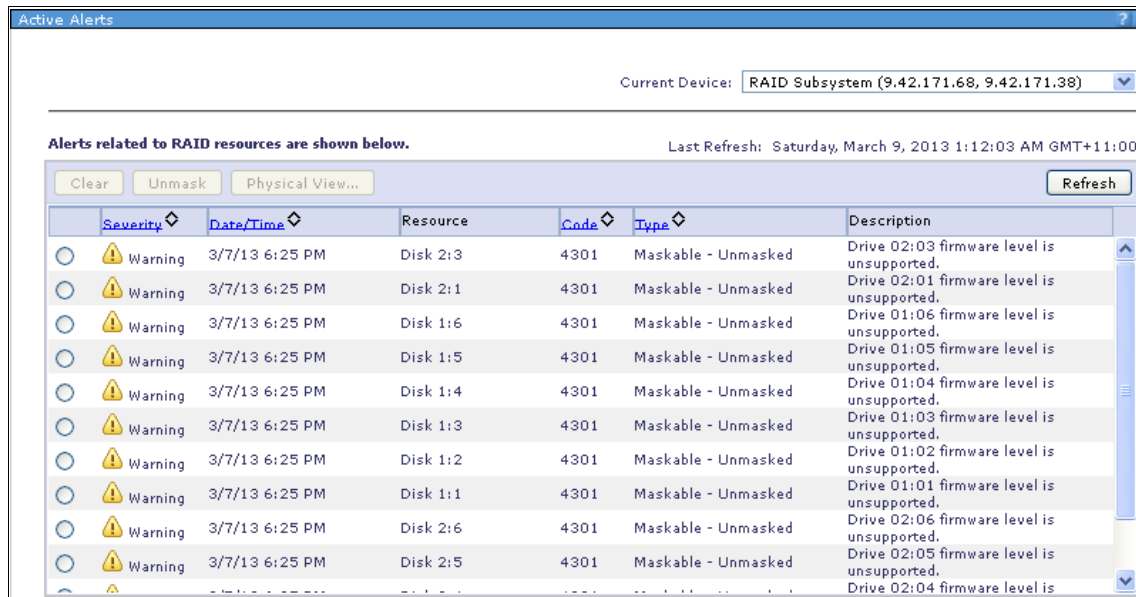
The Properties tab provides you with information about the numbers of hours of reserve power available per battery backup unit, its current charge state, and various other pieces of information.

4.5.9 Active Alerts window

This section applies to the SAS RAID Controller Module only.

The Active Alerts window provides you with a list of alerts related to the SAS RAID Controller Modules that are managed by Storage Configuration Manager. It also provides you with error codes and explanations related to those error codes to assist you with resolving any problems.

To view the Active Alerts window, click the BC-S SAS RAID Module → **Health** → **Active Alerts**, as shown in Figure 4-57.



The screenshot shows the 'Active Alerts' window with a title bar. Below the title bar, there is a 'Current Device' dropdown menu set to 'RAID Subsystem (9.42.171.68, 9.42.171.38)'. A message states 'Alerts related to RAID resources are shown below.' with a 'Last Refresh' timestamp of 'Saturday, March 9, 2013 1:12:03 AM GMT+11:00'. Below this, there are buttons for 'Clear', 'Unmask', 'Physical View...', and 'Refresh'. The main area contains a table with the following columns: Severity, Date/Time, Resource, Code, Type, and Description. The table lists ten warnings, all with a severity of 'Warning' and a date/time of '3/7/13 6:25 PM'. The resources are various disks (Disk 2:3, Disk 2:1, Disk 1:6, Disk 1:5, Disk 1:4, Disk 1:3, Disk 1:2, Disk 1:1, Disk 2:6, Disk 2:5). The code for all is '4301', and the type is 'Maskable - Unmasked'. The descriptions all state that a specific drive's firmware level is unsupported.

Severity	Date/Time	Resource	Code	Type	Description
Warning	3/7/13 6:25 PM	Disk 2:3	4301	Maskable - Unmasked	Drive 02:03 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 2:1	4301	Maskable - Unmasked	Drive 02:01 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:6	4301	Maskable - Unmasked	Drive 01:06 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:5	4301	Maskable - Unmasked	Drive 01:05 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:4	4301	Maskable - Unmasked	Drive 01:04 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:3	4301	Maskable - Unmasked	Drive 01:03 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:2	4301	Maskable - Unmasked	Drive 01:02 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 1:1	4301	Maskable - Unmasked	Drive 01:01 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 2:6	4301	Maskable - Unmasked	Drive 02:06 firmware level is unsupported.
Warning	3/7/13 6:25 PM	Disk 2:5	4301	Maskable - Unmasked	Drive 02:05 firmware level is unsupported.

Figure 4-57 Active Alerts window

4.5.10 Long Running Tasks window

This section applies to the SAS RAID Controller Module only.

The Long Running Tasks window allows you to view the progress of tasks that can take some time to complete. An example is the creation or initialization of a large volume, as seen in Figure 4-58.

To view the Long Running Task window, click the BC-S SAS RAID Module → **Jobs and Processes** → **Long Running Tasks**.

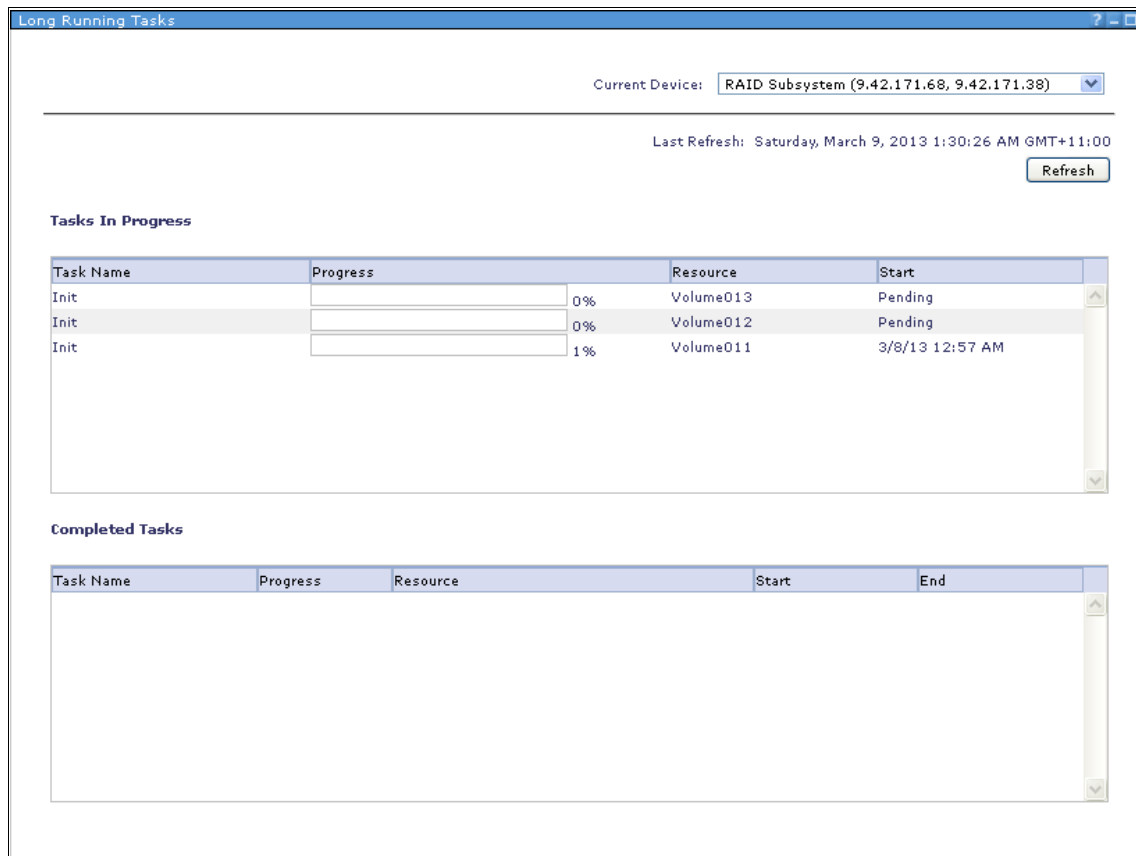


Figure 4-58 A volume initialization process as viewed by using the Long Running Tasks windows

4.5.11 Storage window

This section applies to the SAS RAID Controller Module only.

You can use the Storage configuration window to complete all common tasks that are related to the disks as shown in Figure 4-59. From this window, you can run more granular tasks than are available in the Initial Setup Wizard. This can include a task such as assigning your own global spare disks based on specific slot location.

Because of the intuitive nature of the interface, an in-depth view of the numerous tasks available is not provided. Click the BC-S SAS RAID Module → **Configuration** → **Storage**.

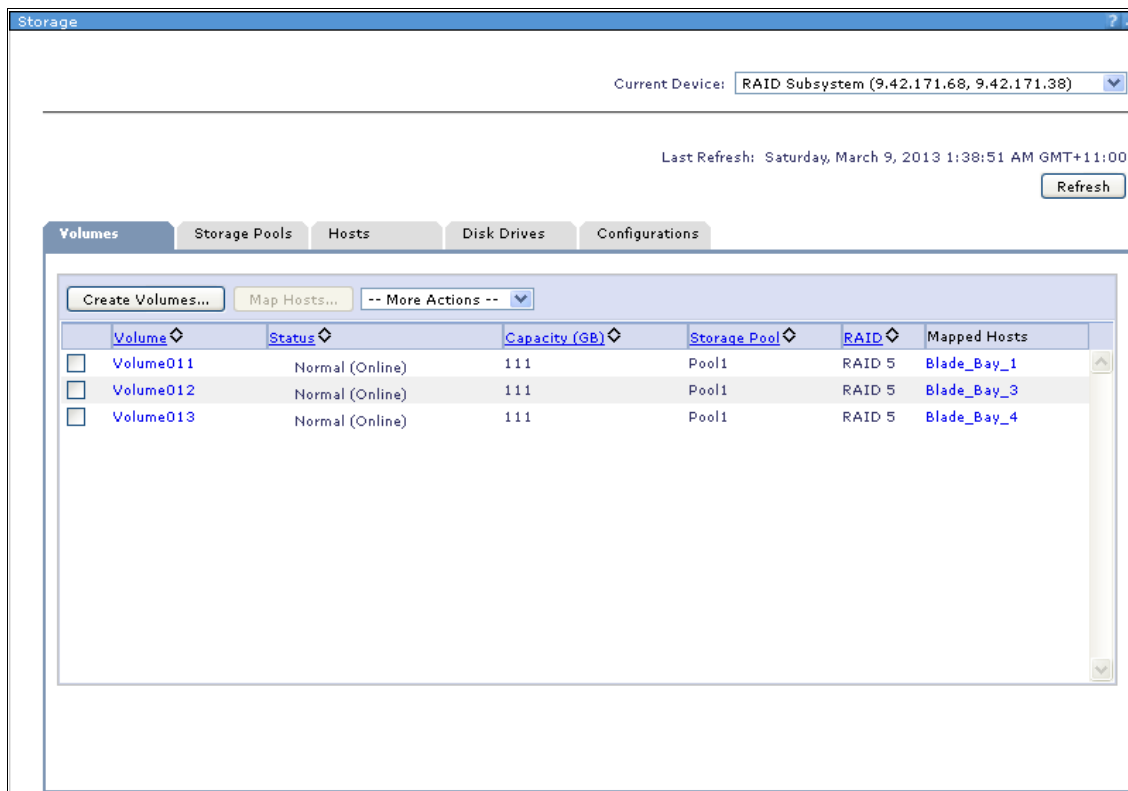


Figure 4-59 Volumes tab on the Storage window

The general tasks that are included with this window are detailed next.

Note: Volume expansion requires that you stop all host I/O activity to the storage during this process. You receive a warning within Storage Configuration Manager when you commence this process.

Volumes tab:

- ▶ Create, delete, expand, and view the properties of volumes
- ▶ Map volumes to hosts and host mapping removal

Storage Pools tab:

- ▶ Create volumes
- ▶ Create, delete, expand, and view the properties of storage pools
- ▶ Assign global hot spare drives

Hosts tab:

- ▶ Discover, create, delete, rename, or view the properties of a host
- ▶ Map or unmap volumes to a host

Disk Drives tab:

- ▶ Assign or unassign specific drives as global spare drives
- ▶ Locate drives and view drive properties

Configuration tab:

- ▶ Save current configuration
- ▶ Restore, apply, download, and back up configurations for the SAS RAID Controller Module

4.5.12 SAS Zoning task

You can use the SAS Zoning task to define and apply user-defined configurations for the SAS RAID Controller Module and SAS Connectivity Module, as well as predefined configurations for the SAS Connectivity Module. For more information about zone activation, see Figure 4-47 on page 224.

4.5.13 Ports and SAS ports

The Ports window allows you to perform the following tasks:

- ▶ Enable or disable port access within the respective SAS module. This includes the internal ports to all six blades, and all the external ports on the switch. For more information, see “Enabling or disabling a port” on page 238.

Note: Disabling internal ports to the blades on the SAS module by using the Ports window might affect your zone configurations. If a blade has access to internal storage by using its zone configuration and you disable its internal port from the Ports window, you might lose access to your storage. This can result in data loss. Only disable ports to blades if you do not intend to use the internal storage available in the BladeCenter S.

- ▶ View the connectivity status of devices (SAS Connectivity module only). For more information, see “Viewing the connectivity status of devices” on page 239.
- ▶ View the properties of the devices, which include basic device information. For more information, see “Viewing the properties of a device” on page 240.

Enabling or disabling a port

To enable or disable a port on either SAS modules, complete these steps:

1. Go to the respective controller module:
 - a. For the SAS Connectivity module, click **BladeCenter SAS Module** → **Configuration** → **Ports**
 - a. For the SAS RAID Module, click **BC-S SAS RAID Module** → **Configuration** → **SAS Ports** as seen in Figure 4-60.

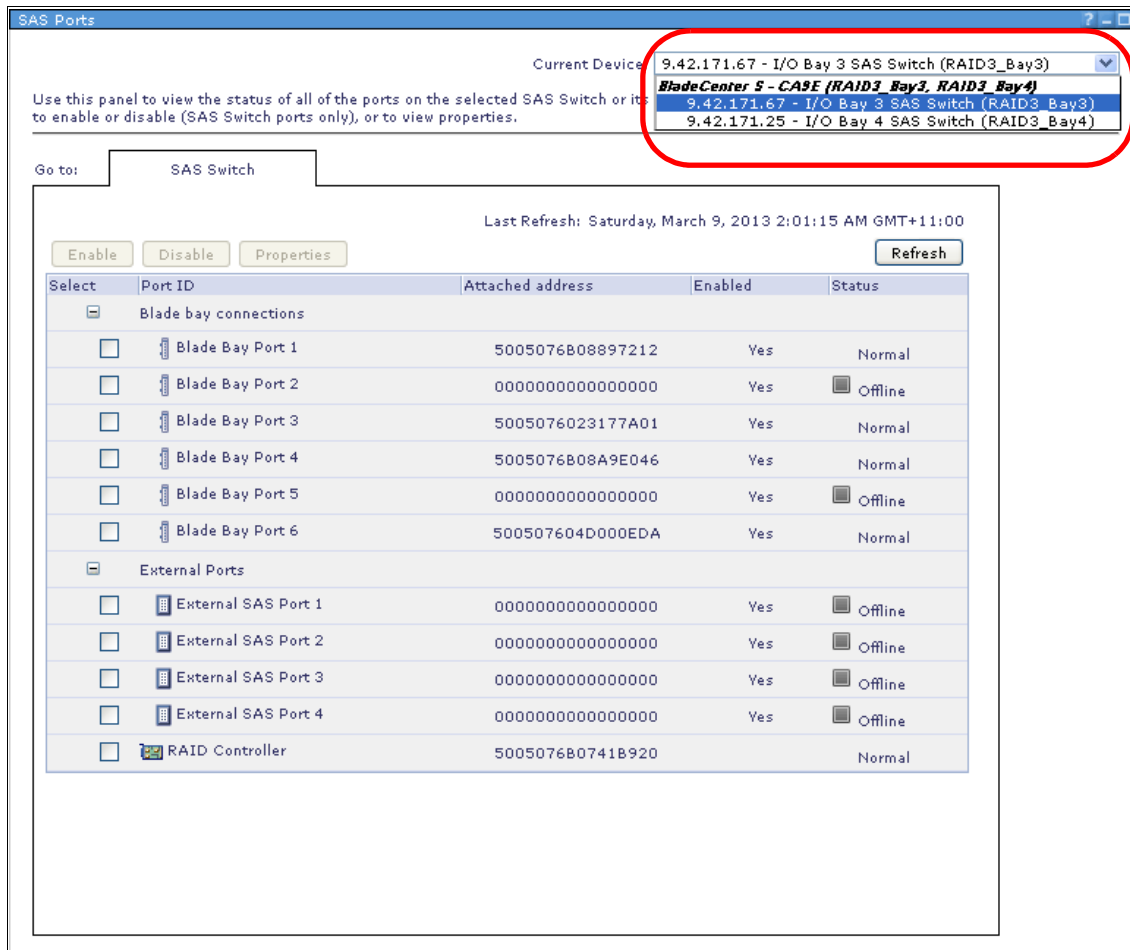


Figure 4-60 Ports window for SAS Switch on the SAS RAID Controller module

2. Select the respective SAS module from the **Current Device** menu in the upper right corner of the window. See section highlighted in Figure 4-60.

3. Select either the Blade Slot Connection or External Port to be enabled or disabled by clicking the check box next to the listed device.
4. Click either **Enable** or **Disable**.

You are asked to confirm your selection. Click **OK** to commit the change or **Cancel** if you do not want to apply the new selection.

Note: Settings that are applied from the Ports window are applied per SAS module.

Viewing the connectivity status of devices

This section applies to the SAS Connectivity Module only.

To view the connectivity status of a device, click **BladeCenter SAS Module** → **Configuration** → **Ports** for the SAS Connectivity Module. The Status column provides you with basic information about the connectivity status of the device, which can be Normal, Offline, or Failed.

There are three tabs in this window (the SAS switch tab exists only for the SAS RAID Controller Module) as shown in Figure 4-61:

- ▶ One tab for the SAS Connectivity Module, which provides connectivity status information for the blades, external ports, and storage module.
- ▶ One tab for each of the storage modules, which provides details about the state of the port connectivity to the individual disks.

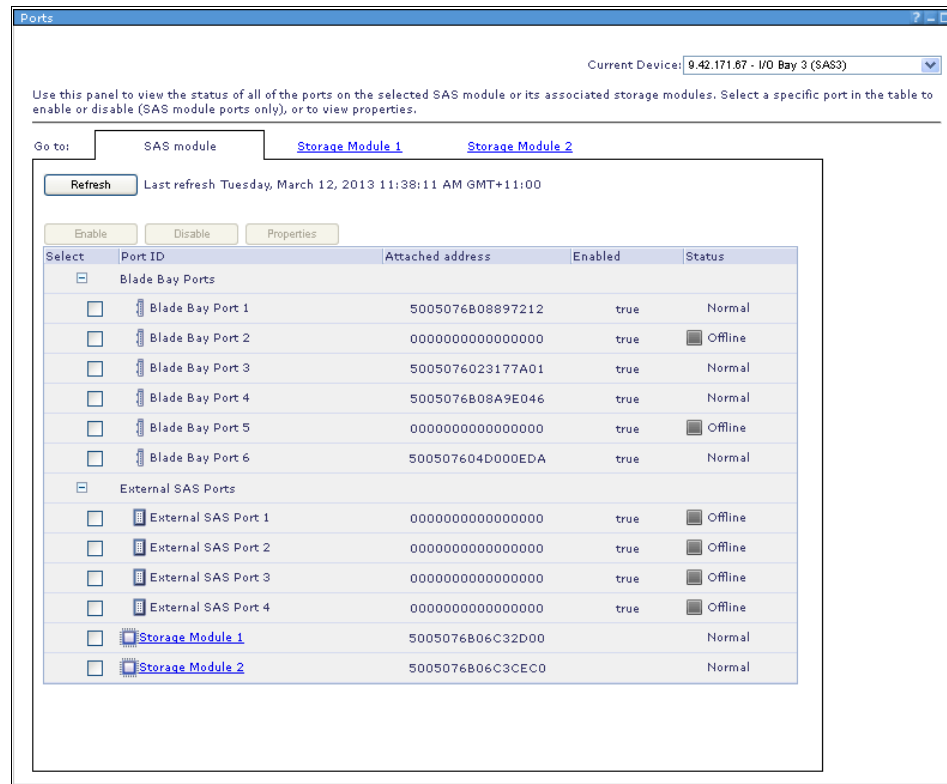


Figure 4-61 Storage Module tab showing the status of the disks

Viewing the properties of a device

To view the properties of a device, complete these steps:

1. Select the applicable SAS module:
 - a. For the SAS RAID Controller Module, select **SAS Switch**, then tab to the device you want to view.
 - b. For the SAS Connectivity Module, select either **Storage Module 1** or **Storage Module 2**, then tab to the device you want to view.
2. Select the device whose properties you want to view.

Note: You can select only one device at a time to see its properties.

3. Click **Properties**. Figure 4-62 shows an example of the window that is displayed.

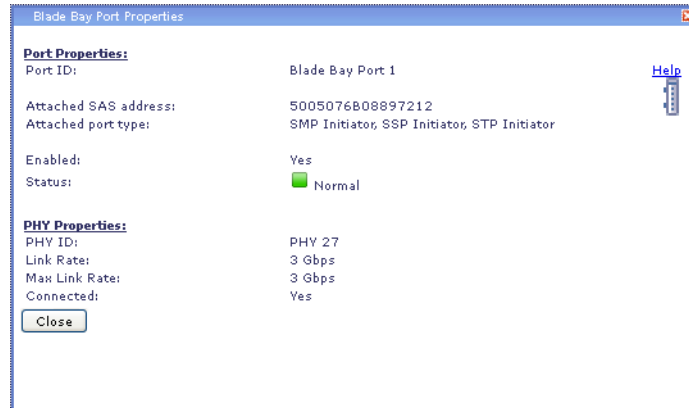


Figure 4-62 Properties window for a blade bay port connection

4.5.14 Audit log

The audit log contains records of all user-initiated actions against devices that the SCM application manages. This information is useful for change control tracking purposes. Figure 4-63 shows an example log. To view the audit log:

- ▶ For the SAS Connectivity Module, click **BladeCenter SAS Module** → **Service** → **Audit Log**.
- ▶ For the SAS RAID Controller Module, click **BC-S SAS RAID Module** → **Service** → **Audit Log**.

The audit log shows a record of the actions the users have initiated while using this application. You can view the entries in the log file below.

IBM Support
Last Refresh: Saturday, March 9, 2013 2:52:59 AM GMT+11:00

Message ID	Date and Time	Device	User ID	Description
GWMSB0024I	Mar 8, 2013 2:29:24 PM	5005076B0741B97F	administrator	Apply configuration, RAID Subsystem [9.42.171.68, 9.42.171.38]; Configuration name: [Pool1_3vol_111GB_LTO6]
GWMSB0026I	Mar 8, 2013 2:18:14 PM	5005076B0741B97F	administrator	Restore configuration, RAID Subsystem [9.42.171.68, 9.42.171.38]; Configuration filepath: [\\wn#5005076B0741B97F], source file name: [Pool1_3vol_111GB_LTO6_copy(1)], target file name: [Pool1_3vol_111GB_LTO6]
GWMSB0044I	Mar 7, 2013 11:28:36 PM	5005076B0741B97F	administrator	Controller [9.42.171.38] has been brought online
GWMSB0044I	Mar 7, 2013 11:26:22 PM	5005076B0741B97F	administrator	Controller [9.42.171.68] has been brought online
GWMSB0042I	Mar 7, 2013 10:24:25 PM	5005076B0741B97F	administrator	Controllers [9.42.171.68, 9.42.171.38] have been shut down to service mode
GWMSB0024I	Mar 7, 2013 9:37:23 PM	5005076B0741B97F	administrator	Apply configuration, RAID Subsystem [9.42.171.68, 9.42.171.38]; Configuration name: [savedConfig]
GWMSB0024I	Mar 7, 2013 9:30:53 PM	5005076B0741B97F	administrator	Apply configuration, RAID Subsystem [9.42.171.68, 9.42.171.38]; Configuration name: [savedConfig]
GWMSB0026I	Mar 7, 2013 9:30:53 PM	5005076B0741B97F	administrator	Restore configuration, RAID Subsystem [9.42.171.68, 9.42.171.38]; Configuration filepath: [C:\Program Files\IBM\SCM\base\archive\wn#5005076B0741B97F], source file name: [Pool1_3vol_111GB_LTO6_copy(1)], target file name: [savedConfig]

Figure 4-63 Audit Log window for SAS RAID Controller module

4.5.15 Update firmware for the SAS Connectivity Module

This section applies to the SAS Connectivity Module only.

Although the Update Firmware option is available for the SAS Connectivity module, at the time of writing it was not supported. You receive a warning message as shown in Figure 4-64. This window allows you to update firmware on the SAS modules and the storage modules.

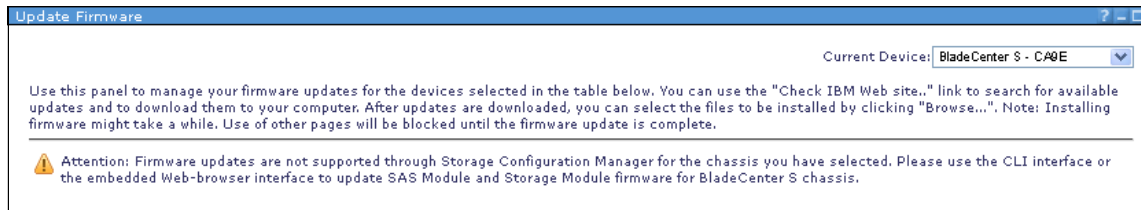


Figure 4-64 Firmware update message

To see alternative ways to upgrade the SAS Connectivity Module firmware, see 4.11.1, "SAS Connectivity Module firmware" on page 290.

4.5.16 Updating firmware for the SAS RAID Controller Module

This section applies to the SAS RAID Controller Module only.

You can use the Update Firmware window to update firmware of the SAS RAID Controller Module, the Disk Storage Modules, and Backup units. Figure 4-65 displays the firmware update window. For more information, see 4.11.2, “SAS RAID Controller Module firmware” on page 294 on how to apply firmware updates to the SAS RAID Controller Module.

Update Firmware

Current Device: RAID Subsystem (9.42.171.68, 9.42.171.38)

Review the [Updating firmware](#) help topic before updating firmware.

Devices selected for firmware updates:

- RAID Subsystem and both SAS switches
- RAID Controller 3 (9.42.171.68)
- RAID Controller 4 (9.42.171.38)
- Storage Module 1
- Storage Module 2
- BBU 1
- BBU 2
- SAS Switch in I/O Bay 3 (9.42.171.67)
- SAS Switch in I/O Bay 4 (9.42.171.25)

Current Firmware Bundle Level:

Type	Level
Controller	1.2.4.011
SAS Switch in I/O Bay 3	R1.07
SAS Switch in I/O Bay 4	R1.07

Download Firmware Bundle:

Go to the [IBM BladeCenter support website](#) to find and download the latest available updates.

Install Downloaded Firmware Bundle:

Enter the path and file name of the firmware bundle on your local machine, or click **Browse**. Then click **Install** to begin the installation.

The RAID controllers are in a normal, bound state. Select Install to proceed with concurrent firmware update.

☒ Verify the RAID subsystem is ready for firmware updates before beginning the install process.(Default)

☐ Update pre-verify has not been run on the RAID controllers

Figure 4-65 SAS RAID Controller firmware update window in SCM

4.5.17 Device log

The Device Log window shows a record of events that have occurred on a selected SAS module. This information includes firmware updates, connectivity

status changes or activities, errors, zone configuration applications, and SAS module power state changes.

To open it, complete these steps:

1. Go to the device log:

For the SAS Connectivity Module, click **BladeCenter SAS Module** → **Service** → **Device Log**.

For the SAS RAID Controller Module, click **BC-S SAS RAID Module** → **Service** → **Device Log**.

2. Select the correct SAS module by clicking the **Current Device** menu and clicking a module, as seen in Figure 4-66.

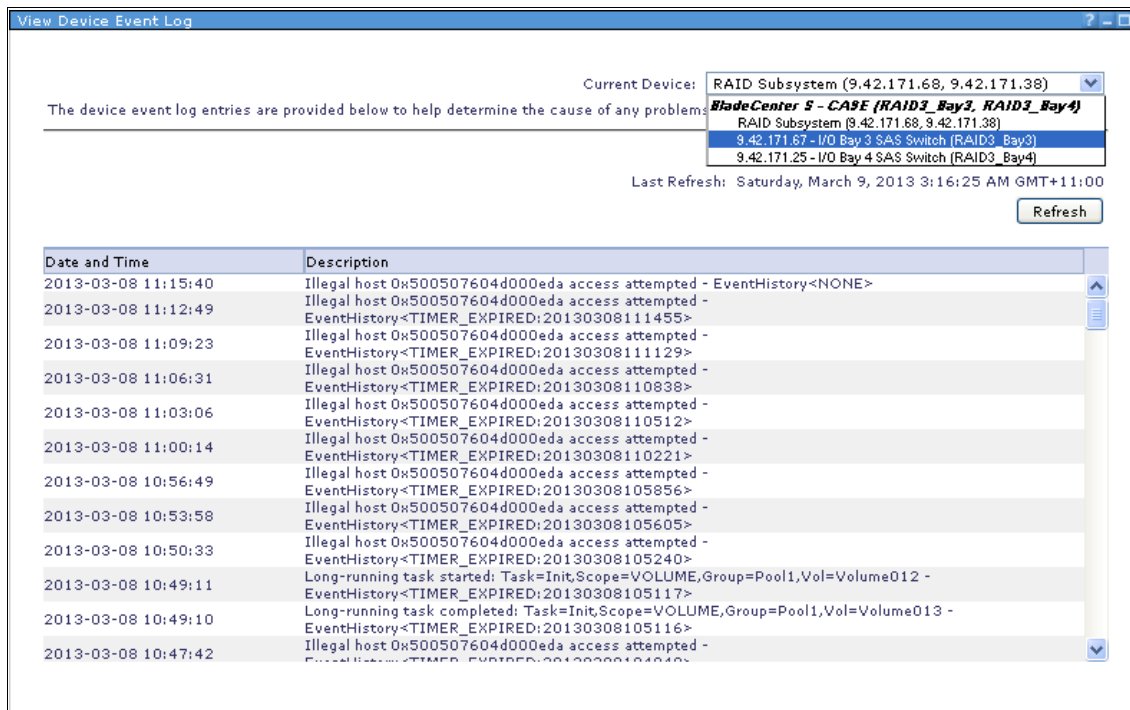
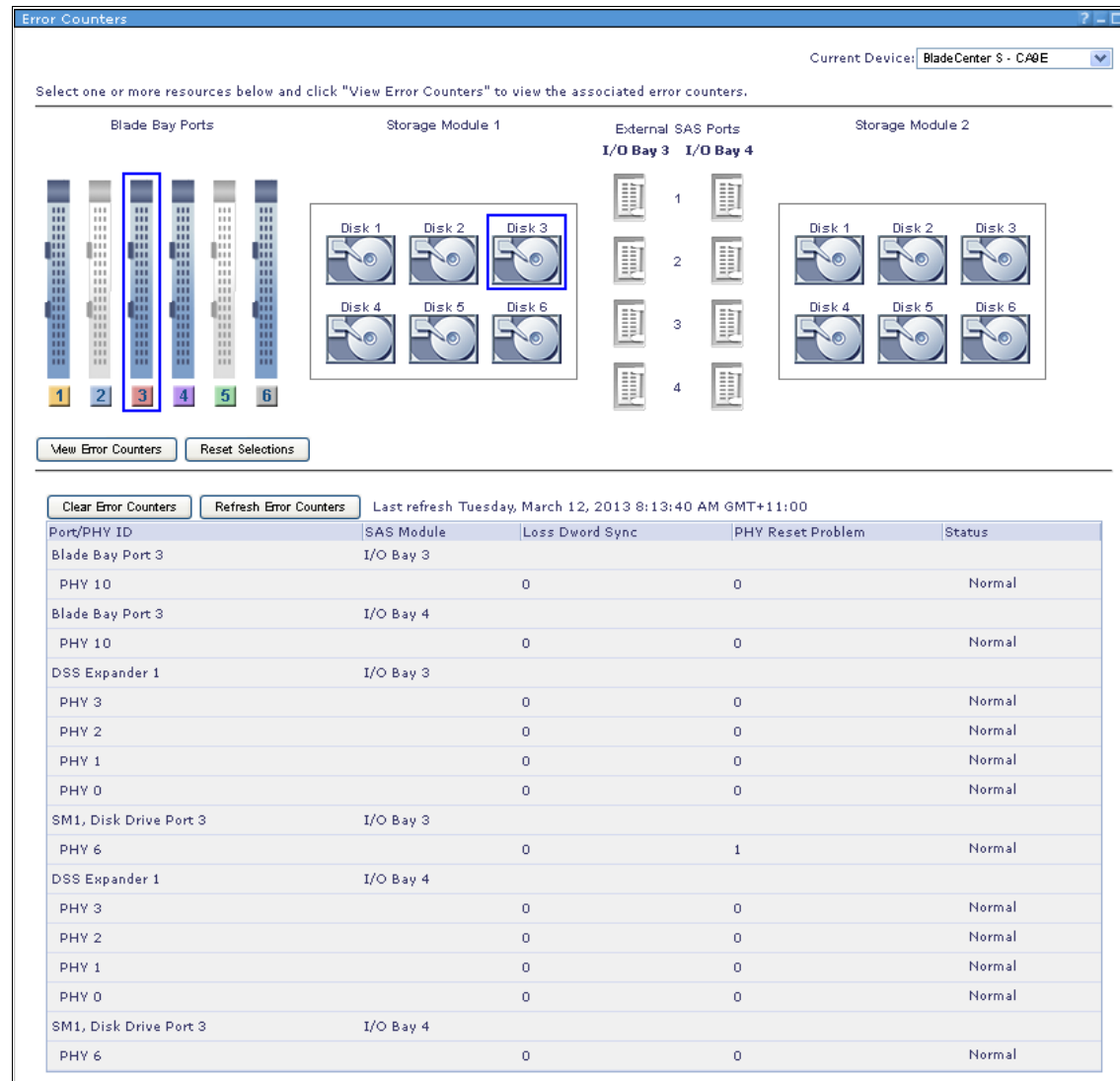


Figure 4-66 Device log FOR SAS RAID Controller showing the SAS module selection menu

4.5.18 Error counters

The Error Counters window, shown in Figure 4-67 for the SAS Connectivity Module and in Figure 4-68 on page 247 for the SAS RAID Controller Module, allows you to view or clear the error counters for a specific device. These error counters can indicate a failing device.

To open it, go to the error counters, and click **Service** → **Error Counters**.



Current Device: BladeCenter S - CAGE

Select one or more resources below and click "View Error Counters" to view the associated error counters.

Blade Bay Ports Storage Module 1 External SAS Ports Storage Module 2

I/O Bay 3 I/O Bay 4

View Error Counters Reset Selections

Clear Error Counters Refresh Error Counters Last refresh Tuesday, March 12, 2013 8:13:40 AM GMT+11:00

Port/PHY ID	SAS Module	Loss Dword Sync	PHY Reset Problem	Status
Blade Bay Port 3	I/O Bay 3			
PHY 10		0	0	Normal
Blade Bay Port 3	I/O Bay 4			
PHY 10		0	0	Normal
DSS Expander 1	I/O Bay 3			
PHY 3		0	0	Normal
PHY 2		0	0	Normal
PHY 1		0	0	Normal
PHY 0		0	0	Normal
SM1, Disk Drive Port 3	I/O Bay 3			
PHY 6		0	1	Normal
DSS Expander 1	I/O Bay 4			
PHY 3		0	0	Normal
PHY 2		0	0	Normal
PHY 1		0	0	Normal
PHY 0		0	0	Normal
SM1, Disk Drive Port 3	I/O Bay 4			
PHY 6		0	0	Normal

Figure 4-67 SAS Connectivity Module Error Counters window

To view the error counters for a specific device, complete these steps:

1. Select one or more devices by clicking the graphic that is associated with each device.
2. Click **View Error Counters** to view the associated error counters.

To clear error counters for a specific device, select the device and click **Clear Error Counters** (Figure 4-68).

Current Device: BladeCenter S - CA9E (RAID3_Bay3, RAID3_Bay4)

Select one or more resources below and click the "View Error Counters" button to view associated error counters.

Blade Bay Ports **RAID Controller 1** **External Ports** **RAID Controller 2**

I/O Bay 3 I/O Bay 4

1 2 3 4 5 6

1 2 3 4

View Error Counters Reset Selections

Clear Error Counters Refresh Error Counters Last Refresh: Saturday, March 9, 2013 3:30:53 AM GMT+11:00

Port/PHY ID	SAS Switch	Loss Dword Sync	PHY Reset Problem	Status
Blade Bay Port 1	I/O Bay 3			
PHY 27		6	0	Normal
Blade Bay Port 1	I/O Bay 4			
PHY 27		6	0	Normal
RAID Controller 1	I/O Bay 3			
PHY 15		6	0	Normal
PHY 10		6	0	Normal
PHY 9		6	0	Normal
PHY 8		2	0	Normal

Figure 4-68 SAS RAID Controller Module error counters for Blade 1 and RAID Controller 1 selected

4.5.19 Collecting support data

You can use the Collect Support Data window to gather and download all of the device status and log information that is needed by IBM support for a specified SAS module. To gather this data, complete these steps:

1. Open the Collect Support Data window, and click **Service** → **Collect Support Data**.
2. Select the correct SAS module from the **Current Device** menu as seen in Figure 4-69.

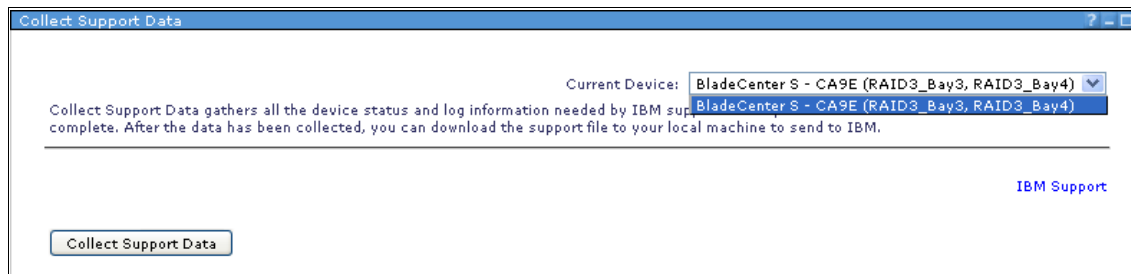


Figure 4-69 Selecting a device in the Collect Support Data window

3. Click **Collect Support Data**. It takes a short time for the data to be gathered.
4. After the data is collected as seen in Figure 4-70, click the **Click here** link to save the data to your local computer. Click **Save** if using Internet Explorer and select a location for the data to be saved. Click **Save** again to complete the process.

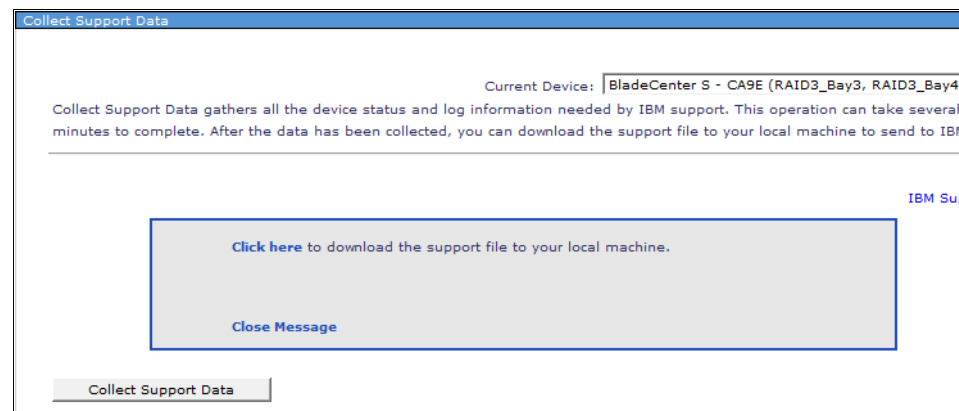


Figure 4-70 Support data post collection phase

4.5.20 User management

On the User Administration window, which is shown in Figure 4-71, you can modify the passwords of the users on the target device selected in the **Current Device** menu.

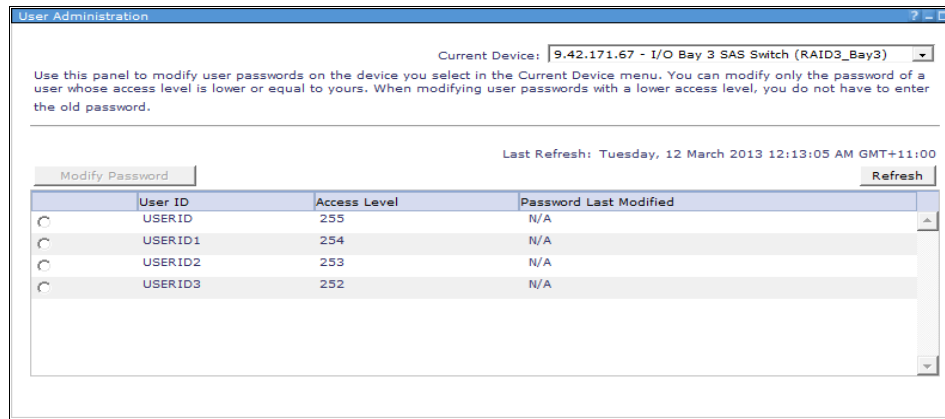


Figure 4-71 User Administration window

You can only modify the password of a user whose access level is lesser than or equal to your own access level as indicated in the Access Level column. When you modify passwords of users with a lesser access level, you are not required to enter the old password.

To modify a user account password, complete these steps:

1. Select the required SAS module from the **Current Device** menu.
2. Select the account that you want to modify and click **Modify Password**.
3. You are then prompted to enter a new password. If you are modifying your own password, you are also prompted to enter your existing password. The new password must be 8-16 characters long.
4. Click **OK** when done.

4.6 Using the AMM Storage Configuration task

The Storage Configuration task within the AMM allows you to carry out the following tasks:

- ▶ For the SAS Connectivity Module:
 - Select and activate a predefined or user-defined zone configuration
 - View the current zone configurations applied
- ▶ For the SAS RAID Controller Module
 - View the current zone configurations applied

You can also use the Storage Configuration task to change the existing zone configuration, which can be useful if your storage requirements change.

Important: You must plan your zone configurations carefully. Depending on the existing zone configuration that you have and the new zone configuration that you want to implement, you might incur data loss. Be sure to back up all data before you implement a zone configuration change.

To review the zone configuration for a SAS Connectivity Module, use these steps:

1. Click **Storage Tasks** → **Configuration**.
2. Click either of the **SAS Conn Mod** links listed to show the zone configuration management view (Figure 4-72).

Storage Configuration ?

Use the following links to jump down to different sections on this page.

[I/O Modules](#)

I/O Modules ?

Zone Configuration

Select any link shown under the "I/O Module Type" column to change the zone configuration for your installed I/O Modules. If no link is displayed, your I/O Module(s) may be powered off, in a fault state, the IP address of the I/O Module is not on the same subnet as the AMM or it may not have completed its initialization. Note that If both SAS RAID Controller Module and SAS Connectivity Module are installed in slot 3 and 4 of BCS chassis, AMM must prevent one of them from powering on otherwise there would be conflict with the Storage Module access and possibly corruption of data.

Bay	I/O Module Type	Active Zone Configuration	Zone Config. Type	
3	SAS Conn Mod	SAS Connectivity 1	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting
4	SAS Conn Mod	SAS Connectivity 1	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting

Figure 4-72 AMM Storage Configuration window for SAS Connectivity modules

3. There are the following viewing options available:
 - Show most appropriate zone configuration with the current chassis hardware.
 - Show all possible zone configurations.
 - Do not change zone configuration.
4. Select **Show all possible zone configurations available. I will choose one myself (recommended for advanced users)**. A full list of zone configurations becomes visible.
5. To change and apply a different zone, select it from the zone configuration list. However, you first must select **Apply the same zone configuration to both I/O Modules**.

Important: You must select an identical zone configuration for both SAS Modules if you have both modules installed. Dissimilar zone configuration between the SAS Modules is not supported.

6. Select the required zone configuration and click **Activate Selected Configuration** to commit the changes, as seen in Figure 4-73 on page 252.
7. The Storage Configuration now reflects the new zone configuration.

Zone Configuration Management for I/O Modules

- ☐ Show the zone configuration that is most appropriate for my current number of blades and SAS I/O Modules
- ☒ Show all possible zone configurations available. I will choose one myself (recommended for advanced users)
- ☐ Do not change the zone configuration at this time

The table below displays zone configurations stored on the given I/O Module. Please select the desired zone configuration from the list and activate it. The 'Refresh' button would be helpful in refreshing the status once the zone is applied. If you have multiple SAS RAID Controller Modules or SAS Connectivity Modules installed and both are in working order, a check box will be provided that allows you to easily apply the same configuration to each I/O Module. The default setting is to apply the same zone configuration to each. If you uncheck the check box, information for both I/O Modules will be presented and you can select a zone configuration from each. However, it is highly recommended that you select the same zone configuration for both I/O Modules.

☒ Apply the same zone configuration to both I/O Modules

I/O Module 3 (SAS Conn Mod)

The table below lists zone configurations stored on this I/O Module.

Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date
<input type="radio"/>		Predefined Config 02	Pre-defined	6	2	1	6	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 03	Pre-defined	6	1	2	7	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 04	Pre-defined	1	2	6	8	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 05	Pre-defined	1	1	12	9	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 06	Pre-defined	3	2	2	10	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 07	Pre-defined	3	1	4	11	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 08	Pre-defined	2	2	3	12	04/24/2007, 02:00:00
<input type="radio"/>		Predefined Config 09	Pre-defined	2	1	6	13	04/24/2007, 02:00:00

Select	Active?	Name	Type	Description	Configuration Store	Date
<input type="radio"/>	<input checked="" type="checkbox"/>	SAS Connectivity 1	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.	1	03/12/2013, 15:35:56
<input type="radio"/>		User Defined Config 02	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.	2	00/00/0000, 00:00:00
<input type="radio"/>		User Defined Config 03	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.	3	00/00/0000, 00:00:00
<input type="radio"/>		User Defined Config 04	User-defined	Chassis: Any. SAS modules: 1 or 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port. Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.	4	00/00/0000, 00:00:00

Activate Selected Configuration Refresh

Figure 4-73 Zone Configuration Management for I/O Modules window

4.7 Using the SAS module web browser interface

Both the SAS Connectivity Module and SAS RAID Controller Module have a browser interface for easy administration. You can perform more comprehensive tasks by using this interface compared to the AMM Storage Configuration tasks pane. This section describes these tasks.

The web browser interfaces for both the SAS Connectivity Module and the SAS RAID Controller Module are almost identical. The SAS Connectivity Module browser interface is used for most of the illustrations provided, but the SAS RAID Controller Module is very similar.

The following tasks are described:

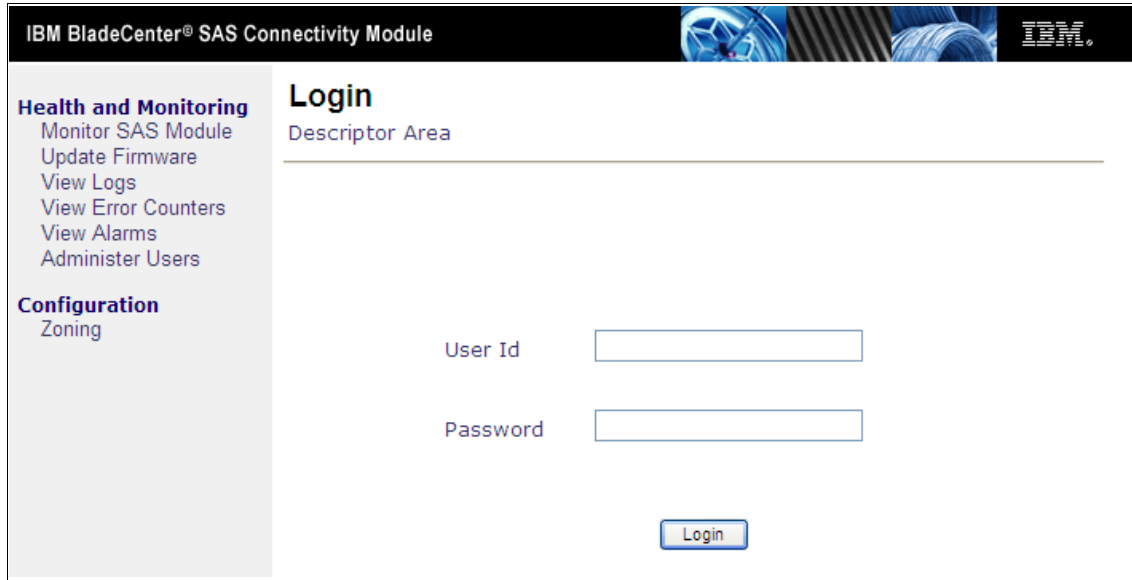
- ▶ 4.7.1, “Logging in” on page 254
- ▶ 4.7.2, “Monitoring SAS subsystem health” on page 255
- ▶ 4.7.3, “Updating firmware: SAS Connectivity Module” on page 256
- ▶ 4.7.4, “Updating firmware: SAS RAID Controller module” on page 257
- ▶ 4.7.5, “View logs” on page 258
- ▶ 4.7.6, “View error counters” on page 259
- ▶ 4.7.7, “View alarms” on page 260
- ▶ 4.7.8, “View RAID” on page 260
- ▶ 4.7.9, “User administration” on page 261
- ▶ 4.7.10, “Zoning” on page 262

Before a SAS module can be managed by using the browser interface, it must already have a valid IP address assigned to it through the AMM. The IP address that you choose must be within the same subnet as your AMM IP address. For more information about configuring an IP address, see 5.5, “I/O module tasks” on page 374.

4.7.1 Logging in

To log in to the SAS module, complete these steps:

1. Open a web browser and enter the IP address or domain name server (DNS) name (if you registered the SAS module name and IP address in DNS) of the SAS module. You are presented with a window similar to Figure 4-74.



The screenshot shows the login interface for the IBM BladeCenter SAS Connectivity Module. At the top, there is a black header bar with the text "IBM BladeCenter® SAS Connectivity Module" on the left and the IBM logo on the right. Below the header, the page is divided into two main sections. On the left is a vertical navigation menu with two main categories: "Health and Monitoring" and "Configuration". Under "Health and Monitoring", there are links for "Monitor SAS Module", "Update Firmware", "View Logs", "View Error Counters", "View Alarms", and "Administer Users". Under "Configuration", there is a link for "Zoning". The right section is titled "Login" and contains a "Descriptor Area" with a horizontal line. Below this line are two input fields: "User Id" and "Password". A "Login" button is positioned below the "Password" field.

Figure 4-74 SAS module Login window

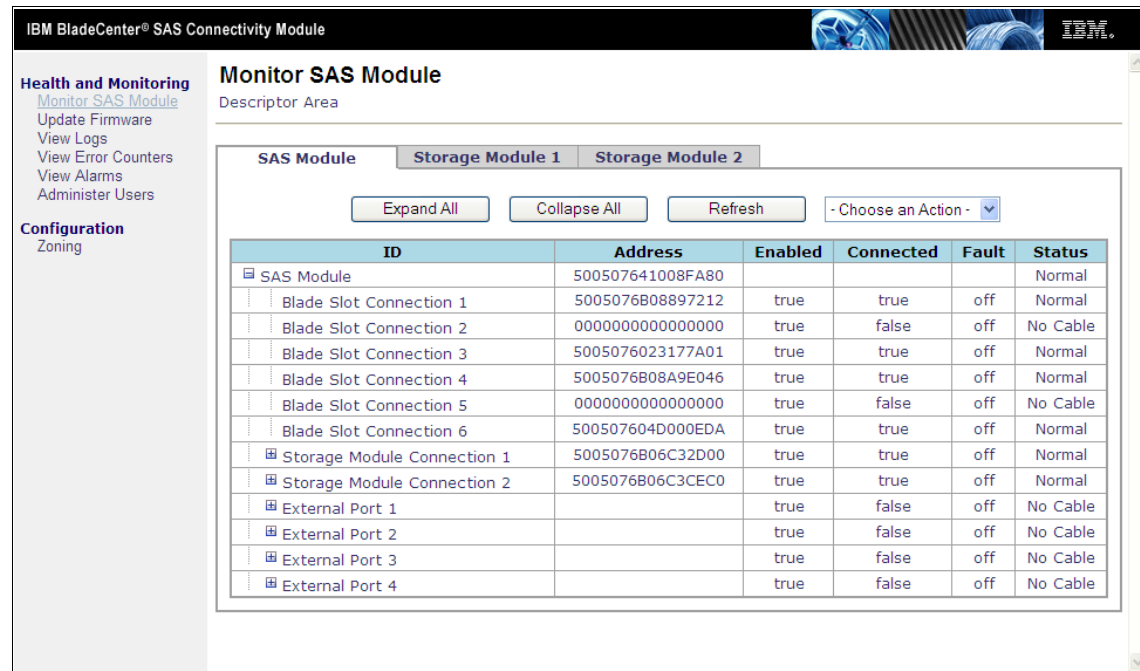
2. Enter the user name and password of the account that has access to the SAS module and click **Login**.

The default user name is USERID in uppercase. The default password is PASSWORD in uppercase, but using the number zero (0) instead of the letter O. You are then presented with the Welcome window. You can navigate to the following topics from the Welcome window.

4.7.2 Monitoring SAS subsystem health

With this choice, you can check the health status of your SAS module and the Storage Modules (Storage Module tabs only apply when connected to the SAS Connectivity Module)

1. Click **Health and Monitoring** → **Monitor SAS Module**.
2. Select either the SAS Module, Storage Module 1, or Storage Module 2 tab. This choice is determined by the information that you want to view. The SAS Module tab presents information about the connectivity status between the various components and the SAS module. The Storage Module 1 or Storage Module 2 tab presents information about the connectivity status between the SAS module and the storage modules, including the disks. Figure 4-75 displays the SAS module status pane.



IBM BladeCenter® SAS Connectivity Module

Health and Monitoring
Monitor SAS Module
Update Firmware
View Logs
View Error Counters
View Alarms
Administer Users

Configuration
Zoning

Monitor SAS Module

Descriptor Area

SAS Module | **Storage Module 1** | **Storage Module 2**

Expand All | Collapse All | Refresh | - Choose an Action -

ID	Address	Enabled	Connected	Fault	Status
[-] SAS Module	500507641008FA80				Normal
[-] Blade Slot Connection 1	5005076B08897212	true	true	off	Normal
[-] Blade Slot Connection 2	0000000000000000	true	false	off	No Cable
[-] Blade Slot Connection 3	5005076023177A01	true	true	off	Normal
[-] Blade Slot Connection 4	5005076B08A9E046	true	true	off	Normal
[-] Blade Slot Connection 5	0000000000000000	true	false	off	No Cable
[-] Blade Slot Connection 6	500507604D000EDA	true	true	off	Normal
[+] Storage Module Connection 1	5005076B06C32D00	true	true	off	Normal
[+] Storage Module Connection 2	5005076B06C3CEC0	true	true	off	Normal
[+] External Port 1		true	false	off	No Cable
[+] External Port 2		true	false	off	No Cable
[+] External Port 3		true	false	off	No Cable
[+] External Port 4		true	false	off	No Cable

Figure 4-75 Monitor SAS Module window

4.7.3 Updating firmware: SAS Connectivity Module

You can use the SAS module browser interface to update the firmware of both the SAS module and the connected disk storage modules.

Firmware is updated by using the **Health and Monitoring** → **Update Firmware** window, as shown in Figure 4-76. For more information, see 4.11.1, “SAS Connectivity Module firmware” on page 290, which includes updating the SAS Connectivity and Disk Storage Module firmware.

IBM BladeCenter® SAS Connectivity Module

Health and Monitoring
Monitor SAS Module
[Update Firmware](#)
View Logs
View Error Counters
View Alarms
Administer Users

Configuration
Zoning

Update Firmware

Descriptor Area

To update firmware, select the firmware file and click "Install".

Current Code Level

Device	Level	Activation	Status
SAS Module	03.71	2012-07-24 16:51:52	Normal
Storage Module 1	1.08		Normal
Storage Module 2	1.08		Normal

Note: It is strongly recommended that the firmware levels of the two Storage Modules be kept the same.

Target Device:

Firmware File:

Figure 4-76 SAS Connectivity Update Firmware window

4.7.4 Updating firmware: SAS RAID Controller module

This section applies to the SAS RAID Controller Module only.

The SAS RAID Controller Module web browser interface allows you to update the firmware of the SAS RAID Controller Module as shown in Figure 4-77.

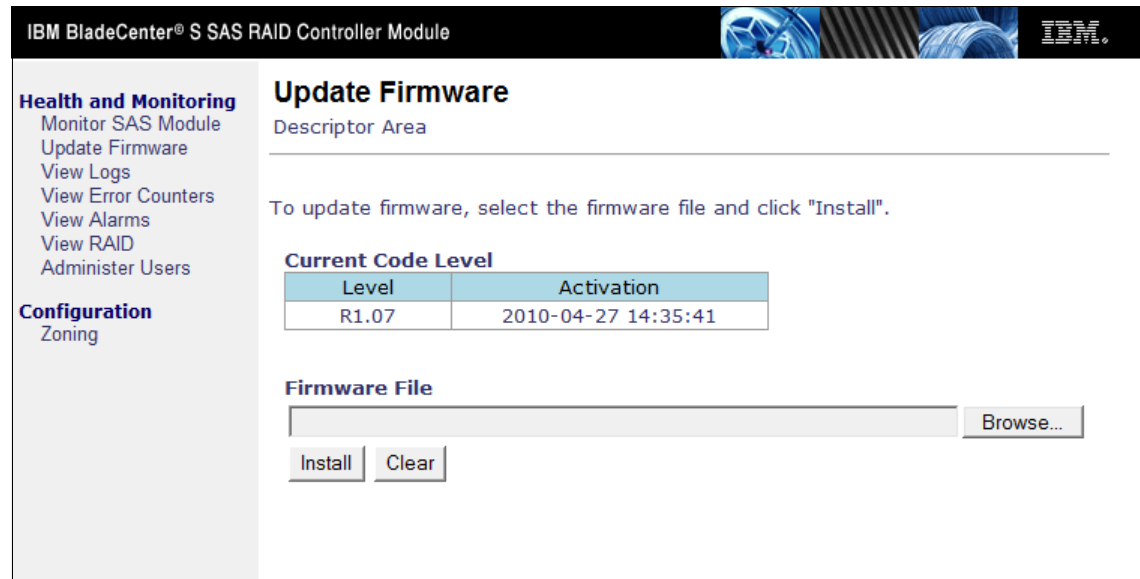



Figure 4-77 SAS RAID Controller Update Firmware window

Service Mode: The SAS RAID Controller Modules that you are updating must be placed offline and in Service Mode before a firmware update can take place. Generally, carry out this procedure by using Storage Configuration Manager or the command-line interface through Telnet because you cannot place a SAS RAID Controller Module in service mode from the web browser user interface.

For more information about updating SAS RAID Controller Module firmware, see “Updating firmware using the CLI” on page 292.

4.7.5 View logs

You can use the View Logs window to view all of the system logs available on the SAS module. You might find this information useful for troubleshooting connectivity problems or for tracking when zone configuration changes or firmware updates occur. To view the logs, click **Health and Monitoring** → **View Logs** as seen in Figure 4-78.

IBM BladeCenter® SAS Connectivity Module


Health and Monitoring
Monitor SAS Module
Update Firmware
View Logs
View Error Counters
View Alarms
Administer Users

Configuration
Zoning

View Logs

Descriptor Area

Logs 1-128 of 1024 [Refresh](#)

Date/Time	Device	Log Description
2013-03-11 21:05:41	SAS Module	Blade Port 4 Link Up
2013-03-11 21:05:40	SAS Module	Blade Port 1,3,6 Link Up
2013-03-11 21:05:40	SAS Module	Blade Port 1,2,3,4,5,6 Phy Enable
2013-03-11 21:05:39	SAS Module	Zone 1 Applied
2013-03-11 20:56:52	SAS Module	Zone Config Stored to Zone 1
2013-03-11 20:39:33	SAS Module	SM Port 1-1,1-2,1-3,1-4,2-1,2-2,2-3,2-4 Link Up
2013-03-11 20:39:33	SAS Module	Ext Port 1-2,1-3,1-4,2-1,2-2,2-3,2-4 Phy Enable
2013-03-11 20:39:33	SAS Module	Ext Port 3-1,3-2,3-3,3-4,4-1,4-2,4-3,4-4,1-1 Phy Enable
2013-03-11 20:39:33	SAS Module	SM Port 1-1,1-2,1-3,1-4,2-1,2-2,2-3,2-4 Phy Enable
2013-03-11 20:39:32	SAS Module	I0104: Boot Up Event
2013-03-11 20:39:32	SAS Module	Zone 0 Applied
2013-03-11 19:37:50	SAS Module	SM Port 1-1,1-2,1-3,1-4,2-1,2-2,2-3,2-4 Link Up
2013-03-11 19:37:50	SAS Module	Ext Port 1-2,1-3,1-4,2-1,2-2,2-3,2-4 Phy Enable
2013-03-11 19:37:50	SAS Module	Ext Port 3-1,3-2,3-3,3-4,4-1,4-2,4-3,4-4,1-1 Phy Enable
2013-03-11 19:37:50	SAS Module	SM Port 1-1,1-2,1-3,1-4,2-1,2-2,2-3,2-4 Phy Enable
2013-03-11 19:37:49	SAS Module	I0104: Boot Up Event
2013-03-11 19:37:49	SAS Module	Zone 0 Applied
2013-03-11 19:23:35	SAS Module	SM Port 1-1,1-2,1-3,1-4,2-1,2-2,2-3,2-4 Link Up

Log pages: Previous [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [Next](#)

Figure 4-78 View Logs window

4.7.6 View error counters

The View Error Counters window allows you to view the error counters for each device that is connected to the SAS module. The error counters naturally increase if you are powering blades on and off. With the blades switched on all the time, the error counters should not consistently increase. This might indicate connectivity errors. Click **Health and Monitoring** → **View Error Counters** to view this window as shown in Figure 4-79.

IBM BladeCenter® SAS Connectivity Module

Health and Monitoring
 Monitor SAS Module
 Update Firmware
 View Logs
 View Error Counters
 View Alarms
 Administer Users

Configuration
 Zoning

View Error Counters
 Descriptor Area

SAS Module **Storage Module 1** **Storage Module 2**

PHY Id	Invalid Dword	Disparity Error	Loss Dword Sync	PHY Reset Problem	Status
Blade Slot Connection 1	0	0	0	0	Normal
Blade Slot Connection 2	67108876	1161925248	0	0	No Connection
Blade Slot Connection 3	27712	3082	0	0	Normal
Blade Slot Connection 4	67982	1078986752	0	0	Normal
Blade Slot Connection 5	0	0	0	0	No Connection
Blade Slot Connection 6	2969567536	2148010066	0	0	Normal
Storage Module Connection 1, PHY 1	0	0	0	0	Normal
Storage Module Connection 1, PHY 2	0	0	0	0	Normal
Storage Module Connection 1, PHY 3	0	0	0	0	Normal
Storage Module Connection 1, PHY 4	0	0	0	0	Normal
Storage Module Connection 2, PHY 1	0	0	0	0	Normal
Storage Module Connection 2, PHY 2	0	0	0	0	Normal
Storage Module Connection 2, PHY 3	0	0	0	0	Normal
Storage Module Connection 2, PHY 4	0	0	0	0	Normal
External Port 1, PHY 1	0	0	0	0	No Connection
External Port 1, PHY 2	0	0	0	0	No Connection
External Port 1, PHY 3	0	0	0	0	No Connection
External Port 1, PHY 4	0	0	0	0	No Connection
External Port 2, PHY 1	0	0	0	0	No Connection
External Port 2, PHY 2	0	0	0	0	No Connection
External Port 2, PHY 3	0	0	0	0	No Connection
External Port 2, PHY 4	0	0	0	0	No Connection
External Port 3, PHY 1	0	0	0	0	No Connection
External Port 3, PHY 2	0	0	0	0	No Connection
External Port 3, PHY 3	0	0	0	0	No Connection
External Port 3, PHY 4	0	0	0	0	No Connection
External Port 4, PHY 1	0	0	0	0	No Connection
External Port 4, PHY 2	0	0	0	0	No Connection
External Port 4, PHY 3	0	0	0	0	No Connection
External Port 4, PHY 4	0	0	0	0	No Connection

Figure 4-79 View Error Counters window

4.7.7 View alarms

The View Alarms window allows you to view the status of the voltage and temperature of the SAS module. Click **Health and Monitoring** → **View Alarms** to view this window as shown in Figure 4-80.

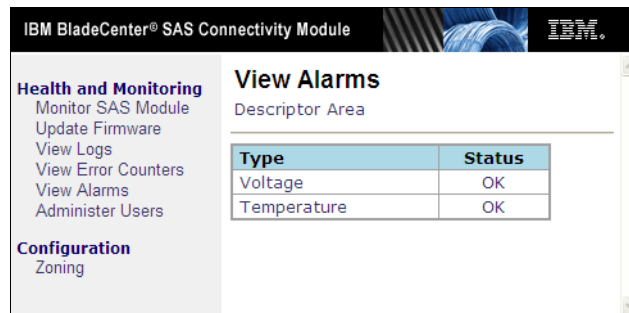


Figure 4-80 View Alarms window

4.7.8 View RAID

This section applies to the SAS RAID Controller Module only.

You can use the View RAID window to view the health status of the SAS RAID Controller Module that you are connecting to. Click **Health and Monitoring** → **View RAID** to view this window, as shown in Figure 4-81.

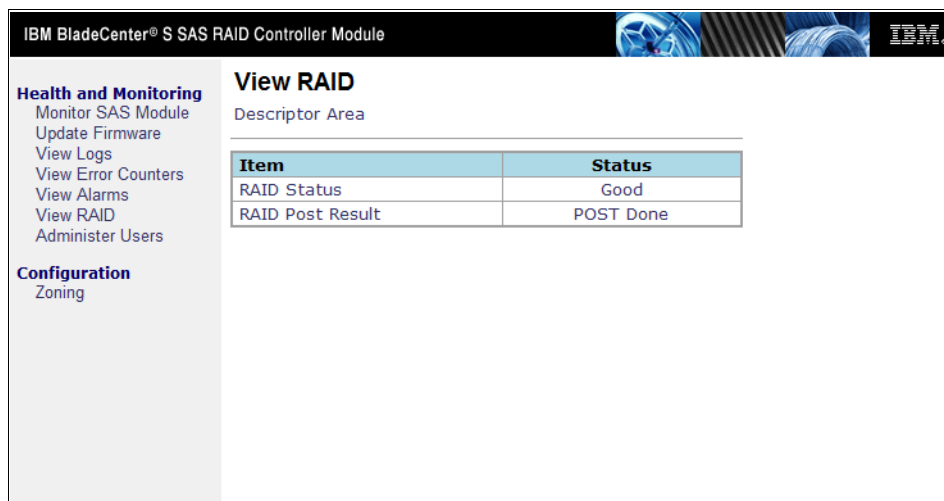


Figure 4-81 View RAID window

4.7.9 User administration

The User Administration window allows you to change the password on one or all of the four built-in USERID accounts that are supplied with the SAS module. To change a password, complete these steps:

1. Click **Health and Monitoring** → **Administer Users** to open the window shown in Figure 4-82.
2. Select the USERID account whose password you want to change and click **Modify Password**.
3. Enter the old password (if the account already has a password assigned to it), then enter a new password and confirm it. Click **OK** when done.

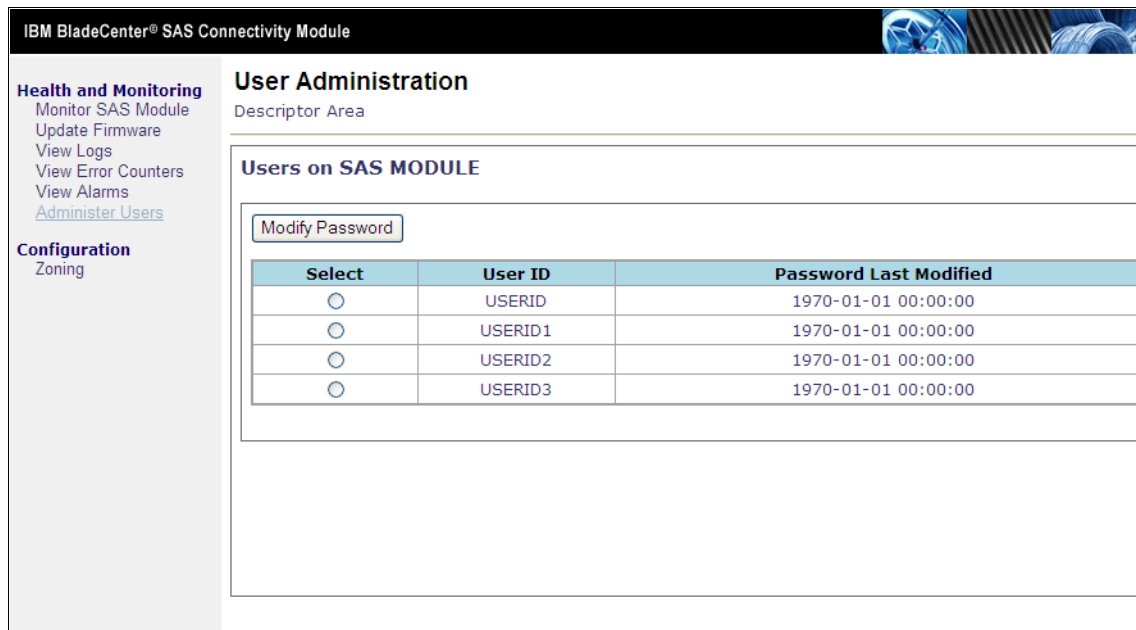




Figure 4-82 User Administration window

4.7.10 Zoning

When you click **Configuration** → **Zoning**, the Manage Fabric window shown in Figure 4-83 opens. From here, you can select a user-defined configuration for the SAS RAID Controller Module or SAS Connectivity Module, and a predefined configuration for the SAS Connectivity Module. You can also view the zone configuration on the SAS module to which you are connected.

Manage Fabric

Descriptor Area

 Working Configuration
  Active Configuration

SAS Connectivity 1

SAS Connectivity 1

Activate this Configuration

Zone Groups

Basic Zone Permission Table

Zone Group ID	SAS Module Ports			Storage Module 1 Ports			Storage Module 2 Ports		
	External	Blade	Storage Module	SAS Module	Disk	SES	SAS Module	Disk	SES
1			1,2	1			1		
30	1								
31	2								
32	3								
33	4								
34		1							
35		2							
36		3							
37		4							
38		5							
39		6							
60						1			
61					1				
62					2				
63					3				
64					4				
65					5				
66					6				
90									1
91								1	
92								2	
93								3	
94								4	
95								5	
96								6	

Figure 4-83 Manage Fabric zoning window for the SAS Connectivity module

Potential data loss: Changing your zone configurations can result in data loss. Ensure that you back up all data and power down all blades before you change the zone configuration.

To activate a new zone, complete these steps:

1. Select a predefined or user-defined configuration from the **Working Configuration** menu as seen in Figure 4-83 on page 262.
2. Click **Activate this Configuration**.
3. A message is displayed to inform you that the selected zone configuration is applied successfully.


Select identical zones on both: You must select an identical zone configuration for both SAS modules if you have two modules installed. Dissimilar zone configuration between the SAS modules is not supported.

It is possible to create user-defined configurations by using the SAS module browser interface. However, this method is not recommended for BladeCenter S. Instead, use Storage Configuration Manager.

- If you click the Basic Zone Permission Table tab, you see a view similar to Figure 4-84. This allows you to view and create user-defined configurations.


Manage Fabric

Descriptor Area



Working Configuration

SAS Connectivity 1



Active Configuration

SAS Connectivity 1

Activate this Configuration

Zone Groups

Basic Zone Permission Table

Select Zone Group

View by: Zone Group ID 34

Port	Attached Port Add	Enabled	Connected	Status
Blade Slot Connection 1	5005076B08897212	true	true	Normal

Mapped to

Remove from Permission Table

Select	Zone Group ID	Port	Attached Port Add	Enabled	Connected	Status
<input type="checkbox"/>	60	Storage Module 1 SES Device	5005076B06C32D13	true	true	Normal
<input type="checkbox"/>	61	Storage Module 1 Disk Drive Connection 1	5000C50008F6756D	true	true	Normal

Not Mapped To

Add to Permission Table

Select	Zone Group ID	Port	Attached Port Add	Enabled	Connected	Status
<input type="checkbox"/>	30	External Port 1		true	false	No Cable
<input type="checkbox"/>	31	External Port 2		true	false	No Cable
<input type="checkbox"/>	32	External Port 3		true	false	No Cable
<input type="checkbox"/>	33	External Port 4		true	false	No Cable
<input type="checkbox"/>	34	Blade Slot Connection 1	5005076B08897212	true	true	Normal
<input type="checkbox"/>	35	Blade Slot Connection 2	0000000000000000	true	false	No Cable
<input type="checkbox"/>	36	Blade Slot Connection 3	5005076023177A01	true	true	Normal
<input type="checkbox"/>	37	Blade Slot Connection 4	5005076B08A9E046	true	true	Normal
<input type="checkbox"/>	38	Blade Slot Connection 5	0000000000000000	true	false	No Cable
<input type="checkbox"/>	39	Blade Slot Connection 6	500507604D000ED9	true	true	Normal
<input type="checkbox"/>	62	Storage Module 1 Disk Drive Connection 2	5000C50008F67561	true	true	Normal
<input type="checkbox"/>	63	Storage Module 1 Disk Drive Connection 3	5000C50008F67931	true	true	Normal

Figure 4-84 Basic Zone Permission Table to create user-defined configurations

4.8 Configuring the SAS RAID Controller Module using the CLI

The command-line interface (CLI) has the most comprehensive set of commands to configure the BladeCenter S. The CLI can be used for both the SAS Connectivity Module and the SAS RAID Controller Module. The following example shows configuring storage that uses two Disk Storage Module (DSM) and two SAS RAID Controller Modules.

To configure the module, complete the following steps:

1. Clear the configuration of both SAS RAID Controller modules by using Telnet to access the AMM. Example 4-1 shows the commands that were issued to log in and clear both SAS RAID Controller modules.

Example 4-1 Clearing configuration from switches in bays 3 and 4 by using AMM

```
telnet 9.42.171.1
```

```
username: USERID
```

```
password:
```

```
Hostname:          bcamm6
```

```
Static IP address:  9.42.171.1
```

```
Burned-in MAC address: 00:14:5E:E1:60:50
```

```
DHCP:              Disabled - Use static IP configuration.
```

```
Last login: Friday March 8 2013 13:49 from 9.42.171.252 (Web)
```

```
system> clear -cnfg -T switch[3]
```

```
OK
```

```
system> clear -cnfg -T switch[4]
```

```
OK
```

```
system>
```

2. Log out of the AMM and Telnet into the first SAS RAID Controller Module. Although there are two SAS RAID Controller Modules, the second module is used for redundancy. Therefore, you must only configure one module and the configuration is automatically replicated to module 2.
3. Example 4-2 shows creating pools. Pool1 is created from four drives, with no spares and in RAID 5. Run the **list pool** command before and after you create the pool to display the difference.

Example 4-2 Pool creation by using CLI on SAS RAID Controller

```
telnet 9.42.171.67
```

```
sername: USERID
```

```
password:
```

<CLI> **list pool**

Current Machine Local Time: 03/08/2013 09:30:13 PM

No drive pools reported

<CLI> **create pool -drives 2:1 2:2 1:1 1:2 -raidtype 5 -port 0 -name Pool1**

Current Machine Local Time: 03/08/2013 09:30:29 PM

Drive group created with total capacity of 729 GB

<CLI> **list pool**

Current Machine Local Time: 03/08/2013 09:30:58 PM

Pool#	ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
0	1	Pool1	5	Slot 0	729GB	729GB	Viable	ONV	No

State: OFN/SN=Offline Non-viable/Service Non-viable

ONF/OFF/SF=Online Failed/Offline Failed/ Service Failed

ONV/OFV/SV= Online Viable/Offline Viable/Service Viable

ONN=Online Non-viable/Pending Non-Viable; one or more drives are missing in this pool.

The pool state changes to ONV if missing drive(s) comes back to the pool.

The pool state changes to OFN if the user acknowledges the alert.

-
- Next, create three volumes, each of which is 111 GB in size and labeled Volume011 to Volume013. Example 4-3 lists the commands issued for each volume. The **list volume** command at the end displays the volume results.

Example 4-3 List volume command

<CLI> **create volume -name Pool1:Volume011 -size 113664MB -seqpostreadcmdsize 0 -seqreadaheadmargin 16384 -writecachepolicy batterydetect**

Working ...

Current Machine Local Time: 03/08/2013 09:31:35 PM

Volume 'Volume011' created on pool 'Pool1' with capacity 113664MB

<CLI> **create volume -name Pool1:Volume012 -size 113664MB -seqpostreadcmdsize 0 -seqreadaheadmargin 16384 -writecachepolicy batterydetect**

Working ...

Current Machine Local Time: 03/08/2013 09:31:53 PM

Volume 'Volume012' created on pool 'Pool1' with capacity 113664MB


```
<CLI> create volume -name Pool1:Volume013 -size 113664MB -seqpostreadcmdsize 0
-seqreadaheadmargin 16384 -writecachepolicy batterydetect
```

Working ...

Current Machine Local Time: 03/08/2013 09:32:23 PM
Volume 'Volume013' created on pool 'Pool1' with capacity 113664MB

```
<CLI> list volume
```

Current Machine Local Time: 03/08/2013 09:32:38 PM

Vol#	VolumeName	Cap	RaidType	Status
0	Pool1:Volume011	111GB	5	VL TRN
1	Pool1:Volume012	111GB	5	VL TRN
2	Pool1:Volume013	111GB	5	VL TRN

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

5. The volumes now must be mapped to the Blade servers. Only Blades with the SAS CIOv expansion card can be assigned a volume. Example 4-4 displays the mapping commands that are used to map a volume to a blade. The host number must be correct for the volume assignment to be successful.

Example 4-4 Mapping of volumes to Blade servers

```
<CLI> hostlun -map -volume Pool1:Volume011 -permission rw -wn 5005076b08897212 -name
Blade_Bay_1 -lun 0
```

Working ...

Current Machine Local Time: 03/08/2013 09:46:39 PM
Host LUN 0 for host 5005076b08897212 and host name Blade_Bay_1 mapped to volume 'Volume011' in 'Pool1'

```
<CLI> hostlun -map -volume Pool1:Volume013 -permission rw -wn 5005076b08a9e046 -name
Blade_Bay_4 -lun 0
```

Working ...

Current Machine Local Time: 03/08/2013 09:47:09 PM
Host LUN 0 for host 5005076b08a9e046 and host name Blade_Bay_4 mapped to volume 'Volume013' in 'Pool1'

```
<CLI> hostlun -map -volume Pool1:Volume012 -permission rw -wn 5005076023177a01 -name
Blade_Bay_3 -lun 0
```

Working ...

Current Machine Local Time: 03/08/2013 09:47:33 PM

Host LUN 0 for host 5005076023177a01 and host name Blade_Bay_3 mapped to volume 'Volume012' in 'Pool1'

<CLI> **detail pool -name Pool1**

Current Machine Local Time: 03/08/2013 09:49:52 PM

ID	Name	RaidType	OwnerCtrlr	TotalCap	AvailCap	Status	State	Degraded
1	Pool1	5	Slot 0	729GB	396GB	Viable-InTransition	ONV	No

State: OFN/SN=Offline Non-viable/Service Non-viable

ONF/OFF/SF=Online Failed/Offline Failed/ Service Failed

ONV/OFV/SV= Online Viable/Offline Viable/Service Viable

ONN=Online Non-viable/Pending Non-Viable; one or more drives are missing in this pool.

The pool state changes to ONV if missing drive(s) comes back to the pool.

The pool state changes to OFN if the user acknowledges the alert.

Drives:

Drive#	E:T	SerialNo	Cap	Pool	Usage	State	Mount State	Ct10	Ct11	RPM	FW level
0	2:1	3LM3N1ND	279GB	Pool1	GRP	OK	Online	1	0	15000	BA29
1	2:2	3LM1T1VM	279GB	Pool1	GRP	OK	Online	1	0	15000	BA2D
2	1:1	3LM3K1NP	279GB	Pool1	GRP	OK	Online	1	0	15000	BA29
3	1:2	3LM3PHJ5	279GB	Pool1	GRP	OK	Online	1	0	15000	BA29

Existing volumes :

Volumes	Cap	GrpName	RaidType	Status
Pool1:Volume011	111GB	Pool1	5	VBL TRN
Pool1:Volume012	111GB	Pool1	5	VBL TRN
Pool1:Volume013	111GB	Pool1	5	VBL TRN

- Next, perform data scrubbing. Data scrubbing is a feature that provides automatic, continuous synchronization during system use. This feature works in the background, and ensures that the redundant data and parity is correct. It keeps data “fresh” by running the following tasks:

- For RAID-5, 5E, 5EE, or 50: Reading data and rewriting the data parity.
- For RAID-1, 1E, 10, 1E0: Reading data and rewriting the mirror data.

The **datascrub** command is shown in Example 4-5.

Example 4-5 datascrub issued for the RAID array created

```
<CLI> datascrub -set -auto off  
Current Machine Local Time: 03/08/2013 09:48:42 PM  
setDataScrub: autcopy : 0  
Data Scrub Policy set successfully
```

4.9 Configuring the SAS Connectivity Module using CLI

This section describes using the CLI interface to configure the same storage allocation as used in 4.5, “Storage Configuration Manager” on page 187.

The CLI interface has the most comprehensive set of commands to configure the BladeCenter S. The CLI can be used for both the SAS connectivity and SAS RAID controller modules. The example configures storage using two DSM and two SAS Connectivity modules.

Clear the configuration of both SAS Connectivity modules by accessing the AMM command line and running the commands in Example 4-6.

Example 4-6 Clearing configuration from switches in bays 3 and 4 by using AMM

```
telnet 9.42.171.1  
  
username: USERID  
password:  
  
Hostname:          bcamm6  
Static IP address: 9.42.171.1  
Burned-in MAC address: 00:14:5E:E1:60:50  
DHCP:              Disabled - Use static IP configuration.  
Last login: Friday March 8 2013 13:49 from 9.42.171.252 (Web)  
  
system> clear -cnfg -T switch[3]  
OK  
system> clear -cnfg -T switch[4]  
OK  
system>
```

After the configuration is cleared and the SAS Connectivity Modules rebooted, use Telnet to log in to each of the SAS Connectivity Modules. Unlike the SAS

RAID Controller Module, the zoning profile must be configured on both SAS Connectivity Modules. User-defined configurations are zones 1-4. Decide which zone you want to use. The zone does not matter if it is the same on both SAS Connectivity Modules.

4.9.1 Understanding the zone matrix on the SAS Connectivity Module

After determining which user-defined zone [1-4] to use, determine how the NSSM handles zoning and masking of drives, blades, and external port by using the **zoneconfig** command:

Usage:

```
zoneconfig <cmd> [<arg2>]
```

Arguments:

```
<cmd>: subcommand to perform
Apply      - Apply a stored zone to hardware zone table
Compare    - Compare two zone configurations
Copy       - Copy zone configuration
Deny       - Clear a permission bit
Disable    - Disable zoning function
Erase      - Erase a stored zone
Get        - Display a stored zone configuration
GroupAssign - Assign group number to a SAS port
Permit     - Set a permission bit
SetName    - Set Zone configuration name
SetDesc    - Set Zone description
Stat       - Status of the zone configuration
```

For more information, enter

```
zoneconfig <cmd> ?
```

Log in to the SAS Connectivity Module command line. Run the **zoneconfig get <zone>** command, where <zone> is the user-defined zone number that you want to use. In Example 4-7, the zoning matrix is cut off at seventy columns because you are not interested in any other ports with this configuration:

Example 4-7 zoneconfig get command

```
MAIN> zoneconfig get 1
Zone Name: User Defined Config 01
Zone Description:
  Chassis: Any. SAS modules: 2. Default zone setting is each SAS mo
  dule port belongs to its own zone and no port can access any other port.
  Can be modified using SCM, the Telnet interface, or the embedded Web br
```

owner interface.

Zone Group Assignment for each SAS Port:

ID	SAS Port Name	Group ID
E1	External Port 1	30
E2	External Port 2	31
E3	External Port 3	32
E4	External Port 4	33
B1	Blade Slot Connection 1	34
B2	Blade Slot Connection 2	35
B3	Blade Slot Connection 3	36
B4	Blade Slot Connection 4	37
B5	Blade Slot Connection 5	38
B6	Blade Slot Connection 6	39
B7	Storage Module Connection 1	1
B8	Storage Module Connection 2	1

Zone Group Assignment for SM1 SAS Port:

ID	SAS Port Name	Group ID
UPL	External Port 1	1
D1	Disk Drive Connection 1	61
D2	Disk Drive Connection 2	62
D3	Disk Drive Connection 3	63
D4	Disk Drive Connection 4	64
D5	Disk Drive Connection 5	65
D6	Disk Drive Connection 6	66
D7	SES Device	60

Zone Group Assignment for SM2 SAS Port:

ID	SAS Port Name	Group ID
UPL	External Port 1	1
D1	Disk Drive Connection 1	91
D2	Disk Drive Connection 2	92
D3	Disk Drive Connection 3	93
D4	Disk Drive Connection 4	94
D5	Disk Drive Connection 5	95
D6	Disk Drive Connection 6	96
D7	SES Device	90

Permission Table:

[illegible]

second disk in each disk storage module and the second external port in the SAS Connectivity Module, and so on. Disable external ports 2-4 and enable disk ports 61 and 91 in the first SAS Connectivity Module for the blade in slot connection 1 to prevent the other blades from having access.

Configuration for the SAS Connectivity Module in Bay 3

Example 4-8 shows the configuration that is used on the SAS Connectivity Module installed in I/O Module Bay3.

Example 4-8 User-defined custom zone

```
MAIN> zoneconfig deny 1 34 31
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 34 32
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 34 33
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 35 30
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 35 32
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 35 33
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 36 30
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 36 31
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 36 33
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 37 30
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 37 31
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig deny 1 37 32
Stored Zone 1 has been modified successfully.
```

```
MAIN> zoneconfig permit 1 34 61
```

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 34 91**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 34 30**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 35 62**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 35 92**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 35 31**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 36 63**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 36 93**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 36 32**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 37 64**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 37 94**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 37 33**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 38 65**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 38 95**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 39 66**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 39 96**

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig SetDesc 1 SAS_Connectivity_1**


```
MAIN> zoneconfig SetName 1 SAS_config_all_blades_2_drives_1_ext_port
```

```
MAIN> zoneconfig apply 1
```

Zone 1 has applied to hardware zone table.

```
MAIN> zoneconfig stat
```

Zone Configuration Status.

```
  Zoning Function:      Enabled
  Current Zone:         SAS config all blades 2 drives 1 ext port
  Default Zone:         MFG EXIT Configuration
  Zone Apply for MAIN:  Applied
  Zone Apply for SM1:   Applied
  Zone Apply for SM2:   Applied
```

Configuration for the SAS Connectivity Module in Bay 4

The configuration for the SAS Connectivity Module in bay 4 is slightly different as shown in Example 4-9.

Example 4-9 User defined configuration for I/O Module 4

```
MAIN> zoneconfig deny 1 44 41
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 44 42
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 44 43
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 45 40
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 45 42
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 45 43
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 46 40
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 46 41
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 46 43
```

Stored Zone 1 has been modified successfully.

```
MAIN> zoneconfig deny 1 47 40
```

Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig deny 1 47 41**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig deny 1 47 42**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 44 76**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 44 106**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 44 40**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 45 77**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 45 107**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 45 41**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 46 78**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 46 108**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 46 42**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 47 79**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 47 109**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 47 43**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 48 80**
Stored Zone 1 has been modified successfully.

MAIN> **zoneconfig permit 1 48 110**
Stored Zone 1 has been modified successfully.

```

MAIN> zoneconfig permit 1 49 81
Stored Zone 1 has been modified successfully.

MAIN> zoneconfig permit 1 49 111
Stored Zone 1 has been modified successfully.

MAIN> zoneconfig SetDesc 1 SAS_Connectivity_1

MAIN> zoneconfig SetName 1 SAS_config_all_blades_2_drives_1_ext_port

MAIN> zoneconfig apply 1
Zone 1 has applied to hardware zone table.

MAIN> zoneconfig stat
Zone Configuration Status.
  Zoning Function:      Enabled
  Current Zone:         SAS config all blades 2 drives 1 ext port
  Default Zone:         MFG EXIT Configuration
  Zone Apply for MAIN:  Applied
  Zone Apply for SM1:   Applied
  Zone Apply for SM2:   Applied

```

After changing the configurations, review them to verify accuracy by using the **zoneconfig get 1** command as shown in Example 4-10. This displays the matrix for user-defined zone 1.

Table length: Because of the size of the matrix, “...” indicates empty rows or columns that have been removed so that the matrix fits the page and is easier to read.

Example 4-10 zoneconfig get 1 on I/O Module 3

```

MAIN> zoneconfig get 1
Zone Name: User Defined Config 01
Zone Description:
  Chassis: Any. SAS modules: 2. Default zone setting is each SAS mo
  dule port belongs to its own zone and no port can access any other port.
  Can be modified using SCM, the Telnet interface, or the embedded Web br
  owser interface.

Zone Group Assignment for each SAS Port:
ID  SAS Port Name          Group ID
---+-----+-----
E1  External Port 1         30
E2  External Port 2         31
E3  External Port 3         32

```

E4	External Port 4	33
B1	Blade Slot Connection 1	34
B2	Blade Slot Connection 2	35
B3	Blade Slot Connection 3	36
B4	Blade Slot Connection 4	37
B5	Blade Slot Connection 5	38
B6	Blade Slot Connection 6	39
B7	Storage Module Connection 1	1
B8	Storage Module Connection 2	1

Zone Group Assignment for SM1 SAS Port:

ID	SAS Port Name	Group ID
---+-----+-----		
UPL	External Port 1	1
D1	Disk Drive Connection 1	61
D2	Disk Drive Connection 2	62
D3	Disk Drive Connection 3	63
D4	Disk Drive Connection 4	64
D5	Disk Drive Connection 5	65
D6	Disk Drive Connection 6	66
D7	SES Device	60

Zone Group Assignment for SM2 SAS Port:

ID	SAS Port Name	Group ID
---+-----+-----		
UPL	External Port 1	1
D1	Disk Drive Connection 1	91
D2	Disk Drive Connection 2	92
D3	Disk Drive Connection 3	93
D4	Disk Drive Connection 4	94
D5	Disk Drive Connection 5	95
D6	Disk Drive Connection 6	96
D7	SES Device	90

Permission Table:

```

0000000000000000000000000000000000000000000000000000000000000000
3333333333...66666666667777777777888888888899999999990000000000111
0123456789...01234567890123456789012345678901234567890123456789012
0 0000000000...000000000000000000000000000000000000000000000000000
1 1111111111...111111111111111111111111111111111111111111111111111
...
30 1000100000...000000000000000000000000000000000000000000000000000
31 0100010000...000000000000000000000000000000000000000000000000000
32 0010001000...000000000000000000000000000000000000000000000000000
33 0001000100...000000000000000000000000000000000000000000000000000
34 1000000000...010000000000000000000000000000000000000000000000000
35 0100000000...001000000000000000000000000000000000000000000000000
36 0010000000...000100000000000000000000000000000000000000000000000
37 0001000000...000010000000000000000000000000000000000000000000000

```

[illegible]

The zoning matrix for I/O Module 4 is shown in Example 4-11.

Example 4-11 zoneconfig get 1 for I/O Module 4

```
MAIN> zoneconfig get 1
```

Zone Name: User Defined Config 01

Zone Description:

Chassis: Any. SAS modules: 2. Default zone setting is each SAS module port belongs to its own zone and no port can access any other port.

Can be modified using SCM, the Telnet interface, or the embedded Web browser interface.

Zone Group Assignment for each SAS Port:

ID	SAS	Port	Name	Group ID
----	-----	------	------	----------

-----+-----+-----

E1	External Port 1	40
----	-----------------	----

E2	External Port 2	41
----	-----------------	----

E3	External Port 3	42
----	-----------------	----

E4	External Port 4	43
----	-----------------	----

B1	Blade Slot Connection 1	44
----	-------------------------	----

B2 Blade Slot Connection 2 45

B3 Blade Slot Connection 3 46

B4 Blade Slot Connection 4 47

B5 Blade Slot Connection 5 48

B6	Blade Slot Connection 6	49
----	-------------------------	----

B7	Storage Module Connection	1	1
----	---------------------------	---	---

B8	Storage Module Connection 2	1
----	-----------------------------	---

Zone Group Assignment for SM1 SAS Port:

ID	SAS Port Name	Group ID
----	---------------	----------

-----+-----+-----

UPL External Port 1	1
---------------------	---

D1	Disk Drive Connection 1	76
----	-------------------------	----

D2 Disk Drive Connection 2 77

D3	Disk Drive Connection 3	78
----	-------------------------	----

D4 Disk Drive Connection 4 79

D5	Disk Drive Connection 5	80
----	-------------------------	----

D6 Disk Drive Connection 6 81

D7	SES Device	75
----	------------	----

Zone Group Assignment for SM2 SAS Port:

ID	SAS Port Name	Group ID
----	---------------	----------

-----+-----+-----

UPL External Port 1	1
---------------------	---

D1	Disk Drive Connection 1	106
----	-------------------------	-----

D2 Disk Drive Connection 2 107

D3	Disk Drive	Connection 3	108
D4	Disk Drive	Connection 4	109
D5	Disk Drive	Connection 5	110
D6	Disk Drive	Connection 6	111
D7	SES Device		105

Permission Table:

[illegible]

As you can see, each SAS Connectivity Module is unique. After you configure the zoning to meet your needs, you can power on the blades and begin installing the operation system.

Zone changes affect drives: It is important to power down all blades when you are making zone changes. Failing to do so can result in lost data, corrupted operating systems, and system and AMM failures.

4.10 Configuring external SAS ports for SAS tape

Both the SAS Connectivity Module and SAS RAID Controller Module have four external SAS ports on each that allow connections to external SAS devices, such as tape drives. These external ports are routed internally to the blades within the BladeCenter S chassis.

Access to these external ports from the blades is managed by zones. Only user-defined configurations can isolate access from a blade server to an external SAS port or ports. Predefined configurations allow all blades to access all

external SAS ports, and cannot be modified. This type of zoning is called a flat zone.

You can also use the SAS module to disable or enable the external SAS ports individually by using the CLI interface or Storage Configuration Manager. After an external port is disabled, a blade is unable to access that port even though its user-defined configuration specifies that it has access.

Note: Ensure that the latest firmware has been applied to the SAS module before you configure it.

To attach and configure an IBM SAS tape device to a SAS RAID Controller Module in a BladeCenter S chassis, complete these steps:

1. Ensure the tape drive and blade server you want to connect to are both powered on.
2. Download and install the tape drive drivers for the supported operating system on the blade (if required).
3. Attach the host end of the SAS interface cable to the SAS connector on the tape device.

4. Attach the other end of the host SAS interface cable to one of the four ports on the SAS RAID Module. In the example, the cable is attached to external port 1 on SAS Module in IO bay3 as shown in Figure 4-85.

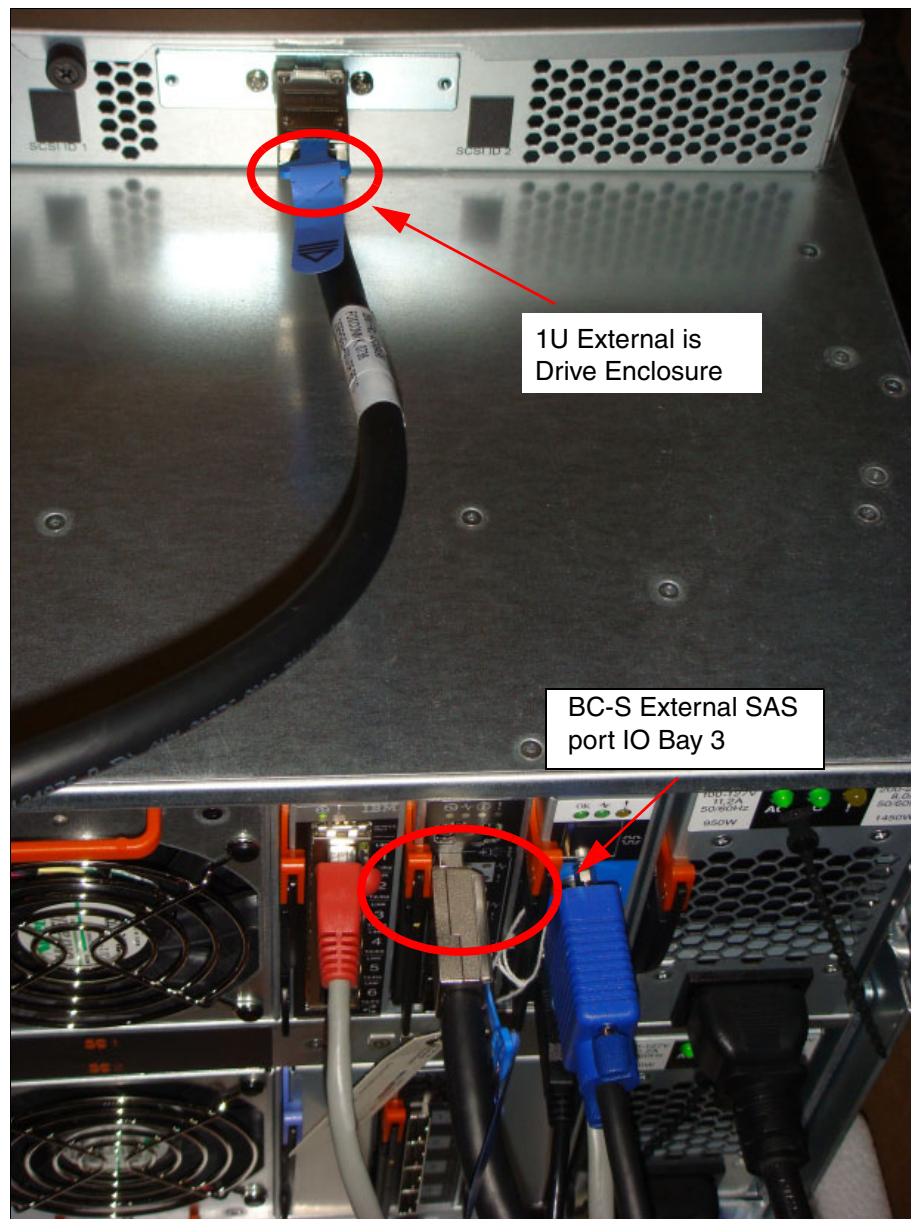


Figure 4-85 Cable connection to SAS external port 1 on IO Bay 3

5. Enable the external ports on the SAS RAID Module by using the Advanced Management Module:
 - a. Log in to the advanced management module.
 - b. Click **I/O Module Tasks** → **Admin/Power/Restart** → **I/O Module Advanced Setup**.
 - c. From the **Select a Module** menu, select **I/O Module 3**.
 - d. From the **Fast Post** menu, select **Enabled**.
 - e. From the **External ports** menu, select **Enabled**.
 - f. Click **Save**.
 - g. Repeat these steps for I/O Module 4.

Figure 4-86 shows these two options enabled.

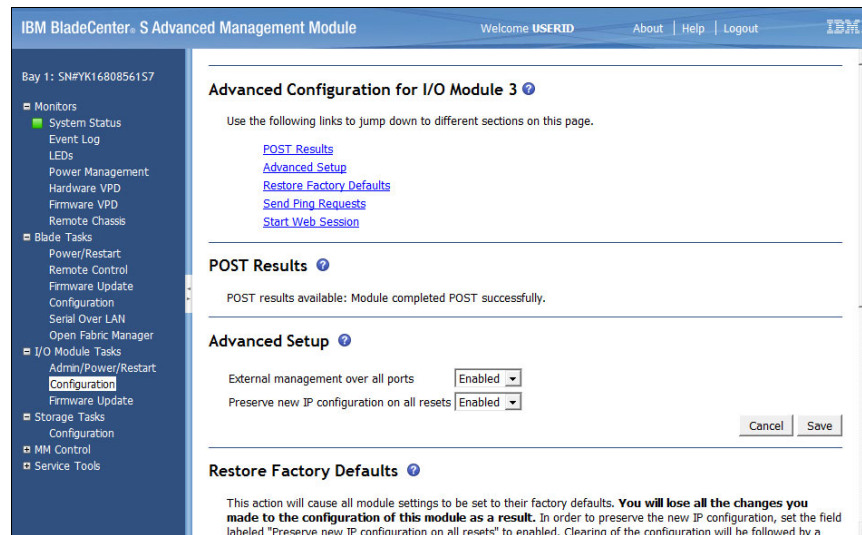


Figure 4-86 Fast Post and External Ports enabled on IO bay 3

6. Next, configure the SAS zoning in Storage Configuration Manager so that the backup blade server has exclusive access to the port. In Storage Configuration Manager, click **BC-S SAS RAID Module** → **Configuration** → **SAS Ports**.

7. Verify that the Current Device points to the correct SAS RAID Controller Module. In the example, this is SAS RAID Controller Module in IO bay 3, IP 9.42.171.67. Enable external port 1 by selecting the check box next to the port and then clicking **Enable**. The window refreshes and indicates a device is attached to the port, as shown in Figure 4-87.

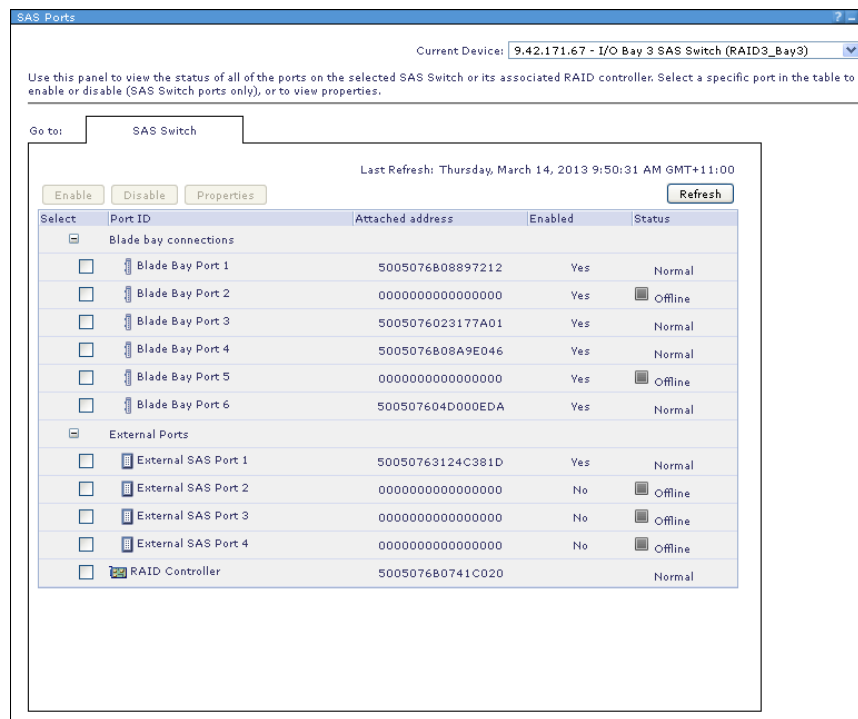


Figure 4-87 External SAS port 1 enabled on IO Bay3 module

8. The default SAS zone grants access to the port to all six blade servers. Change this setting to give exclusive access to blade server 1 by clicking **BC-S SAS RAID Module** → **Configuration** → **SAS Zoning**. A configuration window opens as shown in Figure 4-88.

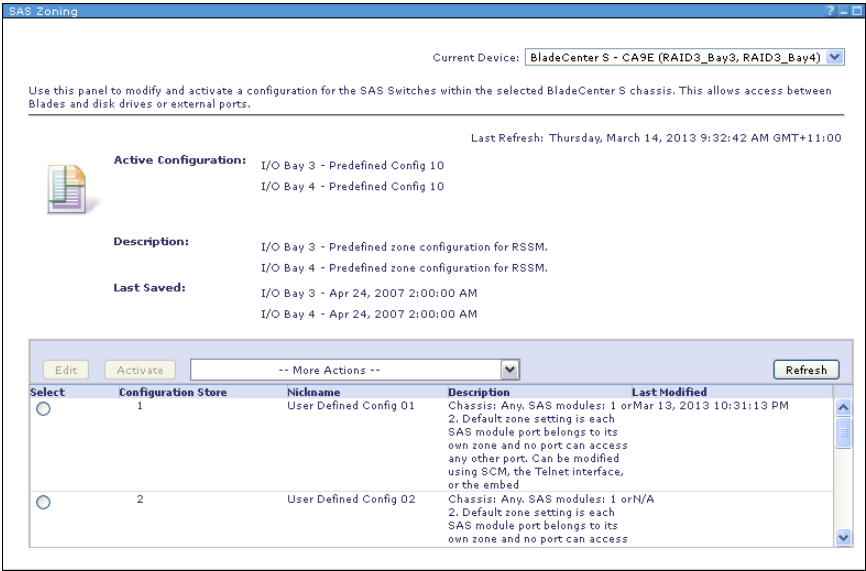


Figure 4-88 SAS zoning

9. Select configuration store 1. Click **Edit**, which is enabled. User Defined Config 01 grants access to blade servers to all external ports. The default configuration is shown in Figure 4-89.

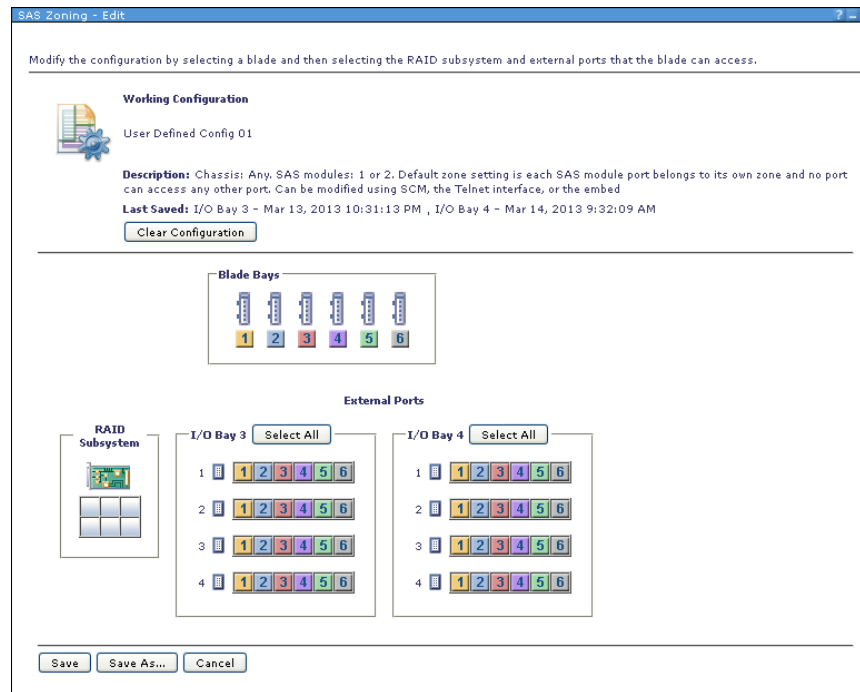


Figure 4-89 Default User Defined Config 01: All blades can access all ports

10. For ease, select **Clear Configuration**. Then, select Blade bay 1 and click **I/O Bay 3 slot 1**. This configures Blade server 1 to have exclusive access to external SAS port 1 on the SAS module in Bay 3. Figure 4-90 shows the completed configuration.

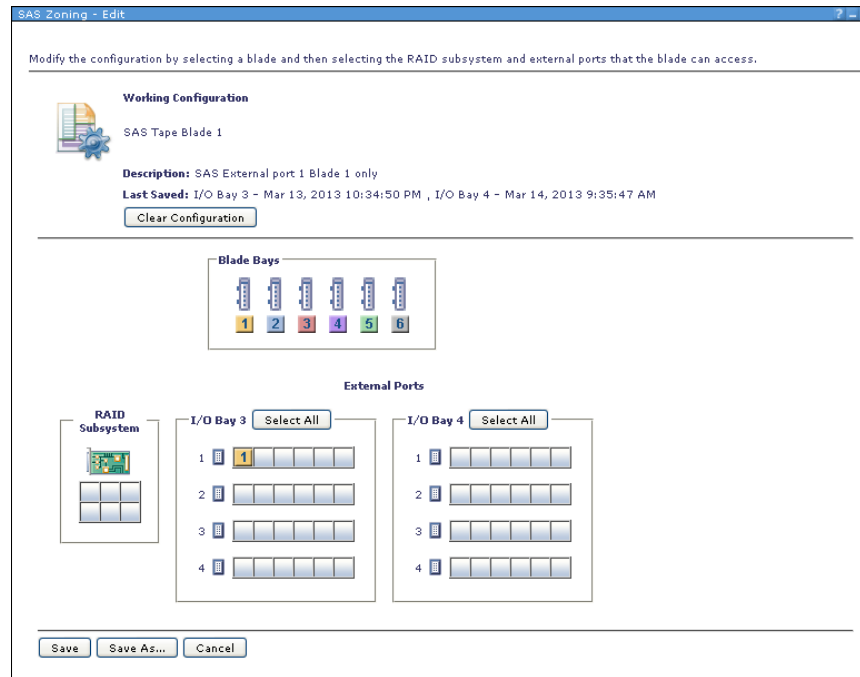


Figure 4-90 Blade bay 1 configured to have access to external port 1 bay 3

11. Click **Save As**. Name this configuration and provide a description to help understand its purpose. Click **OK** when finished.
12. Click **OK** at the next step to confirm the configuration.

13. Activate the new configuration by clicking it and selecting **Activation**. A prompt confirming this change is displayed. Click **OK**. The SAS zoning window updates to show the new configuration has been applied to IO Bays 3 and 4 as shown in Figure 4-91.

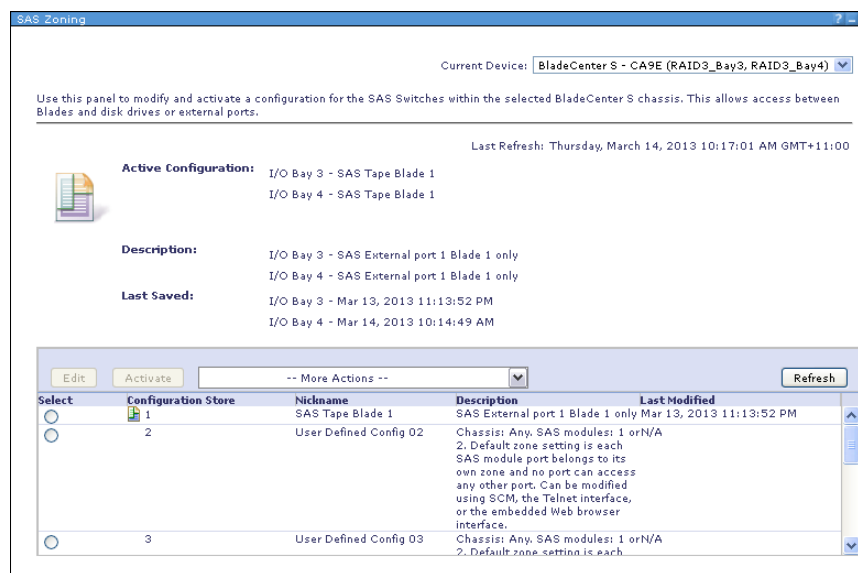


Figure 4-91 New zone configuration activated

14. Verify that the tape device is visible to your operating system. Log on to Blade server 1 remotely and check **Device Manager** as shown in Figure 4-92. For more information about device management, see the documentation that is supplied with your operating system.

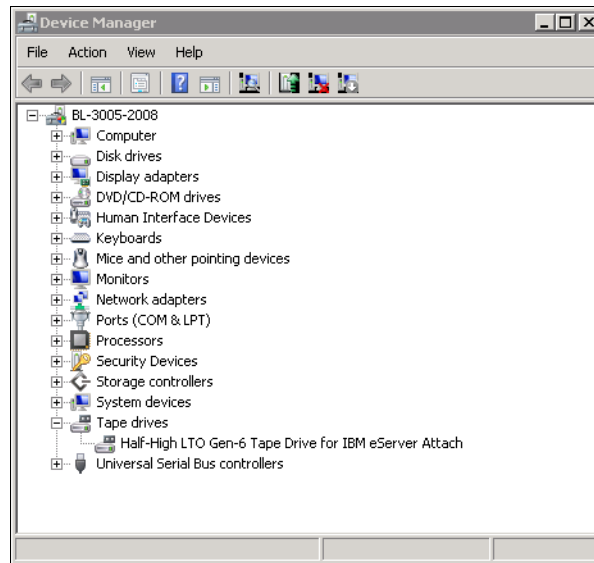


Figure 4-92 Tape drive recognized in Device Manager on blade server

Note: Simultaneous access by several servers cannot be handled by the tape device, so this situation must be avoided.

4.11 Firmware updating

This section describes updating firmware of the various storage components:

- ▶ 4.11.1, “SAS Connectivity Module firmware” on page 290
- ▶ 4.11.2, “SAS RAID Controller Module firmware” on page 294
- ▶ 4.11.3, “Updating firmware for SAS Connectivity Card” on page 304

4.11.1 SAS Connectivity Module firmware

The SAS Connectivity Module and Disk Storage Module firmware can be updated by several methods. Three are documented here:

- ▶ “Updating firmware using the web browser interface”
- ▶ “Updating firmware using the CLI” on page 292
- ▶ “Updating firmware using Storage Configuration Manager” on page 294

Updating firmware using the web browser interface

Complete the following steps to update firmware by using the web browser interface:

1. Download the latest firmware for the SAS Connectivity Module.
2. Extract the files into a local folder.
3. Open a browser and connect to the SAS Connectivity Module by using the IP address that was assigned in the AMM.

Note: All blades that use disks in the storage modules must be powered off before you update the firmware for the SAS Connectivity Modules or the Storage Modules. All the disk paths are shut down during the firmware update process.

4. After you are logged in, click **Health and Monitoring** → **Update Firmware**.

5. The current firmware revision level is displayed for the SAS Connectivity Module and the Disk Storage Modules as shown in Figure 4-93. In the Target Device field, select **SAS module**. Browse and select the firmware file (which has a file extension of .fuf). Click **Install** to begin the process.

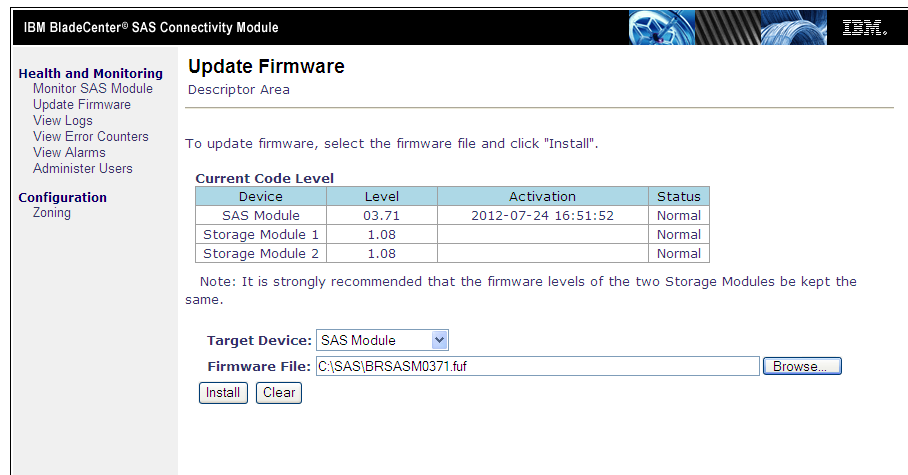


Figure 4-93 SAS Connectivity module firmware update window

6. A warning message is displayed as shown in Figure 4-94 stating that the firmware update process will shut down all data paths to the disks through the switch. Click **OK** to continue.

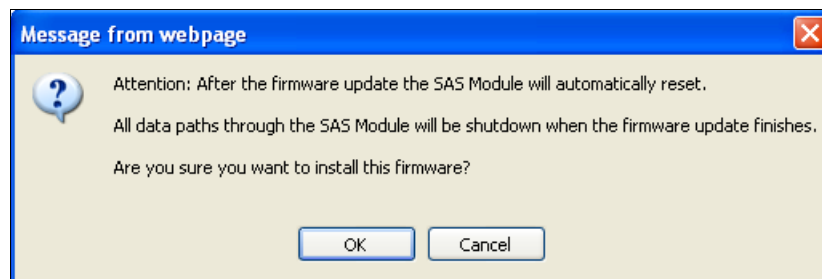


Figure 4-94 Confirming firmware update

7. Several informational messages are displayed that give progress status. After it completes successfully you are presented with a firmware successful window that tells you that the SAS module will be rebooted automatically. This message is shown in Figure 4-95.

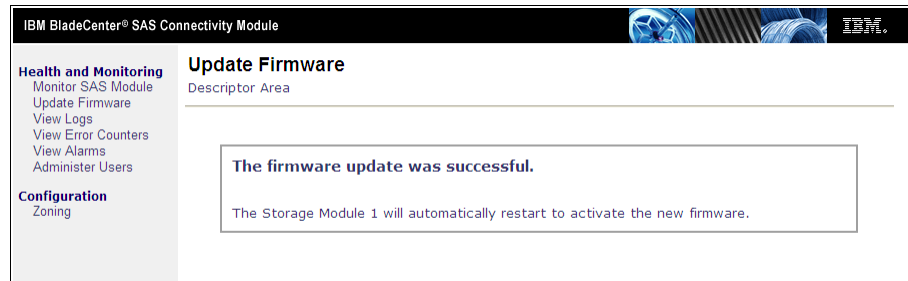


Figure 4-95 Firmware update successful

Updating both SAS modules: If you are updating SAS module firmware, update the firmware on both SAS modules if you have two of them. Open a new browser window and log on to the second SAS module to update its firmware. Each SAS module has a separate web browser interface that only supports updating its own firmware.

8. Repeat this step for the Disk Storage Modules, ensuring you select the firmware files for them. A final notification is displayed confirming that the firmware update was successful, and that the SAS module will be rebooted automatically.

Consideration: Updating the firmware of each Disk Storage Module takes about 12 minutes. Updating the firmware of each SAS module takes about six minutes.

Updating firmware using the CLI

The SAS Connectivity module can be updated by using the command-line interface. Complete the following steps:

1. Download the latest firmware from <http://ibm.com/support>.
2. A tftp server is required to host the firmware file. The example uses the tftp service on the AMM. The firmware must be uploaded to the available AMM storage. To enable tftp on the AMM, log on to the AMM by using a web browser. Then, click **MM Control** → **Network Protocols** → **Trivial File Transfer Protocol (TFTP)**, select **Enabled**, and click **Save**.

3. Power off all blades that have access or assigned storage through the SAS Connectivity module.
4. Telnet into each SAS Connectivity Module as shown in Example 4-12.
5. Issue the **fwdownload** command with the appropriate options. Example 4-12 shows the command syntax and the output when the update is successful.

Example 4-12 Updating the SAS module firmware by using CLI

```
C:\telnet 9.42.171.67
username: USERID
password:
MAIN> fwdownload 9.42.171.1 BRSASM0371.fuf
Firmware Download from TFTP Server
  TFTP Server IP Address....9.42.171.1
  File Name....."BRSASM0371.fuf"
  Silent Mode.....No

----ATTENTION-----
After the firmware update the SAS Module will automatically reset.
All data paths through the SAS Module will be shutdown when the
firmware finishes.
Are you sure you want to install this firmware? (y/n)Y
Start background erasing Flash Memory.
Erasing completed.
Please enter ANY key to stop progress display.
Connection has established successfully.
  FWREVID header received: BRSASM0371
  MATCHID header matched OK.
  MAXIMIC header received and parsed OK.
1241088 bytes received.
CRC over the entire burn checked OK.
Entire firmware image has been received successfully.
All data received. Start activation...
  Sense pin now strapped HIGH.

Connection to host lost.

C:\
```

Updating firmware using Storage Configuration Manager

At the time of writing the Storage Configuration Manager, SCM reported that it did not support updating the firmware of the SAS Connectivity Module. You see the error message shown in Figure 4-96.

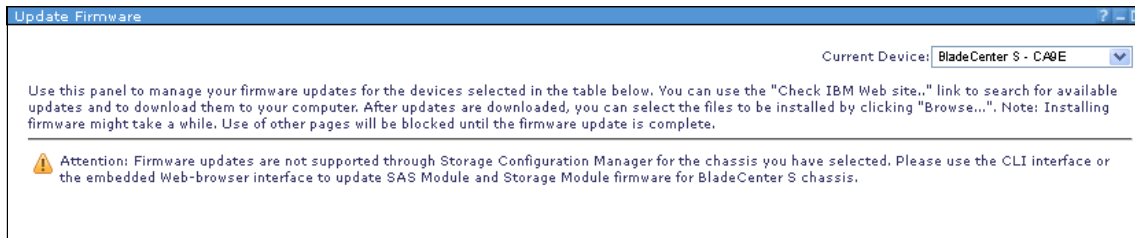


Figure 4-96 SAS connectivity module firmware unsupported in SCM

4.11.2 SAS RAID Controller Module firmware

The SAS RAID Controller module firmware can be updated by several methods. This section provides the necessary steps to complete a firmware upgrade. When you are doing a firmware update to the SAS RAID Controller module, the following items are updated:

- ▶ SAS RAID Controller Module(s)
- ▶ Disk Storage Modules 1 and 2
- ▶ Battery Backup Units
- ▶ SAS switch that is embedded in the SAS RAID Controller Module

Updating firmware using the CLI

The SAS RAID Controller module can be updated by using a CLI. The readme file instructions for the firmware are must be followed closely to ensure a successful update.

The example configuration consists of the following components:

- ▶ One SAS RAID Controller module, IP address 9.42.171.68
- ▶ A PC running Windows from which the updates are performed
- ▶ Python Version 2.5.4, which can be downloaded from:

<http://www.python.org/getit/releases/2.5.4/>

Versions of Python: Testing in the lab indicated that later versions of Python do not work.

There is only one SAS RAID Controller Module in the example, but a dual configuration is upgraded in the same manner.

Complete the following steps to perform the upgrade:

1. Download the latest firmware from <http://ibm.com/support>.
2. Download and install the supported version of Python. Refer to the readme file on how to set up the environment variables for Python to run on your PC.
3. Before starting the firmware update, check and resolve all persistent alerts. This can be checked by viewing the Active Alert list for the SAS RAID Controller Module.
4. Telnet into the IP address of the RAID controller of the SAS RAID Controller Module set earlier in the AMM. Ensure that you are using the RAID controller IP address, not the IP address of the embedded SAS switch.
5. The SAS RAID Controller Modules *must* to be in Service mode before any firmware can be applied. If they are not, you receive an error message that advises you of this fact. To put the modules in service mode, run the **shutdown** command that is shown in Example 4-13.

Example 4-13 Shutting down the SAS RAID Controller Module

```
c:\telnet 9.42.171.67
MontaVista(R) Linux(R) Professional Edition 3.1
Linux/ppc 2.4.20_mvl31-alc

(none) login: USERID
Password:
Linux (none) 2.4.20_mvl31-alc Rel H-2.4.20.12 TuesWed Jun 17 15:03:32 PDT 2009
ppc unknown

MontaVista(R) Linux(R) Professional Edition 3.1

<CLI> list controller
Current Machine Local Time: 03/05/2013 02:13:43 PM
```

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

```
<CLI> shutdown -ctlr 0 -state servicemode
Current Machine Local Time: 03/05/2013 02:17:19 PM
Shutdown Command accepted.

<CLI> list controller
Current Machine Local Time: 03/05/2013 02:17:23 PM
```

Ctlr#	Controller	Status	Ports	LUNs
0	Ctlr0	SERVICE	-	--
1	Ctlr1	NOTAVAILABLE	1	--

6. Check to see whether the firmware that you are applying supports Concurrent Code Load. For firmware 1.2.4.011 Single controller configuration, Non-Concurrent Code Load must be used. The firmware update command reflects this with the additional **-n** flag as shown in Example 4-14. To update your hard disk drive firmware, you must also be in Non-Concurrent Code Load.

7. Open a command prompt window. To start the firmware update, run the following command:

```
ibm_fw_bcs_w_s0cl-N.N.N.NNN_windows_noarch.bat -i X.XXX.XXX.XXX -n
```

Where:

- N.N.N.NNN is the build number of the firmware download package. In the example, the build number is 1.2.4.011.
- X.XXX.XXX.XXX is the IP address of one the RAID Controllers. In the example, the IP address is 9.42.171.68.

Remember: This command assumes that the default passwords have not changed.

8. Example 4-14 shows the command and responses that are issued in the command window.

Example 4-14 Updating the RSSM firmware from the CLI

```
C:\firmware>ibm_fw_bcs_w_s0cl-1.2.4.011_windows_noarch.bat -i 9.42.171.68 -n
```

```
Unpacking image ibm_fw_bcs_w_s0cl-1.2.4.011_windows_noarch.bat.
```

```
.....
```

```
.....
```

```
Image unpacked.
```

```
Package name : rsm.1.2.4.011
```

```
Package level : 1.2.4.011
```

```
Product : rsm
```

```
Image created : Sep24201210:22:39(GMT)
```

```
Raid ctrl uBoot version : H-1.1.4.6
```

Raid ctrlr code version : H-2.1.3.4
Raid ctrlr Linux version : H-2.4.20.12
BMC version : SOBT10A
FPGA version : 01.07
SES version : 0107
BBU version : 58.0
DSM version : 1.08
SAS switch version : R1.07

Initializing firmware update - please wait.....

SAS RAID Controller Module Firmware Update
Image : rssp.1.2.4.014
Non-Concurrent Disk drive firmware update progress:
0...10...20...30...40...50...60...70...80...90..100 %Complete

=====>

Step 8 progress:
0...10...20...30...40...50...60...70...80...90..100 %Complete

Msg 46 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 47 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 48 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 49 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 50 Waiting another 5 sec for 9.42.171.68 CLI.

Non-Concurrent Disk drive firmware update progress:
0...10...20...30...40...50...60...70...80...90..100 %Complete

=====>

Step 8 progress:
0...10...20...30...40...50...60...70...80...90..100 %Complete

=====>

Msg 52 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 53 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 54 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 55 Waiting another 5 sec for 9.42.171.68 CLI.
Msg 56 Controller 0 is PRIMARY - CLI is online.

* SUCCESSFUL Non-Concurrent Disk drive firmware update ! *

Image unpacked.
-bash-4.1\$

-
9. If the controllers have custom passwords, the following syntax must be used:

```
ibm_fw_bcs_w_s0cl-N.N.N.NNN_windows_noarch.bat -i X.XXX.XXX.XXX  
-passwd XXXXXXXX -sas_p1 XXXXXXXX -sas_p2 XXXXXXXX -ftx_pwd XXXXXXXX
```

N.N.N.NNN is the build number of the downloaded package, X.XXX.XXX.XXX is the IP address of either SAS RAID controller, and the following passwords are provided:

-passwd	The Controller CLI password
-sas_p1	CLI password for the SAS Switch in bay 3
-sas_p2	CLI password for the SAS Switch in bay 4
-ftx_pwd	Management interface password

10. The firmware update completes and tells you whether the process was successful. If it fails, check the alerts and clear any issues that are associated with these alerts.
11. Reboot the SAS RAID Controller clear any pre-verify failure alerts.
12. After rebooting, check the firmware levels to see whether they were actually updated. In some cases, a failure message can occur, but the update still takes place.
13. If the process fails, check the `sbinst.py.log` file in the directory that you ran the batch file. In the readme file instructions and the example in Example 4-14 on page 296, the batch file is run from `C:\code\load`.
14. Apply the firmware update again if needed.

Updating the firmware using Storage Configuration Manager

SCM has features to update the firmware of the SAS RAID Controller Modules, the Disk Storage Modules, and the Battery Backup Units.

Unreliable procedure: During lab tests, the Storage Configuration Manager firmware update process was not reliable. Some tests generated error messages that the update failed, but when the SAS RAID Controller Module was checked, the firmware was indeed updated. The instructions are provided here for reference.

To perform the update, complete the following steps:

1. Cease all host activity to volumes managed by the SAS RAID Controller Module. Generally, perform this update in low peak time and shut down all blade servers that access storage managed by the SAS RAID Controller Module.
2. In SCM, click **BC-S SAS RAID Controller** → **Health** → **All Resources** to display the current SAS module environment as shown in Figure 4-97.

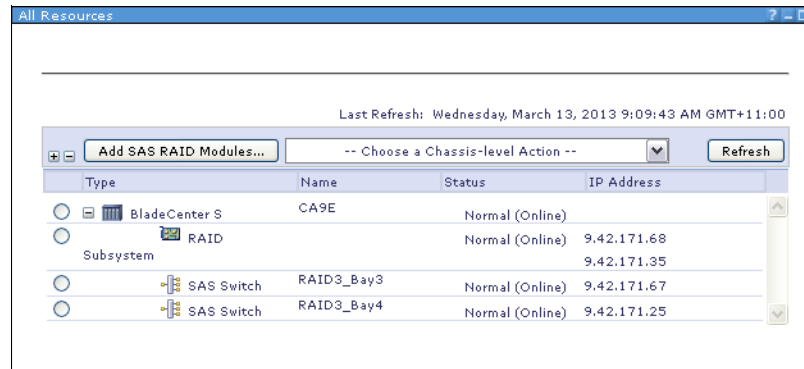


Figure 4-97 SAS RAID Controller on BladeCenter S

3. Check that no long Running Tasks are active. To do this, click BC-S SAS RAID Module → **Jobs and Processes** → **Long Running Tasks** as shown in Figure 4-98.

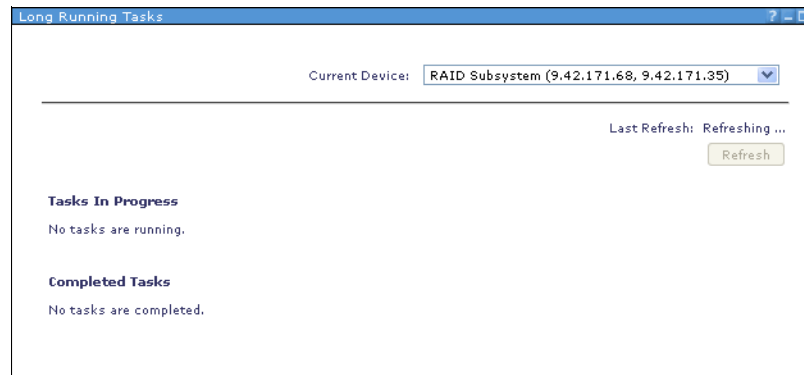


Figure 4-98 Checking that no long running tasks are active for the RAID subsystem

4. Click BC-S SAS RAID Module → **Health** → **Physical View**.
5. Click the Controllers tab, then click one of SAS RAID Controller Modules.

- Click the **Select a Controller Action** menu and select **Service** → **Shutdown and Recover** as shown in Figure 4-99.

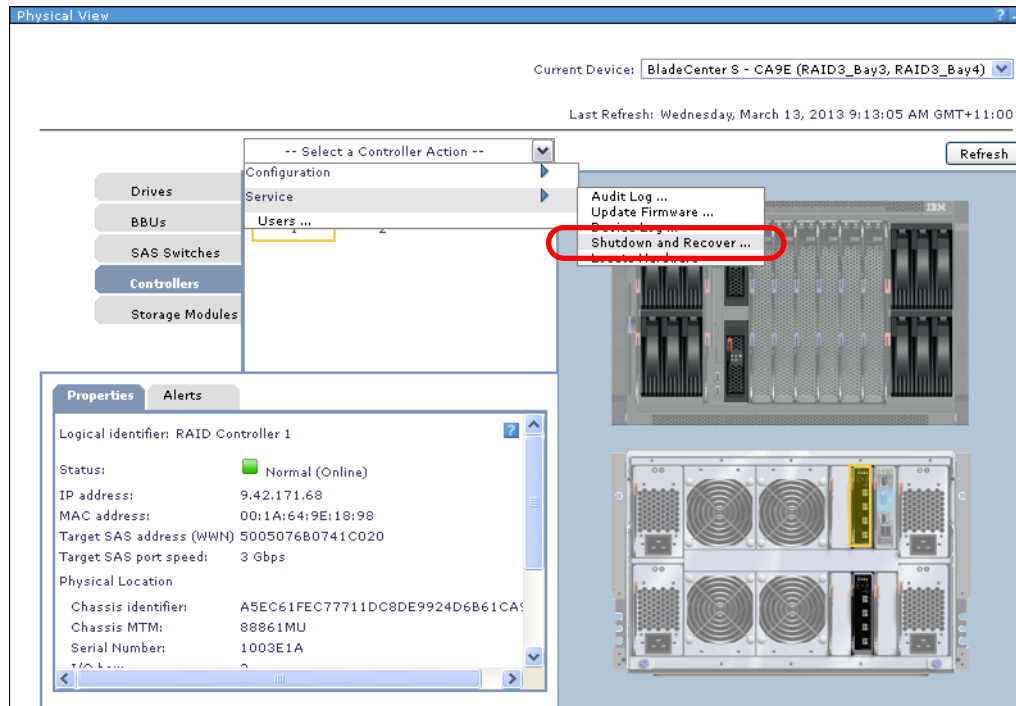


Figure 4-99 SAS RAID Controller Module shutdown and recover selection

7. Select **Shutdown to service mode** and then select **Both Controller 1 and 2**, as shown in Figure 4-100.

The screenshot shows a window titled "Shutdown and Recover". At the top right, it says "Current Device: RAID Subsystem (9.42.171.68, 9.42.171.35)" with a dropdown arrow. Below that, it says "Last Refresh: Wednesday, March 13, 2013 9:26:23 AM GMT+11:00". A "Refresh" button is to the right. A warning message states: "Only use this page when following a documented alert recovery procedure or when working with technical support. Shut down any server Blades mapped to volumes in this storage subsystem, or stop the applications using the storage in this storage subsystem, prior to shutdown of the controller. The controller options change based on the action selected." Below this is a section "Select an action:" with three radio buttons: "Shut down to service mode" (selected), "Prepare for removal", and "Reboot". A note follows: "Note: After removing the SAS RAID Module from the system, run Discover Hosts to update the host port definitions in the RAID subsystem." Below the note are two more radio buttons: "Bring online from service mode" and "Both Controller 1 and 2." (selected). A section "Select controllers to shut down or recover:" follows, with two rows: "Controller 1: 9.42.171.68 - I/O Bay 3 (Main)" and "Controller 2: 9.42.171.35 - I/O Bay 4 (Main)", each with a green "Normal (Online)" status indicator. At the bottom are "OK" and "Cancel" buttons.

Figure 4-100 Shutdown of both SAS RAID controllers

8. A confirmation indicating that the SAS RAID Controller Modules will be shut down to service mode and a warning to shut down any mapped hosts using the storage is displayed. Click **OK** to proceed.

9. After you receive confirmation that both SAS RAID Controller Modules are in Service Mode, as shown in Figure 4-101, click BC-S SAS RAID Module → **Service** → **Update Firmware**.

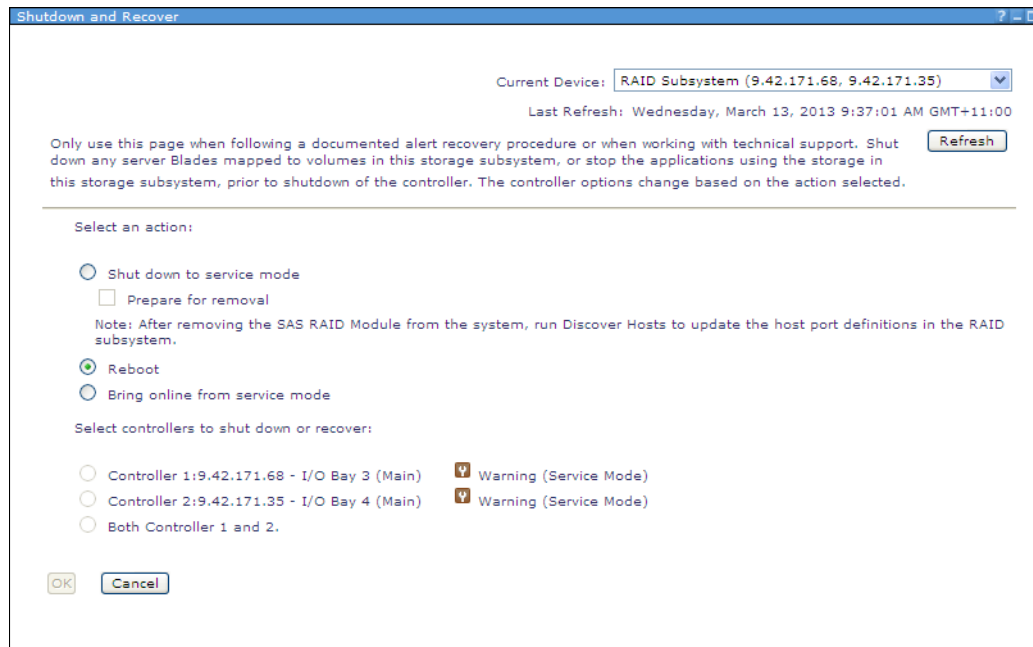


Figure 4-101 Both SAS RAID Controllers in service mode

10. Select the appropriate SAS RAID Controller Module again from the **Current Device** drop box if Storage Configuration Manager is managing more than one chassis.
11. Click **Browse** and locate the relevant firmware update file.

12. Click to clear **Verify the RAID subsystem is ready for firmware updates before beginning the install process (Default)** as shown in Figure 4-102.

The screenshot shows the 'Update Firmware' window. At the top, there's a 'Current Device' dropdown menu set to 'RAID Subsystem (9.42.171.68, 9.42.171.35)'. Below this, a link points to the 'Updating firmware' help topic. A section titled 'Devices selected for firmware updates:' lists several components: RAID Subsystem and both SAS switches, RAID Controller 3 (9.42.171.68), RAID Controller 4 (9.42.171.35), Storage Module 1, Storage Module 2, BBU 1, BBU 2, SAS Switch in I/O Bay 3 (9.42.171.67), and SAS Switch in I/O Bay 4 (9.42.171.25). Below this is a table for 'Current Firmware Bundle Level:'.

Type	Level
Controller	1.2.3.006
SAS Switch in I/O Bay 3	R1.07
SAS Switch in I/O Bay 4	R1.07

Below the table, there's a 'Download Firmware Bundle:' section with a link to the IBM BladeCenter support website. Then, an 'Install Downloaded Firmware Bundle:' section instructs the user to enter the path and file name of the firmware bundle or click 'Browse'. The path 'C:\ibm_fw_bcsfw_s0cl-1.2.4.014_anyos_noarch_scm.zip' is entered. Below this, a message states: 'The RAID controller(s) is/are in service mode. Select Install to proceed with non-concurrent firmware update.' There are two checkboxes: 'Verify the RAID subsystem is ready for firmware updates before beginning the install process.(Default)' which is unchecked, and 'Update pre-verify has not been run on the RAID controllers' which is checked. At the bottom, there is an 'Install' button.

Figure 4-102 Firmware selection and installation

13. Click **Install**. Click **OK** to confirm that you are ready to update the SAS RAID Controller Modules. The process commences, and you are provided with a progress indicator.
14. After the firmware update completes, click BC-S SAS RAID Module → **Physical View**.
15. Select the appropriate SAS RAID Controller Module from the **Current Device** drop box if Storage Configuration Manager is managing more than one chassis.
16. Click the Controllers tab.
17. Click one of the SAS RAID Controller Modules.

18. Click the **Select a Controller Action** menu and select **Service** → **Shutdown and Recover**.
19. Select **Bring online from service mode** and select a controller, then click **OK**.

Bringing the second controller online: At the time of writing, the option to bring both controllers online at the same time is not available. You might need to manually refresh the web page and navigate back to the Shutdown and Recover window to bring the second controller back online.

20. Repeat the process to bring the second controller online.

4.11.3 Updating firmware for SAS Connectivity Card

Blade servers such as the HS23 and PS703 connect to the BladeCenter S Disk Storage Module by way of a SAS Connectivity (CIOv), part number 43W4068. The expansion card is installed internally into the blade server.

Updated support: The CIOv daughter card is now supported on the Power Systems PS700, PS701, PS702, and PS703 blade servers.

For more information about the SAS Connectivity Card (CIOv), see the IBM Redbooks Product Guide at:

<http://www.redbooks.ibm.com/abstracts/tips0701.html>

To apply the latest version of the firmware and driver for SAS Connectivity Card (CIOv) for IBM BladeCenter, visit IBM Fix Central. Search for your blade by machine type or model number and choose your operating system. The latest drivers and firmware are available under the SAS component type.

Fix Central is at:

<http://ibm.com/support/fixcentral/>

To upgrade the firmware using Windows, complete the following steps. The following example uses the HS22 blade server.

1. Confirm the relevant blade server has the expansion card installed. Log in to the AMM, then click **Hardware VPD** → **Expansion Card** on the server you are upgrading the firmware on.

An inventory window for the Expansion Card is displayed as shown in Figure 4-103.

BladeCenter Vital Product Data	
Inventory Ports	
Slot 1 - Expansion Card Information	
Property	Value
Product Name	SAS Connectivity Card (CIOv) for IBM BladeCenter
Description	SAS Conn Card
Part Number	49Y8009
FRU Number	46C4069
FRU Serial No.	YK11900CC131
Hardware Revision	4
Manuf. Date	5010
UUID	0C9E D235 08AA 11E0 B7E2 0013 D4E3 2F93
Manufacturer	IBM (FOXC)
Manuf. ID	20301
Product ID	181

Figure 4-103 Expansion card information from AMM Hardware VPD

2. Start the firmware executable file. This opens a package summary window with version number and applicable hardware as shown in Figure 4-104. Click **Next**.

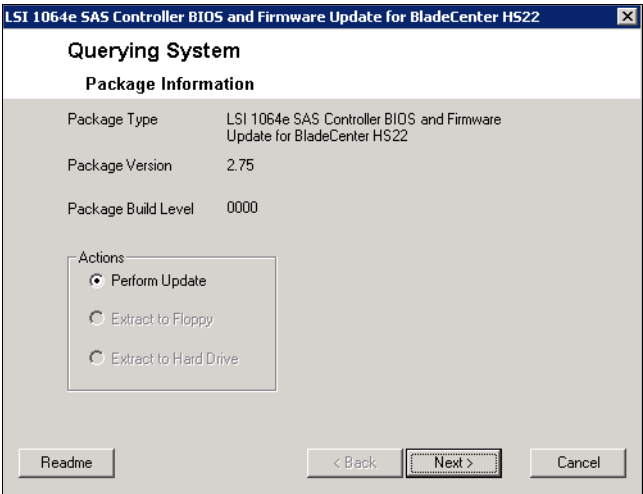


Figure 4-104 Firmware summary for HS22 with LSI 1064e and expansion card

3. A Ready to Update System window is displayed. Click **Update** to proceed.
4. After the process is complete, you see a window giving the update success status. Figure 4-105 shows a successful update.

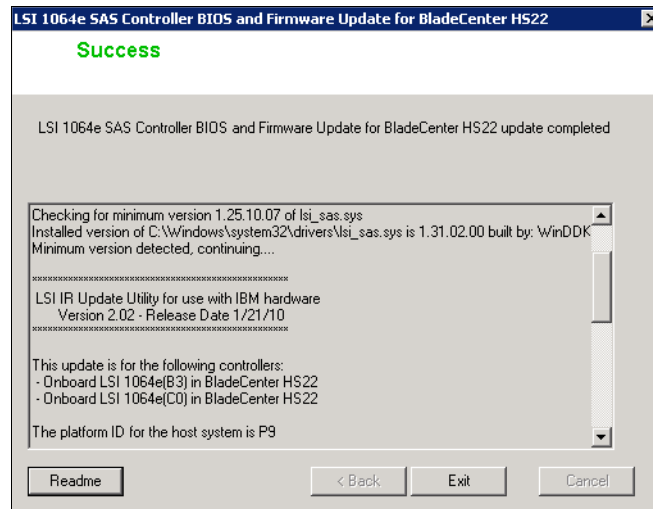


Figure 4-105 Firmware applied successfully

To update the firmware by using AIX, complete the following steps. In this example, a PS700 blade server that is running AIX 5.3 TL12 SP4 is used.

1. Download the firmware from Fix Central
2. Copy the firmware to /etc/microcode.
3. Unmount any file systems on the disks in the storage module.
4. If you are booting from the disks in the disk storage module, reboot from a diagnostics or maintenance mode
5. With the firmware file in /etc/microcode, run this command:
`diag -cd sissas0 -T"download -f"`
6. Run **diag** commands on sissas0 to ensure correct functionality as shown in Example 4-15.

Example 4-15 Updating the SAS firmware from AIX

```
# diag -cd sissas0 -T"download -f"
Installation of the microcode has completed successfully.
The current microcode level for sissas0 is 0420003a.
```

Please run diagnostics on the adapter to ensure that it is functioning properly.


```
# diag -cd sissas0
Starting diagnostics
Testing sissas0
Ending diagnostics.
```

4.12 Firmware update for disk drives

IBM disk drives might at some point in their lifespan require new firmware. New firmware requires the drives to be updated. How this is done depends on how the hard disk drives are configured on the BladeCenter S chassis. This section describes how to update the firmware on the following hard disk drive configurations:

- ▶ HDD installed internally in a blade server
- ▶ HDD installed in a DSM connected to a SAS Connectivity Module
- ▶ HDD installed in a DSM connected to a SAS RAID Controller Module

4.12.1 Firmware update for internal Blade HDD

Internal storage on a Blade server can be updated by using a bootable CD-ROM or by using the firmware update program for your applicable operating system.

This example involves a Blade Server HS22 with two internal SAS HDD. The example boots from a CD image that contains the firmware update.

1. Download the ISO image file for the IBM SAS/SATA hard disk drive update program v1.12.01 - IBM BladeCenter and System x. This is the direct link to the update:

<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-62832>

2. Burn the ISO image to a CD.
3. Ensure that the media tray is assigned to the blade server where the drives are installed.

4. Power on the Blade server, and boot from the CD-ROM. A Linux boot loader starts, ultimately displaying the IBM Drive Update window as shown in Figure 4-106. In this example, the update program has located two supported hard disk drives attached to this blade. Both require a firmware update.

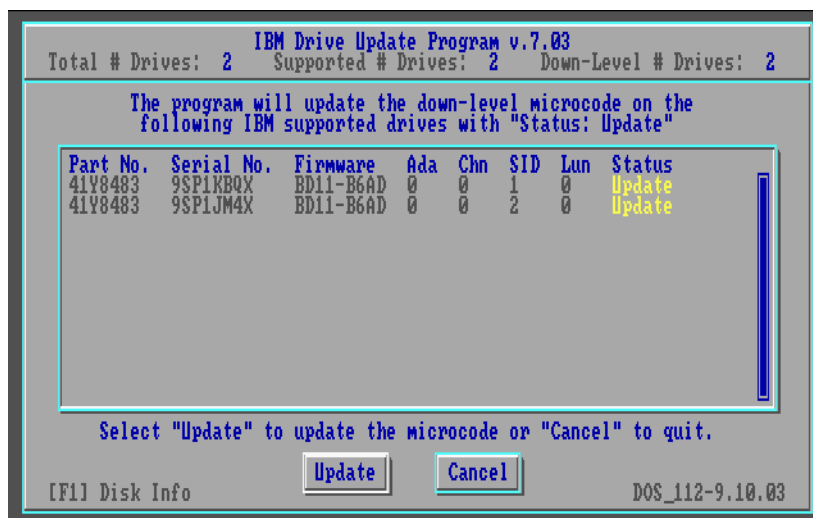


Figure 4-106 Drive update program for firmware update 1.12.01

5. Click **Update** when ready.

6. The firmware process completes and advises the status of the update. In this example, both hard disk drives are updated, and the new firmware version is listed as shown in Figure 4-107.

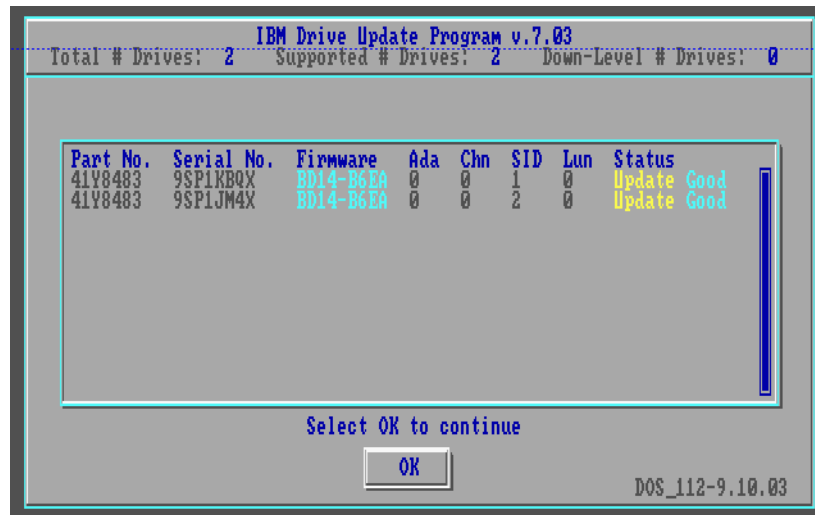


Figure 4-107 Firmware update successful

7. Click **OK** to move to the summary window. After you review this window, click **OK**.
8. The IBM Drive Update Program window, as seen in Figure 4-108, advises you to remove the CD-ROM and when ready click **OK** to restart the server.

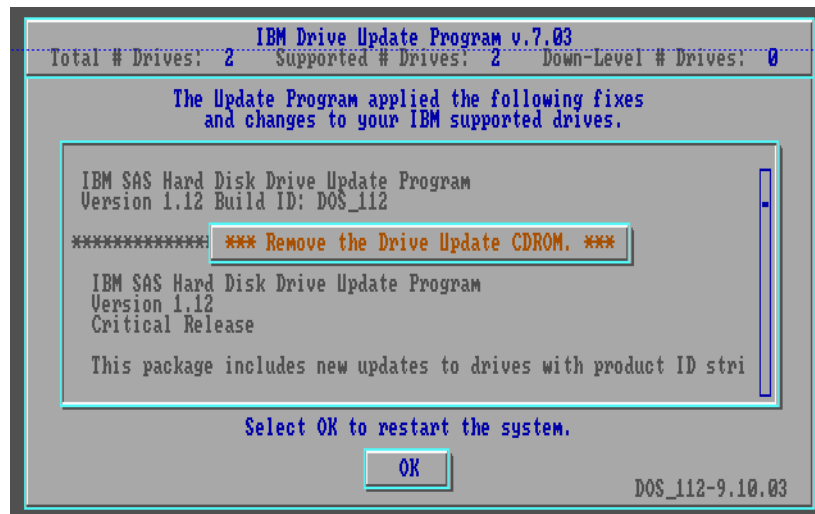


Figure 4-108 Firmware update reboot window.

Blade server - Firmware update program

This example uses a Blade Server HS22 with two internal SAS HDD running Windows 2008 Server 64 bit. To update the firmware by using the downloaded firmware update program, complete these steps:

1. Download the latest firmware update from the IBM website. This example uses IBM SAS/SATA hard disk drive update program v1.12.01 - IBM BladeCenter and System x, which is available at:
<http://ibm.com/support/entry/portal/docdisplay?lnidocid=MIGR-5078767>
2. Log in to the Blade Server you are applying the update to. First, review the current firmware revision on the hard disk drives:
 - a. Click **Start** → **Control Panel** → **System and Security** → **System** → **Device Manager**.
 - b. Expand the **Disk drives** list and select a hard disk drive.
 - c. Double click the hard disk drive and then click the Details tab.
 - d. Select **Hardware Ids** in the property menu.
 - e. The selected hard disk drive firmware version is displayed. The example drive is at SB25 as seen in Figure 4-109. Click **OK** when finished.

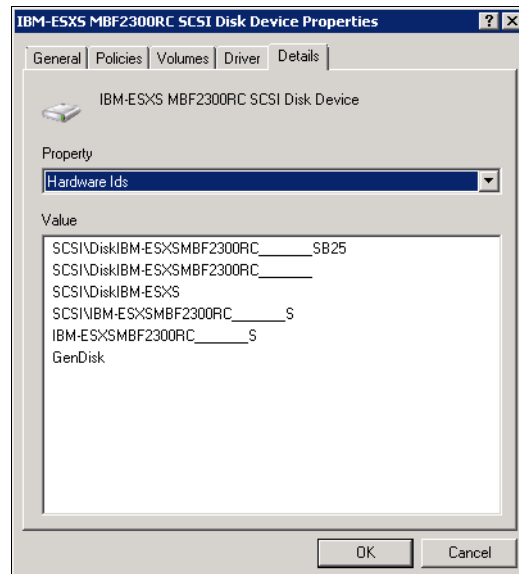


Figure 4-109 Firmware version of local HDD on Blade Server

3. Start the downloaded file. The version used in the example is `ibm_fw_hdd_sas-1.12.01_windows_32-64.exe`. The dialog box is displayed as shown in Figure 4-110. Click **Update** to proceed.

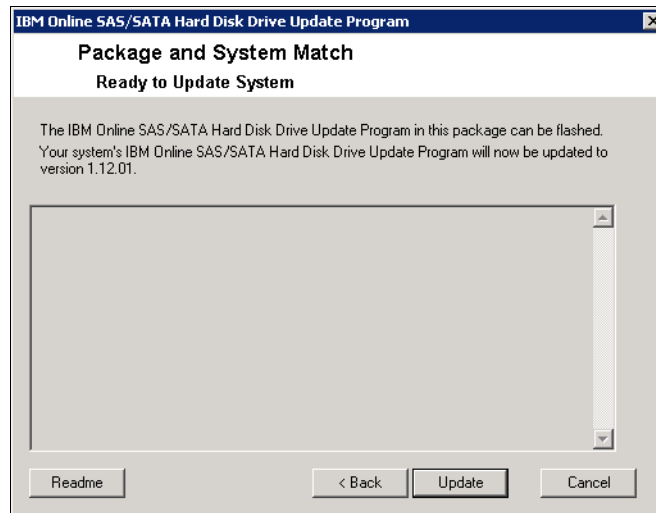


Figure 4-110 Windows firmware update application 1.12.01

4. A summary window, which is shown in Figure 4-111, lists the locally connected hard disk drives and whether the firmware update was applied. In the example, two drives were discovered, but only one firmware was updated.

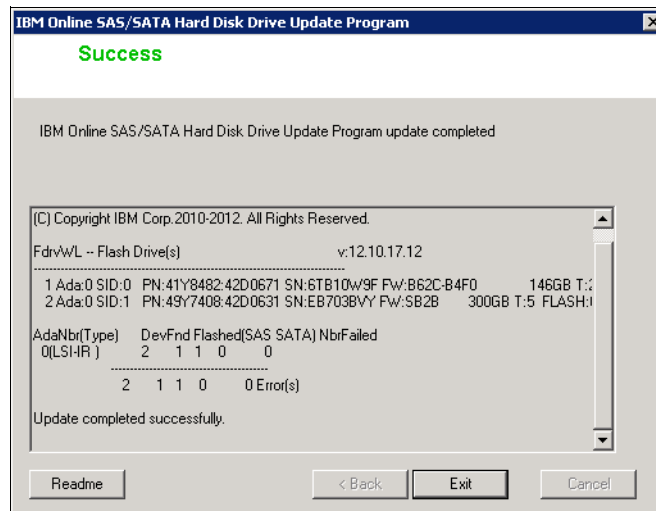


Figure 4-111 Firmware update summary window

5. You must reboot the system for the firmware to be applied. After the server is rebooted, verify the new firmware level by looking at the drive properties in Device Manager again as shown in Figure 4-112.

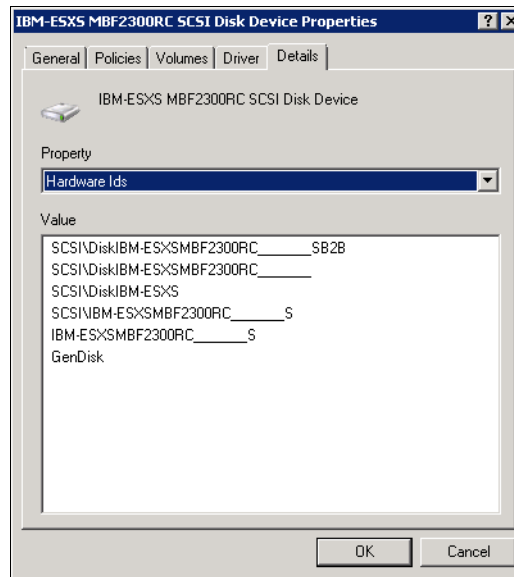


Figure 4-112 Successful firmware update SB2B applied to hard disk drive

4.12.2 HDD firmware updates using SAS Connectivity Module

Hard disk drives connected to a Blade Server through the SAS Connectivity Module can have their firmware updates applied in the same manner as internally attached drive in a blade. SAS Connectivity module allocates DSM hard disk drives using physical port allocations.

For more information, see 4.12.1, “Firmware update for internal Blade HDD” on page 307.

4.12.3 HDD firmware updates using SAS RAID Controller Module

Rather than allocating physical hard disk drives in the DSM units to Blade Servers, the SAS RAID Controller Module assigns volumes. A volume can span several hard disk drives and can even span across the two DSM units in a BladeCenter S chassis.

Hard disk drives attached to a SAS RAID Controller Module have their firmware updates applied when the SAS RAID Controller Module has its own firmware updated. This process also updates the BBUs, and the DSMs as well.

For more information about performing the update, see 4.11.2, “SAS RAID Controller Module firmware” on page 294.

Non-Concurrent mode required: To update hard disk drive firmware, the SAS RAID Controller Module firmware must be installed in Non-Concurrent Code Load (NCCL). See Example 4-14 on page 296 for an example of this command.

The drive firmware is *not* updated if Concurrent Code Load is used to upgrade. This can result in a 4301 maskable alert being reported for any drive with firmware different from the drive firmware in this update package.

4.13 IBM System Storage multipath driver

The IBM System Storage Multipath Subsystem Device Driver (SDD) supports a storage-redundant configuration environment for a host system that is attached to storage devices. It provides enhanced data availability, dynamic input/output (I/O) load balancing across multiple paths, and automatic path-failover protection. The IBM BladeCenter S uses this application within the SAS RAID Controller Module.

The IBM System Storage Multipath Subsystem Device Driver Path Control Module (SDDPCM) provides AIX Multipath I/O (MPIO) support. It is a loadable module. During the configuration of supported storage devices, SDDPCM is loaded and becomes part of the AIX MPIO Fibre Channel protocol device driver. The AIX MPIO-capable device driver with the SDDPCM module provides the same functions that SDD provides.

The IBM System Storage Multipath Subsystem Device Driver Device Specific Module (SDDDSM) provides multipath I/O support for Windows platforms. This support is based on the MPIO technology that is provided by Microsoft and Linux supported operating systems.

4.13.1 IBM Subsystem Device Driver Device Specific Module

The SDDDSM is the IBM multipath IO solution that is based on Microsoft MPIO technology. It is a device-specific module designed to support IBM storage devices. Together with MPIO, it supports the multipath configuration

environments in the IBM TotalStorage Enterprise Storage Server®, the IBM System Storage SAN Volume Controller, IBM TotalStorage DS6000™ and DS8000®, and IBM BladeCenter S SAS RAID Controller Module (RSSM). It resides in a host system with the native disk device driver, and provides the following functions

- ▶ Enhanced data availability
- ▶ Dynamic I/O load-balancing across multiple paths
- ▶ Automatic path failover protection
- ▶ Concurrent download of Licensed Internal Code
- ▶ Path-selection policies for the host system

Below is the link to the support matrix for the IBM Subsystem Device Driver, Subsystem Device Driver Path Control Module, and Subsystem Device Driver Device Specific Module. This section is concerned with the IBM BladeCenter S SAS RAID Controller Module RSSM in a Windows or Linux environment.

The latest drivers can be linked from:

<http://ibm.com/support/docview.wss?uid=ssg1S7001350>

4.13.2 IBM Subsystem Device Driver Path Control Module

The SDDPCM installation package is for the IBM AIX operating system.

SDDPCM is a loadable path control module. It is designed to support the multipath configuration environment on the IBM TotalStorage Enterprise Storage Server, the IBM System Storage SAN Volume Controller, the IBM Storwize® V7000, the IBM TotalStorage DS family, and IBM BladeCenter S SAS Raid Controller Module (RSSM).

When the supported devices are configured as MPIO-capable devices, SDDPCM is loaded and becomes part of the AIX MPIO FCP (Fibre Channel Protocol)/FCoE (Fibre Channel over Ethernet) device driver or SAS device driver. The AIX MPIO device driver or SAS device driver with the SDDPCM module enhances the data availability and I/O load balancing. SDDPCM manages the paths to provide these benefits:

- ▶ High availability and load balancing of storage I/O
- ▶ Automatic path-failover protection
- ▶ Concurrent download of Licensed Internal Code
- ▶ Prevention of a single-point failure caused by host bus adapter, Fibre Channel cable, Ethernet cable, or host-interface adapter on supported storage

Below is the link to the support matrix for the IBM Subsystem Device Driver, Subsystem Device Driver Path Control Module and Subsystem Device Driver Device Specific Module. This section is concerned specifically with the Subsystem Device Driver Path Control Module (SDDPCM), for the P series environment.

The latest drivers can be linked from:

<http://ibm.com/support/docview.wss?uid=ssg1S7001350>



AMM user interface guide

IBM BladeCenter advanced management module (AMM) includes both web and command-line interfaces that you can use to proactively manage the system and diagnose any problems. This chapter describes common tasks that are performed through the web interface, and the associated command, syntax, and output from the command line.

For more information about the CLI commands, see the Information Center at:

http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bc_bc_cli_command_syntax.html

This chapter covers the following topics:

- ▶ 5.1, “Introduction” on page 318
- ▶ 5.2, “Command-line interface” on page 318
- ▶ 5.3, “Monitors” on page 325
- ▶ 5.4, “Blade tasks” on page 348
- ▶ 5.5, “I/O module tasks” on page 374
- ▶ 5.6, “Storage tasks” on page 380
- ▶ 5.7, “Management module control” on page 382
- ▶ 5.8, “Service tools” on page 426

5.1 Introduction

The advanced management module (AMM) is the center point for the BladeCenter's infrastructure intelligence. The AMM is the primary means of management for the chassis, and controls all aspects of power, connectivity, and communication. It uses a web and command-line user interface to run all routine hardware-based management tasks for blades, expansion modules, and configuration of storage modules.

The AMM also acts as a proxy for expansion modules, allowing access through direct (that is, IP address) or indirect (that is, internal chassis) methods for specific module management.

Unlike the other BladeCenter chassis, the BladeCenter S allows a maximum of only one AMM to be installed for chassis management.

This section describes the features of the AMM that allow you to successfully manage and diagnose problems on the BladeCenter S.

Each of the following menu items that are displayed on the left side of the interface are addressed:

- ▶ 5.3, "Monitors" on page 325
- ▶ 5.4, "Blade tasks" on page 348
- ▶ 5.5, "I/O module tasks" on page 374
- ▶ 5.6, "Storage tasks" on page 380
- ▶ 5.7, "Management module control" on page 382
- ▶ 5.8, "Service tools" on page 426

For each menu item, corresponding command to use while logged in to the command-line interface is described. The command and all of the available options are addressed, a specific example of the command usage and expected output is provided.

5.2 Command-line interface

You can use the command-line interface (CLI) to target commands to the management module or to other devices in the BladeCenter chassis. The command-line prompt indicates the persistent command environment. This is the environment in which commands are entered unless they are otherwise redirected. When a command-line interface session is started, the persistent command environment is `system`. This indicates that commands are being directed to the BladeCenter chassis.

5.2.1 Connecting to the CLI

Before accessing the command-line interface, the AMM must have a valid IP address. For more information about connecting the AMM to your network, see 3.1.1, “Setting up the advanced management module” on page 100. After the AMM is in the network, you can use Telnet to connect directly to the AMM CLI by using the default USERID PASSWORD login (note the zero, not an O) Figure 5-1 shows the initial login prompt.

```
telnet 9.42.171.1
Trying 9.42.171.1...
Connected to 9.42.171.1.
Escape character is '^]'.

username: USERID
password:

Hostname:                bcamm6
Static IP address:       9.42.171.1
Burned-in MAC address:  00:14:5E:E1:60:50
DHCP:                    Enabled - Try DHCP. If fails use static IP.
Last login: Thursday March 7 2013 10:05 from 9.42.171.252 (Web)

system>
```

Figure 5-1 Accessing the AMM command line

The **Hostname** and **Burned-in MAC address** entries are unique to your environment. **DHCP** is Enabled by default and the **Last login** entry reports the date, time, IP address, and type of connection (web or CLI) from the last login.

5.2.2 Command help

At any time, you can type “?” or **help** from the command line for a list of commands and overall syntax help. **<command> -h** displays the usage and syntax for that particular command as shown in Figure 5-2.

```
system> help
      ? -- Display commands

Type "<command> -h" for individual command syntax help.
  [ ] is used for indexing (by bay number)
  < > denotes a variable
  { } denotes optional arguments
  | denotes choice
```

Figure 5-2 Command syntax and help

5.2.3 Targeting

There are two ways to indicate the target of your commands:

- ▶ Set the target by using the **env** (environment) command. This command sets the target for the remainder of the session. The target that you choose is indicated as part of the command-line prompt, for example, **system>**.
- ▶ Indicate the target by using the **-T** option to specify the target for the one command only. The syntax is:
<command> -T {target} [X]
where:
 - **<command>** is the command
 - **-T** instructs the AMM to run the command against a specific target
 - **{target} [X]** is a chassis component. See Table 5-1 for a list of valid targets.

Table 5-1 Targets for env command or -T parameter

Component	Target path
BladeCenter unit	system
Management module	system:mm[x]
Blade server	system:blade[x]
Blade server integrated system management processor (IMMv2, IMM, BMC)	system:blade[x]:sp

Component	Target path
Blade server I/O-expansion card	system:blade[x]:exp[y]
Blade server management card	system:blade[x]:mgmtcrd
Blade server microprocessor	system:blade[x]:cpu[y]
Blade server storage expansion unit	system:blade[x]:be[y]
Blade server high-speed expansion card	system:blade[x]:hsec[y]
Blade server memory	system:blade[x]:memory[y]
Blade server mezzanine for double-width form factor	system:blade[x]:sb
Blade server concurrent KVM feature card	system:blade[x]:ckvm
I/O (switch) module	system:switch[x]
Power module	system:power[x]
Blower	system:blower[x]
Media tray	system:mt[x]
Media tray battery backup unit	system:mt[x]:bbu[y]
Storage module (BladeCenter S unit only)	system:storage[x]
Storage module disk drive (BladeCenter S unit only)	system:storage[x]:disk[y]

You can specify target environments by using the full path name or by using a partial path name that is based on the persistent command environment. Full path names always begin with `system`. The levels in a path name are divided by using a colon (:).

The following are examples of targeting:

- ▶ Use the **-T system:mm[1]** option to redirect a command to the management module in bay 1. If your current environment is `system`, you can use the **-T mm[1]** option.
- ▶ Use the **-T system:switch[1]** option to redirect a command to the I/O (switch) module in I/O (switch) module bay 1. If your current environment is `system`, you can use the **-T switch[1]** option.
- ▶ Use the **-T sp** option to redirect a command to the integrated service processor in the blade server in blade server bay 3, when the persistent command environment is set to the blade server in blade server bay 3.

Tip: Only bays with modules installed allow targeting. For example, if you have only one switch module installed in Bay 3, switch[4] does not return information.

5.2.4 Complete CLI example: Configuring the AMM

By using a combination of commands and targets, you can configure the AMM for your environment, combining the CLI and your specific chassis information into a powerful tool for deploying the BladeCenter S chassis.

Table 5-2 lists a set of commands you can use to configure a BladeCenter S chassis:

- ▶ On the left are the commands plus the expected response to the command.
- ▶ On the right is a brief explanation of the commands.

All commands inside “{ }” are installation-specific parameters. For example, enter {AMMIP} as the IP address of your AMM.

Table 5-2 Configuring the chassis using the command line

Command and response	Purpose
system> ifconfig -eth0 -i {AMMIP} -g {AMMGateway} -s {NETMASK} -n {AMMHOSTNAME} -c static -dn {DOMAIN} -ipv6 disabled -T mm[1] These configuration changes will become active after the next reset of the MM.	Configures the AMM IP address, gateway, netmask, host name, and domain; and disables DHCP and IPv6.
system> ifconfig -i {SASMODULE1IP} -g {MODULEGATEWAY} -s {NETMASK} -ipv6 disabled -T switch[3] OK system> ifconfig -i {SASMODULE2IP} -g {MODULEGATEWAY} -s {NETMASK} -ipv6 disabled -T switch[4] OK	Configures the IP address, gateway, and netmask; and disables IPv6 for both SAS connectivity modules.
system> clock -d {DATE} -t {TIME} -g {TIMEZONE} -dst uc -T mm[1] OK	Sets the date, time, time zone, and daylight saving time to the US configuration.
system> ports -ftpe on -tftpe on -telnet off -sshe on -snmpte on -T mm[1] OK	Turns on FTP, TFTP, SSH, and SNMP while disabling Telnet.
system> accseccfg -ct 300 -T mm[1] OK	Sets the login inactivity timeout to five minutes.

Command and response	Purpose
<pre>system> ntp -en enabled -i {TIMESERVER} -f 1440 -T mm[1] dns -i1 {PRIMARYDNS} -i2 {SECONDDNS} -on -T mm[1] OK</pre>	Enables NTP, points it to the time server entered, and sets it to update once a day.
<pre>system> accseccfg -am localldap -T mm[1] OK</pre>	Enables DNS, and configures primary and secondary DNS servers.
<pre>system> ldapcfg -v v2 -server preconf -i1 {AMMIP} -t {AMMHOSTNAME} -T mm[1] OK</pre>	Enables local LDAP authentication, and preconfigures the AMM IP address and host name.
<pre>system> monalerts -ca enabled -cb enabled -ccd enabled -ccsm enabled -ciom enabled -cpm enabled -cstg enabled -T mm[1] OK</pre>	Enables all critical alerts.
<pre>system> smtp -s {YOURMAILSERVER} -T mm[1] OK</pre>	Enables SMTP and sets the mail server.
<pre>system> sshcfg -cstatus enabled -T mm[1] OK</pre>	Enables command-line access through SSH.
<pre>system> snmp -a -on -t -on -cli2 -cl {COMMUNITYNAME} -cli3 -cli1 {SNMPSERVER} -ca1 trap -cn {CONTACTNAME} -l {CONTACT#} -T mm[1] OK</pre>	Resets the alert user and then configures a critical SNMP alert recipient to the host name or IP indicated.
<pre>system> alertentries -l -del -T mm[1] OK system> alertentries -l -status on -n Monitor_alert -f critical -t snmp -i {SNMPSERVER} -T mm[1] OK system> pmpolicy -pm acredov OK</pre>	Sets the power management policy to “AC Power Source Redundancy with Blade Throttling Allowed”.
<pre>system> users -l -n administrator -p password -a super -ms 5 -T mm[1] OK</pre>	Changes the default elevated account “USERID” to “administrator” with the password “password,” and allows five simultaneous sessions of that user.
<pre>system> users -2 -clear -T mm[1] OK system> users -2 -n Operator -p PASSWORD -a rbs:ba co clm bo brp ba so:c1 b1 b2 -ms 10 -T mm[1] OK</pre>	Configures a second account with the ID “Operator” and password “PASSWORD”. This is a role-based account with chassis operator, switch operator, blade administration, and blade operator privileges to the chassis, blade 1, and blade 2.

Command and response	Purpose
system> trespass -twe on -tw "This system is for authorized personnel only. Use by unauthorized individuals is a violation of federal and or state law." -T mm[1] OK	Sets a trespass message.
system> config -name {AMMHOSTNAME} -T mm[1] OK	Changes the displayed name of the AMM to the AMM host name.
system> config -name {BLADE1HOSTNAME} -T blade[1] OK system> config -name {BLADE2HOSTNAME} -T blade[2] OK	Changes the displayed name of blade 1 and blade 2 to match their host names.
system> reset -T switch[3] OK system> reset -T switch[4] OK system> reset -T mm[1] OK	Resets switch 3, 4, and the AMM so the settings become active.
system> exit Connection closed by foreign host.	Ends the CLI session.

After the AMM reboots, pings on the IP address you specified, and completes the discovery of all modules, you can update firmware or configure your storage.

For more information about chassis configuration management, see Chapter 5, “AMM user interface guide” on page 317.

For an entire list of all commands, their functions, and examples, see the “BladeCenter Advanced Management Module Command Line Interface Reference Guide” at:

http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bc_pdf.pdf

The remaining sections describe all tasks that can be performed with the AMM, and include information about both the web interface and the command-line interface.

5.3 Monitors

This section describes the monitor actions as shown in Figure 5-3. The tasks are covered in the following sections:

- ▶ 5.3.1, “System status” on page 326
- ▶ 5.3.2, “Event log” on page 327
- ▶ 5.3.3, “LEDs” on page 329
- ▶ 5.3.4, “Power management” on page 331
- ▶ 5.3.5, “Hardware vital product data” on page 340
- ▶ 5.3.6, “Firmware vital product data” on page 344
- ▶ 5.3.7, “Remote Chassis” on page 346

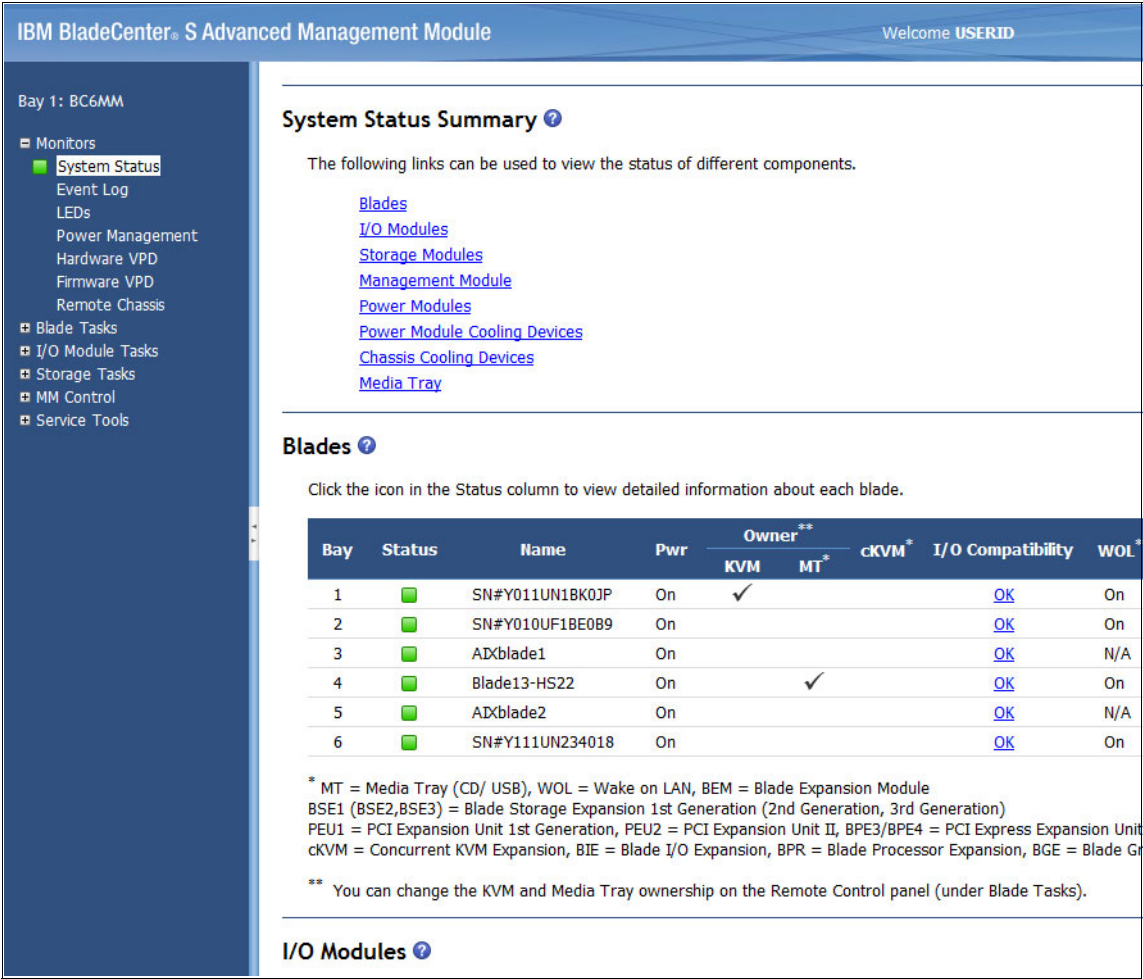


Figure 5-3 The AMM browser interface showing the chassis status

5.3.1 System status

The status window provides an overview of your system health. It is your first point of reference if you experience problems with the chassis or components. The health status of all components that are listed in Figure 5-3 on page 325 can be viewed from here.

To view the health of the chassis from the command-line interface, use the following command:

```
health {-l {1|2|a|all}} | -f {-t}}
```

where:

-l 1	Current target status
-l 2	Current target and next level status
-l a	Tree status
-l all	Tree status
-f	Current target detail
-f -t	Current target detail with time stamp

Example output of the health command is shown in Figure 5-4.

```
system> health -l all
system: Non-Critical
      mm[1]      :      OK
      blade[1]   :      OK
      blade[2]   :      OK
      blade[3]   :      OK
      blade[4]   :      Non-Critical
      blade[5]   :      OK
      blade[6]   :      OK
      power[1]   :      OK
      power[2]   :      OK
      power[3]   :      OK
      power[4]   :      OK
      blower[2]  :      OK
      blower[4]  :      OK
      switch[1]  :      OK
      switch[3]  :      Non-Critical
      switch[4]  :      Non-Critical
```

Figure 5-4 Detailed system health

Non-critical alerts are information warnings that do not impact the overall health of the chassis. Critical alerts point to hardware issues that might impact your

environment. For example, to examine the non-critical alert for blade[4] in Figure 5-4 on page 326, use the command shown in Figure 5-5.

```
system> health -f -T blade[4]
system:blade[4] : Non-Critical
                  (Blade13-HS22) Blade incompatible with I/O module configuration
                  (Blade13-HS22) Blade incompatible with I/O module configuration
```

Figure 5-5 Detailed health of Blade 4

This chassis shows a non-critical alert because the I/O modules installed in bays 3 and 4 are incompatible with the card that is installed in blade 4.

5.3.2 Event log

The event log, which is stored on the AMM, provides the following useful information:

- ▶ Information and error logging for the blades and components that are installed in the chassis
- ▶ Auditing of user login attempts to the AMM

You can sort the event log by date, severity, source, date and time, the event ID, or the text of the event. You can also apply filters by severity, date, source, or call home status so that you see only the events important to you. Checking the event log in conjunction with the system window assists you when problems occur.

The event log is a fixed capacity. When it is 75% full, the Information LED on the chassis glows as shown in Figure 5-8 on page 330. The Information LED can be switched off by clicking **Monitors** → **LEDs** → **Media Tray and Rear Panel LEDs** and clicking **Off** next to the Information LED. You can also switch off the Information LED by clearing the event log.

New entries overwrite the oldest entries until you clear the log. You can save the event log before you clear it by selecting **Save Log as Text File**. If you do not want the management module to monitor the state of the event log, click to clear

Monitor log state events at the top of the Event Log window. Figure 5-6 shows a sample of the event log.

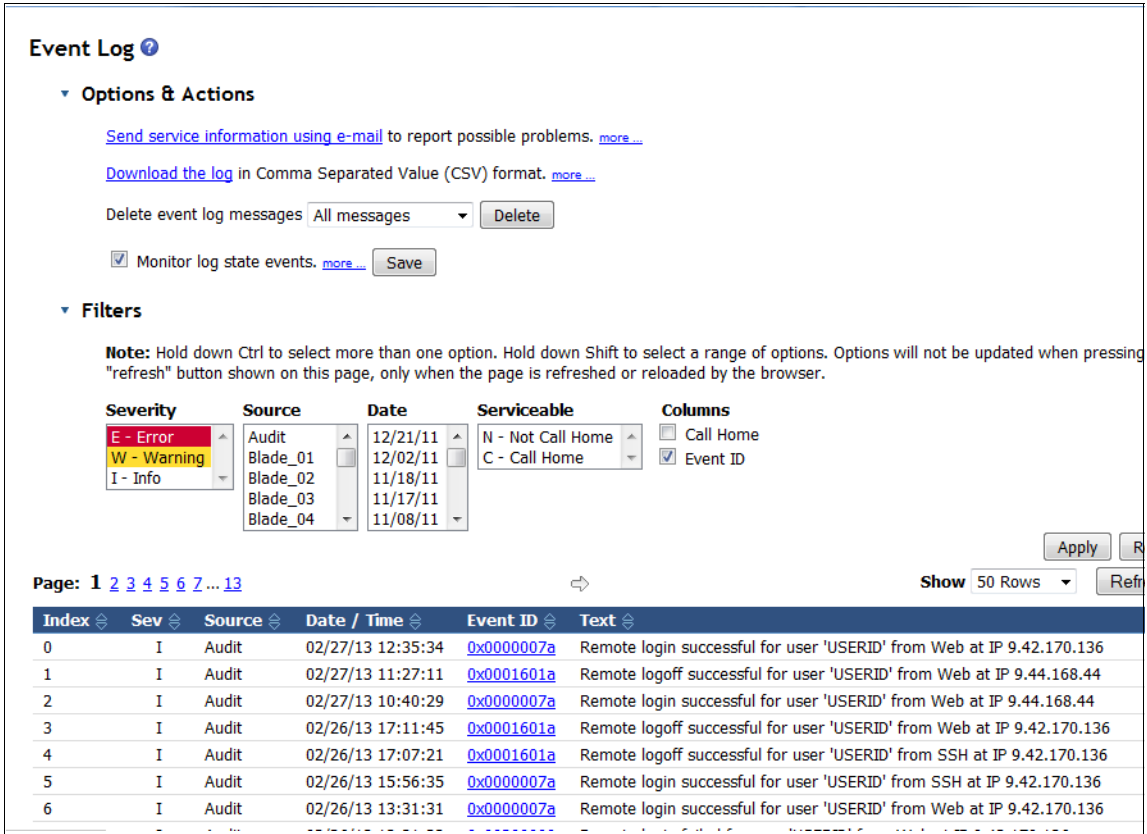


Figure 5-6 Advanced management module Event Log window

To view the event log from the command-line interface, use the following command and syntax:

```
displaylog
{-filters} | {{{{-f}} | {{-a}} | {{-e|-c|-date|-sev|-src|-ch}}} | {{-i|-l|-lse}}
```

where:

- f: Reset the counter and display the five most recent event log entries
- a: Display all the log entries at a specific time
- e: Display log entries with their Event ID
- c: Display log entries with their call home flag

-filters:	Display all possible filters
-date:	Pipe ()-separated list of date filters (mm/dd/yy)
-sev:	Pipe-separated list of severity filters (I, W, E)
-src:	Pipe-separated list of source filters. A range for modules can be specified by using a hyphen '-' (for example, Blade_01-14)
-ch:	Call home flag filters (N, C)
-l:	File name to save the event log to TFTP server
-i:	IP address of TFTP server that is used to save the event log
-lse:	Monitor log state events (enabled, disabled)

Restrictions: The command has these restrictions:

- -i and -l, or -lse must be used exclusive of other options.
- ! (exclamation mark) can be used with any of the filter options to specify an inverse filter (for example -sev !E|I displays all warning entries).

An example of the **displaylog** command is shown in Figure 5-7.

```
system> displaylog -T mm[1]
1 I Audit 02/28/13 09:02:21 Remote login for user 'USERID' from Telnet at IP 9.42.170.136
2 I Audit 02/28/13 08:19:27 Remote login for user 'USERID' from Web at IP 9.42.170.136
3 I Audit 02/27/13 18:20:30 All audit messages deleted from event log by 'USERID'.
4 I Audit 02/27/13 18:20:30 All system messages deleted from event log by 'USERID'.
```

Figure 5-7 displaylog output from the command line

5.3.3 LEDs

You can use the LEDs window to view the LED status of a number of components within the chassis. The following actions are also available from this window:

- You can activate the Location LED for the BladeCenter S or any blades installed in the chassis to allow for easy identification. To activate, click the Location's **On** or **Blink** button. To deactivate the Location LED, click **Off**.

- You can switch off the Information LED for the BladeCenter S or the individual blades installed in the chassis from this window by clicking the Information **Off** button as shown in Figure 5-8.

Media Tray and Rear Panel LEDs ?

☐ Text mode

LED	Status	Action
System error	Off	
Information	Off	<button>Off</button>
Temperature	Off	
Location	Off	<button>On</button> <button>Off</button> <button>Blink</button>

Blade LEDs ?

☐ Text mode

Click the hyperlinks in the Name column to view detailed LED state information about a specific blade.

Bay	Name	Pwr*	Error	Information	KVM	MT	Location
1	SN#Y011UN1BK0JP	Off	Off	Off <button>Off</button>	Off	Off	Off <button>On</button> <button>Off</button> <button>Blink</button>
2	SN#Y010UF1BE0B9		Off	Off <button>Off</button>			Off <button>On</button> <button>Off</button> <button>Blink</button>
3	ADXblade1		Off	Off <button>Off</button>	n/a	Off	Off <button>On</button> <button>Off</button> <button>Blink</button>
4	Blade13-HS22		Off	Off <button>Off</button>	Off	Off	Off <button>On</button> <button>Off</button> <button>Blink</button>
5	ADXblade2		Off	Off <button>Off</button>	n/a	Off	Off <button>On</button> <button>Off</button> <button>Blink</button>
6	SN#Y111UN234018		Off	Off <button>Off</button>	Off	Off	Off <button>On</button> <button>Off</button> <button>Blink</button>

* If a blade is powered off, its physical LEDs are not lit. This table represents the status of all LEDs, even for powered-off blades.

Figure 5-8 LEDs interface

The `led` command provides the same functions from the command-line interface:

```
led {-l|-info|-loc|-d}
```

where:

- l Get status of all LEDs on target blade and its subcomponents.
- info Turn off Information LED (off).
- loc Turn off/on/blink location LED (off/on/blink).
- d Turns on the Identification LED of the system for the specified number of seconds. The `-d` option must be used with `-loc on`, and is only valid for the system target.

Examples of the led command are shown in Figure 5-9.

```
system> led
-loc: off
-info on
System Error: off
Temperature: off
system> led -info off
OK
system> led
-loc: off
-info off
System Error: off
Temperature: off
```

Figure 5-9 Turning off the Information LED

5.3.4 Power management

This window, which is shown in Figure 5-10 on page 332, allows you to view power consumption, and control how the BladeCenter S distributes its power when a power module fails. Choose a power management policy that suites your environment.

There are five sections on this window:

- ▶ BladeCenter Power Domain Summary, see Figure 5-10 on page 332
- ▶ BladeCenter Power Domain Planning, see Figure 5-10 on page 332
- ▶ BladeCenter Chassis Power Summary
- ▶ BladeCenter Chassis Configuration Setting
- ▶ BladeCenter Chassis Power Consumption, see Figure 5-11 on page 334

BladeCenter power domain summary

This section displays the following information as shown in Figure 5-10 on page 332:

- ▶ Status: The health status of your power domain. Unlike its other family members, the BladeCenter S has only one power domain.
- ▶ Power Modules: The total number of power modules installed.
- ▶ Power Management Policy: The power management policy that the chassis is configured to use, which determines how the chassis manages its power when one or more power modules fail.

- ▶ **Maximum Power Limit:** The maximum power available to the chassis, which is determined by the number of power modules installed and the current power management policy selected.
- ▶ **Power in Use:** The current physical power consumption of all components within the Power Domain.
- ▶ **Power Service:** The type of power that is supplied to the chassis, which can be 110 VAC or 220 VAC.

BladeCenter Power Domain Summary ?	
Power Domain	
Status	<div> <div></div> Power domain status is good. </div>
Power Modules	Bay 1: 950W Bay 2: 950W Bay 3: 950W Bay 4: 950W
Power Management Policy	AC Power Source Redundancy with Blade Throttling Allowed Very similar to the AC Power Source Redundancy. This policy allows you to draw more total power than the chassis power limit. Blades may be allowed to throttle down if one AC power source fails.
Maximum Power Limit [†]	2250W
Power in Use ^{††}	704W
Power Service	110 VAC

BladeCenter Power Domain Planning ?	
Power Domain	
Maximum Power Limit [†]	2250W
- Allocated Power (Max) ^{†††}	1289W
= Remaining Power	961W

BladeCenter Chassis Power Summary ?	
Total DC Power Available	2250W
Total AC Power In Use ^{††}	786W
Total Thermal Output	2,681.8 BTU/Hour

Figure 5-10 Power Domain Summary window

There are two links in the Power Domain Summary that give you more information:

- ▶ Click **Power Domain** to see details about power in use, minimums, and maximums. For more information about the power domain in “BladeCenter power domain details” on page 335.
- ▶ Click **AC Power Source Redundancy with Blade Throttling Allowed** (or whatever the name of the current power management policy is) to see

information about all power management policies and to select a different power management policy. For more information, see “Power management policy” on page 336.

BladeCenter power domain planning

This section has the following information as shown in Figure 5-10 on page 332:

- ▶ **Maximum Power Limit:** The maximum power available to the chassis. This amount is determined by the number of power modules that are installed, the current power management policy selected, and whether the power source is 110 VAC or 220 VAC.
- ▶ **Allocated Power (Max):** Displays the total amount of power that is reserved for use by the components that are installed in the chassis. This value can also include power required for components that are not currently installed, such as I/O modules. The AMM pre-allocates power for these components because it is typically assumed that they are installed for normal BladeCenter operation. Blades that are installed in the chassis but are switched off also have power pre-allocated to them.
- ▶ **Remaining Power:** This is the amount of available power after the Allocated Power (Max) value has been subtracted from the Maximum Power Limit value. The AMM uses this value to determine whether any newly installed components or blades can be switched on.

BladeCenter chassis configuration setting

This section determines how the AMM responds to an over-temperature condition on a blade:

- ▶ **Acoustic Mode Disabled:** This is a global policy that allows the user to decide how the system reacts in a thermal event on a blade. The two options are to increase the Chassis Cooling Device speeds (if acoustic mode is disabled), or to attempt to throttle the blade to stay within acoustic noise limits (if acoustic mode is enabled). Regardless of the acoustic mode policy setting, if a blade reaches its thermal warning limit, the Chassis Cooling Devices change to full speed.
- ▶ **Data Sampling Interval:** This field allows you to indicate whether you want the system to collect and provide historical power consumption data for the chassis, power domains, and modules. This process also includes the collection and reporting of the ambient and Chassis Cooling Device temperatures. This function is enabled by default, and is automatically set to collect this information every 10 minutes. If you do not want this function, select **No Trending** from the menu.

BladeCenter chassis power consumption

This section of the window, Figure 5-11, is a graph that displays a historical trend of the power consumption for the entire chassis. By default, this information is shown for the past hour the first time that the window is displayed. You can view trending information for the past six hours, 12 hours, or 24 hours by making the selection from the **Trend Period** menu.

Active Energy Manager: IBM Systems Director Active Energy Manager can be used to monitor power consumption beyond 24 hours. For more information, see *Implementing IBM Systems Director Active Energy Manager 4.1.1*, SG24-7780, available at:

<http://www.redbooks.ibm.com/abstracts/sg247780.html?Open>

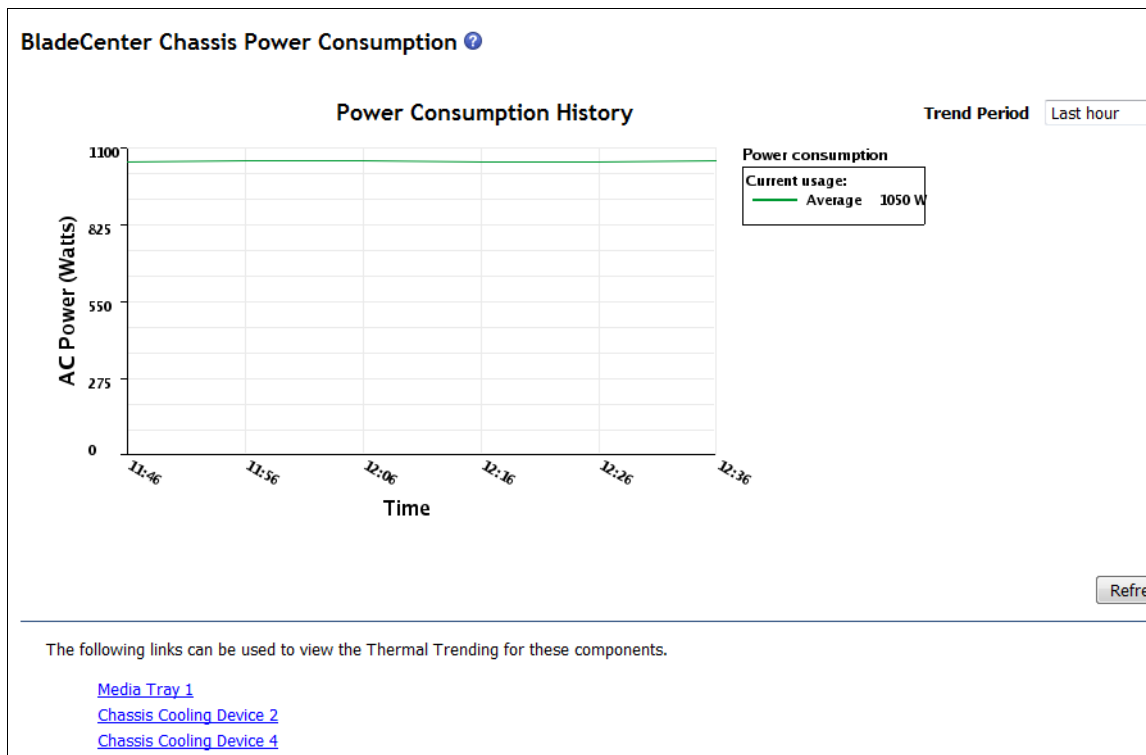



Figure 5-11 BladeCenter Chassis Power Consumption graph

Accuracy directly after a reboot: After a reboot of the AMM or a complete power loss to the chassis, the first data sample that is captured will not be as accurate as subsequent samples.

BladeCenter power domain details

If you want to view a breakdown summary of the power used by the individual components and blades, open the Power Domain window by clicking **Power Domain** on the Power Domain Summary window in Figure 5-10 on page 332. Doing so opens a window similar to Figure 5-12.

BladeCenter Power Domain Details 

Bay(s)	Status	Module	State	Power In Use	Allocated Power		CPU Duty Cycles
					Maximum	Minimum	
Chassis Components							
		Midplane	On	10W	10W	10W	n/a
1		Media devices container	On	10W	10W	10W	n/a
Power Module Cooling Devices							
1		Power supply	On	10W	10W	10W	n/a
2		Power supply	On	10W	10W	10W	n/a
3		Power supply	On	10W	10W	10W	n/a
4		Power supply	On	10W	10W	10W	n/a
Chassis Cooling Devices							
2		Cooling device	On	58W	68W	68W	n/a
4		Cooling device	On	57W	68W	68W	n/a
Storage							
1		Storage devices container	On	100W	100W	100W	n/a
2		Storage devices container	On	100W	100W	100W	n/a
Management Modules							
1		BC6MM	On	25W	25W	25W	n/a
I/O Modules							
1		Ethernet SM	On	45W	45W	45W	n/a
3		SAS Conn Mod	On	45W	45W	45W	n/a
4		SAS Conn Mod	On	45W	45W	45W	n/a
Blades							
[1]		SN#Y011UN1BK0JP	On	107W	294W	214W	n/a ^{††}
[2]		SN#Y010UF1BE0B9	On	108W	314W	192W	n/a ^{††}
[3]		ADXblade1	On	134W	350W	245W	n/a ^{††}
[4]		Blade13-HS22	On	128W	301W	221W	n/a ^{††}
[5]		ADXblade2	On	142W	350W	245W	n/a ^{††}
[6]		SN#Y111UN234018	On	55W	137W	82W	n/a ^{††}
<div><div>[†] This blade may throttle if redundancy is lost in this power domain.</div><div>^{††} Click on the module name to view CPU speeds.</div><div>[*] Cannot communicate with the blade. The power values for this blade are assumed.</div></div>							

Figure 5-12 Sample of the Power Domain Details interface

Power management policy

Power management policies determine how the BladeCenter S manages its use of power when power modules fail.

To select a power management policy, click the link on the Power Domain Summary window shown in Figure 5-10 on page 332. In this example, the currently active policy is **AC Power Source Redundancy with Blade Throttling Allowed**. The power management policies window opens, which is shown in Figure 5-13.

BladeCenter Power Management Policies ?

Links [Power Summary](#)

This table lists the power management policies ordered from most conservative to least conservative.

Select	Option Name	Power Supply Failure Limit [†]	Maximum Power Limit (Watts)	U
<input type="radio"/>	AC Power Source Redundancy Intended for dual AC power sources into the chassis. Total allowed power draw is limited to the capacity of two Power Modules. This is the most conservative approach and is recommended when all four Power Modules are installed. When the chassis is correctly wired with dual AC power sources, one AC power source can fail without affecting blade operation. Note that some blades may not be allowed to power on if doing so would exceed the policy power limit. More...	2	2900	
<input type="radio"/>	AC Power Source Redundancy with Blade Throttling Allowed Very similar to the AC Power Source Redundancy. This policy allows you to draw more total power; however, capable blades may be allowed to throttle down if one AC power source fails. More...	2	3400	
<input type="radio"/>	Power Module Redundancy Intended for a single AC power source into the chassis where each Power Module is on its own dedicated circuit. Total allowed power draw is limited to one less than the number of Power Modules when more than one Power Module is present. One Power Module can fail without affecting blade operation. Multiple Power Module failures can cause the chassis to power off. Note that some blades may not be allowed to power on if doing so would exceed the policy power limit. More...	1	3562	
<input type="radio"/>	Power Module Redundancy with Blade Throttling Allowed Very similar to Power Module Redundancy. This policy allows you to draw more total power; however, capable blades may be allowed to throttle down if one Power Module fails. More...	1	3562	
<input checked="" type="radio"/>	Basic Power Management Total allowed power is higher than other policies and is limited only by the total power capacity of all the Power Modules up to the maximum of chassis power rating. This is the least conservative approach, since it does not provide any protection for AC power source or Power Module failure. If any single power supply fails, blade and/or chassis operation may be affected. More...	0	3562	

Figure 5-13 Power management policy options

Each power policy displays the following information:

- ▶ Maximum number of power modules that might fail for that policy.
- ▶ The maximum power limit for that policy.

- ▶ The estimate power utilization of all components that are installed, which is represented as a percentage of the maximum power limit allowed for that policy.

The BladeCenter S has five predefined power policies as shown in Figure 5-13 on page 336:

- ▶ **AC Power Source Redundancy**

Intended for dual AC power sources into the chassis. Total allowed power draw is limited to the capacity of two Power Modules. This is the most conservative approach and is preferable when all four Power Modules are installed. When the chassis is correctly wired with dual AC power sources, one AC power source can fail without affecting blade operation.

Blades will not power on: Some blades might not be allowed to power on if doing so exceeds the policy power limit.

- ▶ **AC Power Source Redundancy with Blade Throttling Allowed**

This policy is similar to the AC Power Source Redundancy. You can use it to draw more total power. However, capable blades might be throttled down if one AC power source fails.

- ▶ **Power Module Redundancy**

Intended for a single AC power source into the chassis where each Power Module is on its own dedicated circuit. Total allowed power draw is limited to one less than the number of Power Modules when more than one Power Module is present. One Power Module can fail without affecting blade operation. Multiple Power Module failures can cause the chassis to power off.

- ▶ **Power Module Redundancy with Blade Throttling Allowed**

This policy is similar to Power Module Redundancy. You can use it to draw more total power, but capable blades might be throttled down if one Power Module fails.

- ▶ **Basic Power Management**

Total allowed power is higher than other policies, and is limited only by the total power capacity of all the Power Modules up to the maximum of the chassis power rating. This is the least conservative approach. It does not provide any protection during AC power source or Power Module failure. If any single power supply fails, blade and chassis operation can be affected.

After you select the power management policy that you want to apply, click **Save** to commit the change.

If you need more information about power management policies, click the help icon, shown as a question mark (?) next to Power Domain Details in Figure 5-12 on page 335.

To view the power management policy from the command line, use the **pmpolicy** command:

```
pmpolicy {<pd> {-pm}} (acred|acredov|redwoperf|redwperf|nonred)
```

where:

- pd: Power domain
- pm: Power management settings

Running the command with no options returns the current power management policy. Using the **-pm** flag requires one of the options in Table 5-3.

Table 5-3 *pmpolicy* parameters

Option Name:	Description:
acred	AC Power Source Redundancy Intended for dual AC power sources into the chassis. Total allowed power draw is limited to the capacity of two Power Modules. This is the most conservative approach and is preferable when all four Power Modules are installed. When the chassis is correctly wired with dual AC power sources, one AC power source can fail without affecting blade operation.
acredov	AC Power Source Redundancy with Blade Throttling Allowed Similar to the AC Power Source Redundancy policy. This policy allows you to draw more total power, but capable blades might be throttled down if one AC power source fails.
redwoperf	Power Module Redundancy Intended for a single AC power source into the chassis where each Power Module is on its own dedicated circuit. Total allowed power draw is limited to one less than the number of Power Modules when more than one Power Module is present. One Power Module can fail without affecting blade operation. Multiple Power Module failures can cause the chassis to power off. Some blades might not be allowed to power on if doing so exceeds the policy power limit.
redwperf	Power Module Redundancy with Blade Throttling Allowed Similar to Power Module Redundancy policy. This policy allows you to draw more total power, but capable blades might be throttled down if one Power Module fails.

Option Name:	Description:
nonred	Basic Power Management Total allowed power is higher than other policies, and is limited only by the total power capacity of all the Power Modules up to the maximum of chassis power rating. This is the least conservative approach because it does not provide any protection during AC power source or Power Module failure. If any single power supply fails, blade and chassis operation can be affected.

The use of the **pmpolicy** command without parameters is shown in Figure 5-14.

```
system> pmpolicy

Power Domain
-----

Power Management Policy:
  Basic Power Management (nonred)
Description:
  Total allowed power is higher than other policies and is limited only
  by the total power capacity of all the Power Modules up to the
  maximum of chassis power rating. This is the least conservative
  approach, since it does not provide any protection for AC power
  source or Power Module failure. If any single power supply fails,
  blade and/or chassis operation may be affected.
Power Supply Failure Limit:      0
Maximum Power Limit (Watts):    3562
Your Estimated Utilization:      29%

NOTE:
Power Supply Failure Limit: This is the maximum number of power supplies
that can fail while still guaranteeing the operation of the domain in the
selected policy.
Your Estimated Utilization: The estimated utilization is based on the
maximum power limit allowed in this policy and the current aggregated power
in use of all components in the domain.
```

Figure 5-14 Displaying the power management policy

In Figure 5-15, the policy is changed by using the **-pm** flag.

```
system> pmpolicy -pm acredov
OK
system> pmpolicy

Power Domain
-----

Power Management Policy:
  AC Power Source Redundancy with Blade Throttling Allowed
  (acredov)
Description: Very similar to the AC Power Source Redundancy. This
policy allows you to draw more total power; however, capable blades
may be allowed to throttle down if one AC power source fails.
Power Supply Failure Limit:      2
Maximum Power Limit (Watts):    3400
Your Estimated Utilization:      30%

NOTE:
Power Supply Failure Limit: This is the maximum number of power
supplies that can fail while still guaranteeing the operation of the
domain in the selected policy.
Your Estimated Utilization: The estimated utilization is based on
the maximum
```

Figure 5-15 Changing the power management policy

5.3.5 Hardware vital product data

You can use this window to view the vital product data (VPD), which includes serial numbers, part numbers, and other data that you might need about the components and blades installed in the chassis. The AMM populates this information in non-volatile memory during startup, and adds and removes data as components or blades are added or removed.

Figure 5-16 shows all of the components in the AMM inventory.

BladeCenter Hardware Vital Product Data

A summary of hardware inventory for all components is also available on the [BladeCenter Summary](#) page. For individual component details, click on the specific component link in the topology table.

The summary process may take a few moments to complete, depending upon your installed hardware.

Hardware Topology

Activity

?

Help

Collapse all

Expand all

Module Name	Module Description	Presence
Chassis and Chassis Managed Components		
Chassis	BladeCenter-S	Installed
<div> <div></div> <div>[1] Media Module</div> </div>	Media Tray	Installed
<div> <div></div> <div>[1] Battery</div> </div>	Battery Backup Unit	Installed
<div> <div></div> <div>[2] Battery</div> </div>	Battery Backup Unit	Installed
<div> <div></div> <div>[1] Serial Port Module</div> </div>	---	Not Installed
Blades		
<div> <div></div> <div>[1] SN#Y011UN1BK0JP</div> </div>	HS22 (Type 7870)	Installed
<div> <div></div> <div>Processors</div> </div>		
<div> <div></div> <div>[1] Processor</div> </div>	CPU 1	Installed
<div> <div></div> <div>[2] Processor</div> </div>	CPU 2	Installed
<div> <div></div> <div>Memory</div> </div>		
<div> <div></div> <div>[1] Memory</div> </div>	---	Not Installed
<div> <div></div> <div>[2] Memory</div> </div>	DIMM 2	Installed
<div> <div></div> <div>[3] Memory</div> </div>	---	Not Installed
<div> <div></div> <div>[4] Memory</div> </div>	DIMM 4	Installed
<div> <div></div> <div>[5] Memory</div> </div>	---	Not Installed
<div> <div></div> <div>[6] Memory</div> </div>	DIMM 6	Installed
<div> <div></div> <div>[7] Memory</div> </div>	---	Not Installed
<div> <div></div> <div>[8] Memory</div> </div>	DIMM 8	Installed

Figure 5-16 BladeCenter hardware vital product data

Clicking an individual component provides you with more details as shown in Figure 5-17.

Slot 1 - Chassis Information

Property	Value
Description	BladeCenter-S
Machine Type/Model	88861MU
Machine Serial No.	1003E1A
Part Number	44T1407
FRU Number	43W3631
FRU Serial No.	YK109081C0B0
Hardware Revision	4
Manuf. Date	0408
UUID	A5EC 61FE C777 11DC 8DE9 924D 6B61 CA9E
Manufacturer	IBM (FOXC)
Manuf. ID	20301
Product ID	155

[Edit BladeCenter System Vital Product Data](#)

Figure 5-17 Chassis hardware VPD

Figure 5-18 shows the detailed information for Blade 1.

BladeCenter Vital Product Data

Inventory

Ports

Slot 1 - SN#Y011UN1BK0JP Information

Property	Value
Product Name	IBM BladeCenter HS22
Description	HS22 (Type 7870)
Machine Type/Model	7870AC1
Machine Serial No.	06RPN99
Part Number	81Y9486
FRU Number	68Y8186
FRU Serial No.	Y011UN1BK0JP
Hardware Revision	7
Manuf. Date	4811
UUID	45A6 0F2A 1CF9 11E1 99A0 5CF3 FC97 A82C
Manufacturer	IBM (FOXC)
Manuf. ID	20301
Product ID	176

Processor Information

Slot	Description	Machine Type/Model	Machine Serial No.	Part Number	FRU Number	FRU Serial No.	Hardware Revision
1	CPU 1	---	---	---	---	---	---
2	CPU 2	---	---	---	---	---	---

Memory Information

Slot	Description	Machine Type/Model	Machine Serial No.	Part Number	FRU Number	FRU Serial No.	Hardware Revision
2	DIMM 2	---	---	M392B1K70CM0-YF8	---	4425c47c	---
4	DIMM 4	---	---	M392B5170EM1-CH9	---	46161827	---
6	DIMM 6	---	---	M392B5170EM1-CH9	---	4616187b	---
8	DIMM 8	---	---	M392B1K70CM0-YF8	---	4425c427	---
10	DIMM 10	---	---	M392B1K70CM0-YF8	---	4425c3cf	---

Expansion Card Information

Slot	Description	Part Number	FRU Number	FRU Serial No.	Hardware Revision	Manuf. Date	Hardware Revision
1	SAS Conn Card	49Y8009	46C4069	YK11900CC131	4	5010	0C9E D23

Thu, 28 Feb 2013 14:05:36


















Figure 5-18 Blade Hardware VPD

5.3.6 Firmware vital product data

This window allows you to view the firmware levels, build IDs, release dates, and revision numbers for the following components installed into the chassis. Clicking any of the links at the top goes to that section.

- Blade firmware
- I/O module firmware
- Management module firmware
- Power Module Cooling Device firmware
- Chassis Cooling Device firmware
- Storage module firmware

Figure 5-19 shows a sample of the Blade Firmware Vital Product Data window. You can manually reload the firmware vital product data for a blade by clicking **Reload VPD**.

Blade Firmware Vital Product Data						
Bay(s)	Name	Firmware Type	Build ID	Released	Revision	Level 
1	SN#Y011UN18K0JP	FW/BIOS	P9E157A	06/14/2012	1.18	
		Diagnostics	DSYTA1N	06/16/2012	9.21	
		Blade Sys Mgmt Processor	YUOOE3C		1.33	
2	SN#Y010UF18E0B9	FW/BIOS	P9E157A	06/14/2012	1.18	
		Diagnostics	DSYTA1N	06/16/2012	9.21	
		Blade Sys Mgmt Processor	YUOOE3C		1.33	
3	ADXblade1	FW/BIOS	AA710_088	07/29/2010	1030	 ?+
		Blade Sys Mgmt Processor	BOBT001		7.12	 ?+
4	Blade13-HS22	FW/BIOS	P9E146C	04/26/2010	1.08	
		Diagnostics	DSYT60K	02/25/2010	3.01	
		Blade Sys Mgmt Processor	YUOO57H		1.10	
5	ADXblade2	FW/BIOS	AA710_088	07/29/2010	1030	 ?+
		Blade Sys Mgmt Processor	BOBT001		7.12	 ?+
6	SN#Y111UN234018	FW/BIOS	TKE116RUS	06/13/2012	1.10	 ?+
		Diagnostics	DSYTA1N	06/16/2012	9.21	 ?+
		Blade Sys Mgmt Processor	1A0030W		1.50	 ?+

To reread firmware Vital Product Data for a blade, select the blade, and click "Reload VPD".
This process may take a while.


Target All Blades  Reload VPD

Figure 5-19 Blade Firmware VPD window

You can use the **info** command to view the Firmware and Hardware Vital Product Data from the command line. Running the command without options shows the serial number and machine type for the entire chassis as shown in Figure 5-20.

```
system> info
UUID: A5EC 61FE C777 11DC 8DE9 924D 6B61 CA9E
Manufacturer: IBM (FOXC)
Manufacturer ID: 20301
Product ID: 155
Mach type/model: BladeCenter-S/88861MU
Mach serial number: 1003E1A
Manuf date: 0408
Hardware rev: 4
Part no.: 44T1407
FRU no.: 43W3631
FRU serial no.: YK109081C0B0
CLEI: Not Available
AMM slots: 1
Blade slots: 6
I/O Module slots: 4
Power Module slots: 4
Blower slots: 4
Media Tray slots: 1
```

Figure 5-20 The info command

Running the command on a target provides the FRU, part number, serial number, and firmware revision for the target. Figure 5-21 shows the information about the AMM.

```
system> info -T mm[1]
Name: BC6MM
UUID: 489B 768D 1D79 11DD 84F8 0014 5EE1 6050
Manufacturer: IBM (ASUS)
Manufacturer ID: 20301
Product ID: 65
Mach type/model: Advanced Management Module
Mach serial number: Not Available
Manuf date: 1908
Hardware rev: 4
Part no.: 39Y9659
FRU no.: 39Y9661
FRU serial no.: YK16808561S7
CLEI: Not Available
AMM firmware
Build ID:BPET54V
File name:CNETCMUS.PKT
Rel date:03/30/2011
Rev:54
```

Figure 5-21 Detailed Firmware VPD for the AMM

5.3.7 Remote Chassis

This window allows you to perform the following actions:

- ▶ Discover other BladeCenter Chassis on the local network.
- ▶ View the health status of the discovered chassis.
- ▶ Obtain more information about the discovered chassis by selecting the name of the discovered chassis in the Chassis Name column.
- ▶ Gain console access to the discovered systems management interface by selecting the discovered systems IP address in the Console IP column.

Figure 5-22 illustrates a sample of what you can see on the Remote Chassis window.

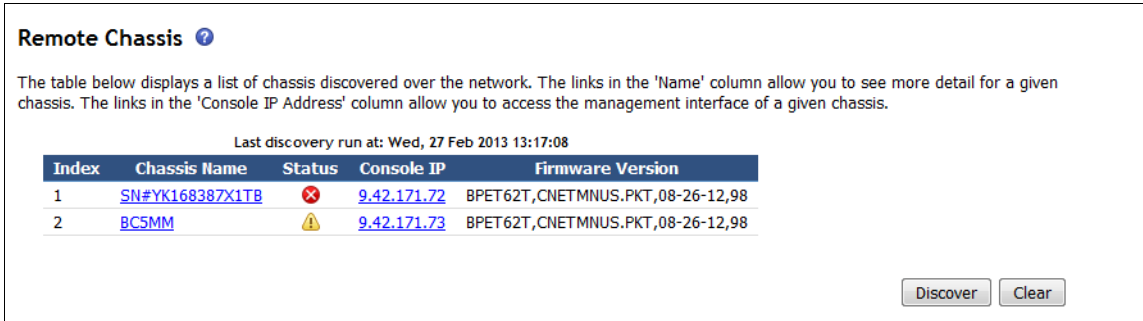


Figure 5-22 Remote Chassis window displaying discovered chassis

The **remotechassis** command provides this function on the command line:

```
remotechassis {-ip|-name|-health}{-clear}
```

where:

- ip <filter> Filter by IP address pattern. Example: -ip 192.*
- name <filter> Filter by system name pattern. Example: -name System*
- clear Clears the list of discovered chassis.
- health Show the chassis grouped by status.

Examples of the **remotechassis** command are shown in Figure 5-23.

```
system> remotechassis -T mm[1]
Running chassis discovery...
-----
Name:          SN#YK168387X1TB
IP:            9.42.171.72
IPv6:          Disabled
Status:         critical
Firmware:       BPET62T,CNETMNUS.PKT,08-26-12,98
Type:           management-module
Serial:         YK168387X1TB
FRU:            39Y9661
Chassis Serial: 23A4318
Chassis FRU:    25R5780
Chassis MTM:    885223Z
Chassis UUID:   3AEF456FB1857A9C564C189C4D874D16
-----
Name:          BC5MM
IP:            9.42.171.73
IPv6:          fe80::211:25ff:fec3:23ba
Status:         attention
Firmware:       BPET62T,CNETMNUS.PKT,08-26-12,98
Type:           management-module
Serial:         YK118165A1M8
FRU:            39Y9661
Chassis Serial: KQL6083
Chassis FRU:    25R5780
Chassis MTM:    88524XU
Chassis UUID:   8AC177F05ECC3C789C8329C6FF1811AA
-----
```

Figure 5-23 The **remotechassis** command

5.4 Blade tasks

This section addresses the tasks that you are able to perform by using the Blade Tasks window within the AMM:

- ▶ 5.4.1, “Blade Power/Restart” on page 349
- ▶ 5.4.2, “Remote Control Status” on page 352
- ▶ 5.4.3, “Updating blade firmware” on page 362
- ▶ 5.4.4, “Configuration” on page 364
- ▶ 5.4.5, “Serial Over LAN” on page 374

5.4.1 Blade Power/Restart

You can use the Blade Power/Restart window to perform a number of tasks related to powering one or more blades on and off as shown in Figure 5-24.

Blade Power / Restart ?

Blade selection and status

Click the checkboxes in the first column to select one or more blades; then, click one of the actions in the action list below the table and click "Perform Action" to perform the desired action.

This table will automatically refresh.

<input type="checkbox"/>	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect	Management Network
<input type="checkbox"/>	1	SN#Y011UN1BK0JP	Off	Enabled	On		<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	SN#Y010UF1BE0B9	On	Enabled	On		<input checked="" type="checkbox"/>
<input type="checkbox"/>	3	ADXblade1	On	Enabled	N/A		<input checked="" type="checkbox"/>
<input type="checkbox"/>	4	Blade13-HS22	On	Enabled	On		<input checked="" type="checkbox"/>
<input type="checkbox"/>	5	ADXblade2	On	Enabled	N/A		<input checked="" type="checkbox"/>
<input type="checkbox"/>	6	SN#Y111UN234018	On	Enabled	On		<input checked="" type="checkbox"/>

Available actions

Some actions presented in the dropdown list may not be supported on all blade types. Please consult your blade hardware documentation and support to understand any limitations.

Power On Blade

Standard blade actions

Power On Blade

Power Off Blade

Shut Down OS and Power Off Blade

Restart Blade

Issue NMI to Blade

Enable Local Power Control

Disable Local Power Control

Enable Wake on LAN

Disable Wake on LAN

Restart Blade System Mgmt Processor

POWER blade specific actions

Restart Blade and clear NVRAM

Restart Blade with Diagnostic Boot

Restart Blade with Diagnostic Boot and Default Bootlist

Restart Blade to SMS boot menu

Perform action

Figure 5-24 Blade Power/Restart window

you can select from the following power choices:

- Power on blade

Allows you to power on any blade in the chassis. Select the check box next to the blade name and then click **Power On Blade** to complete the action.

► Power off blade

Allows you to power off any blade in the chassis. Select the check box next to the blade name and then click **Power Off Blade** to complete the action.

Hard shutdown: Choosing this option does not save any user data. The blade will shut down immediately. Data loss might occur.

► Shutdown OS and Power Off Blade

Choose this option to shut down the OS and then power off the blade. It is the equivalent of shutting down the blade from inside the operating system. This option is not supported on all blade types.

► Restart blade

Choose this option to immediately power cycle the selected blades. User data is saved before restart.

► Issue NMI to Blade

Choose this option to issue a non-maskable interrupt (NMI) to the selected blades. This option is not supported on all blades.

► Enable local power control

With this option enabled for a blade, a user can power the blade on and off using the power button on the blade itself.

► Disable local power control

With this option disabled for a blade, a user cannot power the blade on and off using the power button on the blade itself.

► Enable Wake on LAN

Enables the Wake on LAN feature on the blade.

► Disable Wake on LAN

Disables the Wake on LAN feature on the blade.

► Restart blade system management processor

This option allows you to restart the baseboard management controller (BMC) service processor that is integrated into a blade. This might be required when you update firmware for the BMC.

From the command line, you can interact with blades by using the **power**, **reset**, and **shutdown** commands:

```
power -off|-cycle {-c}|-state|-on {-c}|-softoff|-wol|-local|-fp|-ap
reset {-c}|-std|-exd|-full|-sft|-clr|-dg|-ddg|-sms}
shutdown {-f}
```

The **power** command has the following options:

-off	Power off
-cycle	Power off, then on
-c	Enter console mode at power-on (used on blades with -on or -cycle)
-state	Display current blade power state
-on	Power on
-softoff	Shut down OS and power off blade
-wol	Enable/Disable wake on LAN globally, or on a per blade basis (enabled, disabled)
-local	Enable/Disable local power control globally, or on a per blade basis (enabled, disabled)
-ap	Blade auto-power on policy (restore, auto, or manual)

The **reset** command has the following options:

-c	Enter console mode after reset
-sft	Soft reset
-clr	Reset and clear NVRAM
-dg	Reset and run diagnostic tests
-ddg	Reset and run diagnostic tests with the default boot list
-sms	Reset to SMS boot menu

The shutdown command has the following option:

-f	Forces a shutdown for the specified blade server
----	--

Restrictions: The following options have restrictions:

- ▶ **-c** and **-softoff** are not supported on all blade types.
- ▶ **-wol**, **-local**, and **-fp** must be used exclusive of the other options.

5.4.2 Remote Control Status

The Remote Control Status window, which is shown in Figure 5-25, allows you to assume remote control of any xSeries blade that is installed in the chassis.

Remote Control Status ?

Firmware status: Active

KVM owner (since 10/19/2011 11:11:48): Blade2 - SN#Y010UF1BE089 ▼

Media tray owner (since 02/26/2013 13:22:35): Blade2 - SN#Y010UF1BE089 ▼

Console redirect: No session in progress.

Refresh

Start Remote Control ?

Click "Start Remote Control" to control a blade remotely. A new window will appear that provides access to the Remote Console and Remote Disk functionality. On this window, you will have full keyboard and mouse control of the blade which currently owns the KVM. You will also be able to change KVM and media tray ownership.

Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java Plug-in is not already installed. Remote Control is supported for Sun JRE 6.0 update 10 or later versions.

Start Remote Control

Remote Control Settings ?

- ☒ Enable local KVM switching
- ☒ Enable remote KVM switching
- ☒ Enable local media tray switching
- ☒ Enable remote media tray switching
- ☒ Allow multiple concurrent remote video sessions per blade

[Concurrent KVM Configuration](#)

Save

Figure 5-25 Remote Control Status main window

Remote Control Status

You can use this window to perform these tasks:

- ▶ Determine the blade that currently owns the keyboard, video, mouse (KVM). If no blade is selected, no user owns the KVM.
- ▶ Check which blade currently owns the use of the media tray.
- ▶ See the console redirect, which allows you to determine the user account and IP address of the user who might has a console session open to one of the blades.

Start Remote Control

Click **Start Remote Control** in Figure 5-25 on page 352 to remotely control the KVM of a blade that is installed in the chassis.

When you start the remote control, the local console of the selected blade along with various controls is displayed at the top of the browser window as shown in Figure 5-26.

By default, no remote console is displayed. Select a blade from the KVM menu under **Remote Console**. Doing so enables the console output for the selected blade.

Tip: To start using remote control, click your mouse in the area of the console. To release the mouse pointer, press the left Alt key.

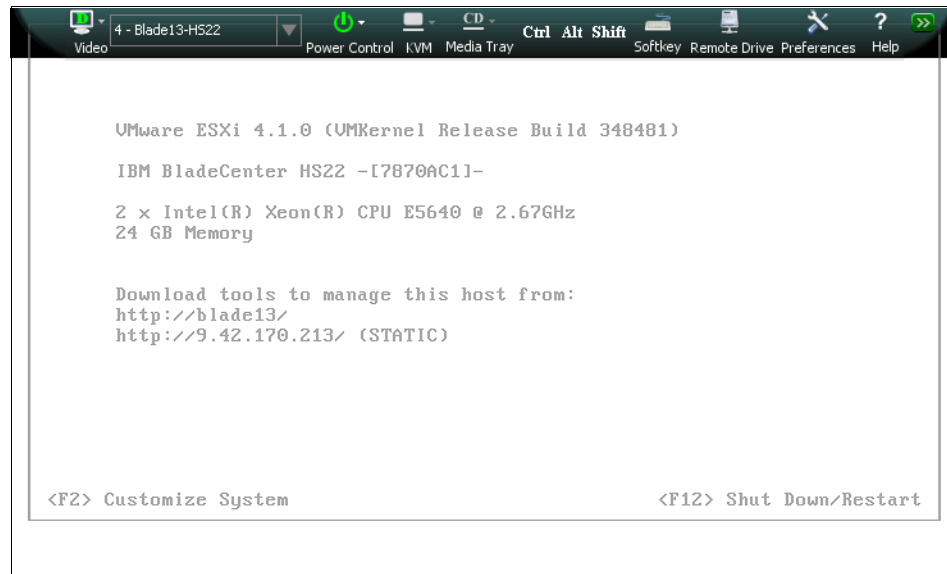


Figure 5-26 A sample window of the Remote Console interface

There are a number of options available within this console. The most common are described. For more information, see the help icons, shown as a question

mark (?), that are included with the console. Use Figure 5-26 on page 353 to refer to the options listed:

► Video

When a Blade is selected using the pull-down list, either an “A” or a “D” is displayed in the Video icon. This informs the user which Video Mode, Analog or Digital, is being displayed.

No display: When the KVM menu is set to “None”, nothing is displayed.

► KVM

This pull-down list is used to control which blade's video is displayed. For blades that do not have functional concurrent video, this menu also controls which blade owns the physical chassis KVM. The default selection is None, which means that no video is being displayed. To view the video output for a blade, click the arrow and select the blade that you want to view.

Servers not shown: Blades that do not have video controllers are not shown in this list.

When the blade's video is displayed, left-click the server's video image. Commands from the client system's local mouse and keyboard are then directed to the remote blade server instead of the local client. To redirect keyboard and mouse commands to the local client, “release” the mouse by pressing the **LEFT-ALT** key on the client's local keyboard.

► Power Control

When a blade is selected in the KVM pull-down, this button shows the current power state of the selected blade. If the blade is powered on, the power icon is green. The icon is gray when the blade is powered off, and yellow when it is hibernating or in standby mode. This button is used to change the power state of the selected blade. When you click it, a drop down list opens and shows the available options. If the blade is off, hibernating, or in standby mode, the only option is **Power On**. The options **Power Off**, **Restart**, **Shut down OS and power off**, and **Issue NMI to blade** are available when the selected blade is on.

► KVM button

This button is used to assign the physical chassis KVM ownership to a blade. Clicking it displays a list with the blades in the chassis. The blade that currently owns the chassis KVM has a mark before its name, and the blade name is gray. If **None** is selected in the KVM pull-down, the icon is gray. The icon is green when a blade is selected.

The **kvm** command provides this function from the command line:

kvm {-b|-local}

where:

- b: Blade number of the KVM owner (a blade number of 0 indicates no owner)
- local: Enable/Disable local KVM switching globally (enabled, disabled)

Figure 5-27 shows running the **kvm** command to set blade 2 as the KVM owner and disable local KVM control. The **kvm** command without options displays the current KVM settings.

```
system> kvm -b 2 -local disabled
OK
system> kvm
-b 2
-local disabled
```

Figure 5-27 The kvm command

► Media Tray button

This button is used to control which blade owns the physical media tray of the chassis. To assign the media tray to a blade, click the arrow and select the blade that you want to own the media tray. The blade that currently owns the chassis media tray has a mark before its name, and the blade name is gray.

The **mt** command displays and configures media tray functions:

mt {-b|-local|-remote}

where:

- b: Blade number of the media tray owner (a blade number of 0 indicates no owner)
- local: Enable/Disable local media tray switching globally (enabled, disabled)
- remote: Enable/Disable remote media tray switching globally (enabled, disabled)

Figure 5-28 shows running the **mt** command to set blade 2 as the media tray owner and disable local media try control. The **mt** command without options displays the current media tray settings.

```
system> mt -b 2 -local disabled -remote enabled
OK
system> mt
-b 2
-local disabled
-remote enabled
```

Figure 5-28 The *mt* command

Pull-down menu disappears: If you use this pull-down list several times in a row, it might disappear. This is a known limitation of web browsers. If this happens, refresh or reload the browser window.

Disabling the Remote Disk feature also disables remote Media Tray switching and Remote Disk on Card switching from blade to blade.

► Remote Drive

Clicking **Remote Drive** opens the Remote Drive window, which is used to mount and unmount virtual media. You cannot set or configure the remote drive from the command line. Figure 5-29 shows the Remote Disk window.

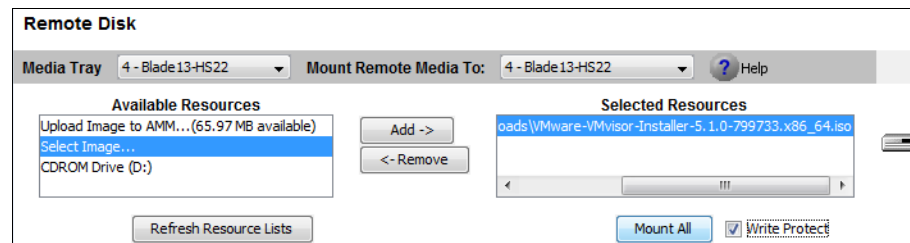



Figure 5-29 Remote Disk window

– Available Resources

Use this selection to specify the virtual media that can be mounted to the blade selected in the Mount Remote Media To list box. The following items are available:


- Upload Image to AMM (xxMB available)

Use this selection to upload files to the embedded storage space available on the AMM. The amount of available space on the AMM is

shown as xxMB (32MB, for example). When you select this item and click , you are presented with a dialog box used to select the image file. The image file is then uploaded to the AMM and added to the Selected Resources box. You can then click **Mount All** to mount the image to either the chassis KVM owner, which is the current blade displayed in the KVM window, or the Chassis Media Tray Owner device, which is the current blade displayed in the media tray window.


- Select image

Use this selection to select images that you want to mount. These images are not uploaded to the AMM. When you use this selection, a USB connection is established between the file on your client system and the device selected in the Mount Media To menu.

To select an image file, click **Select Image** in the Available Resources menu, then click . Browse to the file that you want to use. After you select the file, the file is automatically listed in the Selected Resources list box. Click **Mount All** to make the file available to the blade that you have selected.

You can use diskette and CD images. Diskette images must have either the IMG or BIN extension. CD images must have a valid iso9660 file system, and are expected to have the ISO file extension.

- CD-ROM (x) or Removable Drive (x)

If you have a local CD-ROM or diskette drive attached to your computer, you can select this device as a resource to be available to the selected blade. The (x) represents the CD-ROM or diskette drive letter that is recognized by your local computer. To make the drive available, select the required drive and click . Click **Mount All** to make it available to the blade.

- Write Protect

This check box is used to write protect diskette images and physical diskette drives when they are mounted. It has no effect on images that are uploaded to the AMM, or when mounting ISO images or physical CD-ROM drives.

Note: This check box must be selected *before* you mount the diskette image or physical diskette drive.

- KVM pull-down list

This menu allows you to select the blade that you want to control remotely. The default selection is **None**, which means that no video is being displayed. Selecting a server from the list displays its video, and transfers mouse and

keyboard control to you. Blades, such as the JS20 and JS21 that do not have video controllers, are not shown in this list.

If the blade that you select does not have a cKVM card installed, selecting a server from this list also makes the blade server active on the local console.

If the blade that you select does have a cKVM card installed, selecting a server from this list does not change the blade server active on the local console. To force the local console to also switch to the server that is being viewed in this remote session, click **KVM**.

Note: The KVM button is only displayed when you show a blade server that has a cKVM card installed, and that blade's display does not also appear on the local console.

Connecting to blades without video cards

Blades that do not have video card installed cannot use the Remote Control function from the AMM web interface. The AMM provides serial over LAN support through the command line for accessing the console on supported blades. The **sol** and **console** commands are used to achieve this.

The syntax for the **sol** command is as follows:

```
sol {-c|-e|-i|-r|-s|-t|-status}
```

The command displays and configures the sol settings for the advanced management module (AMM) or specified blade. It has these options:

-c	Retry count (0-7)
-e	Escape sequence
-i	Retry interval (10-2550ms, increments of 10)
-r	Blade reset sequence
-s	Send threshold (1-251 bytes)
-t	Accumulate timeout (5-1275ms, increments of 5)
-status	SOL status (enabled, disabled)

An example of the **sol** command is shown in Figure 5-30.

```
system> sol -T blade[3]
-status enabled
SQL Session: Ready
SQL retry interval: 250 ms
SQL retry count: 7
SQL bytes sent: 16737
SQL bytes received: 0
SQL destination IP address: 192.199.199.83
SQL destination MAC: 00:21:5E:BF:97:2C
SQL I/O module slot number: 1
SQL console user ID:
SQL console login from:
SQL console session started:
SQL console session stopped:
Blade power state: On
```

Figure 5-30 The sol command

The syntax for the **console** command is as follows:

```
console {-l|-o}
```

This command starts SOL session to the target blade. It has these options:

- l Causes the SOL session not to reconnect if it drops
- o Override existing SOL session (if there is one), and start a new one

An example of the **console** command is shown in Figure 5-31.

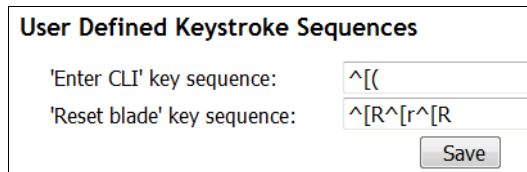
```
system> console -T blade[3]

AIX Version 7
Copyright IBM Corporation, 1982, 2012.
Console login:
```

Figure 5-31 The console command

After you are connected to the console, use the escape sequence to exit. This setting is configured in the AMM. To view the current settings, click **Blade**

Tasks → Serial Over Lan → Serial Over LAN Configuration → User Defined Key Stroke Sequences. Figure 5-32 shows the default settings.



The window is titled "User Defined Keystroke Sequences". It contains two text input fields. The first field is labeled "'Enter CLI' key sequence:" and contains the text "^[(". The second field is labeled "'Reset blade' key sequence:" and contains the text "^[R^[r^[R". Below these fields is a "Save" button.

Figure 5-32 User Defined Keystroke Sequences window

You can also review this from the command line by using the **-e** option as shown in Figure 5-33.

```
system> sol -T mm[1]
-status enabled
-c 7
-e ^[(
-i 250
-r ^[R^[r^[R
-s 250
-t 150
VLAN ID 4095
```

Figure 5-33 SOL settings

The default escape sequence is **Esc+Shift+9**. You can change these settings in the web page in Figure 5-32 or by using the **sol -e value** command where *value* is the key sequence. In this sequence, ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences.

Examples:

- ▶ v ^[((the carat symbol followed by a left bracket) means Esc v.
- ▶ ^M (the carat symbol followed by a capitol M) means carriage return.

Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences.

Remote control settings

Remote control settings are at the bottom of the Remote Control main window as seen in Figure 5-25 on page 352. The following Remote Control Settings can be applied. Click **Save** to commit any changes:

- ▶ **Enable local KVM switching**

With this check box selected, a user standing in front of a chassis is able to change the KVM owner by using the push buttons on each blade.

- ▶ **Enable remote KVM switching**

If this box is selected, remote users can change the KVM owner by using the menu on the Remote Control applet. To disable the KVM ownership switching on the Remote Control applet, click to clear this box and click **Save**.

- ▶ **Enable local media tray switching**

With this check box selected, a user standing at chassis is able to change the media tray owner by using the push buttons on the blade. This setting does not prevent another remote user from changing the media tray ownership through the web interface.

- ▶ **Enable remote media tray switching**

With this check box selected, remote users are able to change the media tray owner by using the menu on the Remote Control applet. This setting does not prevent a user from changing the media tray ownership through the button on a blade. If the remote disk feature is disabled, this check box is disabled.

- ▶ **Allow multiple concurrent remote video sessions per blade**

If this box is checked, a maximum of four users can concurrently view the video of the same blade by using the remote console applet. To limit this setting to allow only one user to access it at a time, click to clear this check box.

5.4.3 Updating blade firmware

Use the Update Blade Firmware window, which is shown in Figure 5-34, to update the BMC firmware on a specific blade. It cannot be used to update the blade system BIOS, diagnostics, or other firmware.

Update Blade Firmware ?

To update a firmware component, select a target blade and a firmware file, and click "Update".

Bay	Name
<input type="checkbox"/>	1 SN#Y011UN1BK0JP
<input type="checkbox"/>	2 SN#Y010UF1BE0B9
	3 ADXblade1 (cannot be flashed)
<input type="checkbox"/>	4 Blade13-HS22
	5 ADXblade2 (cannot be flashed)
<input type="checkbox"/>	6 SN#Y111UN234018

Firmware file

☐ Remote file

Browse...

Update

Figure 5-34 Update Blade Firmware window

- To perform the update, complete these steps:
1. Browse to the file by using **Browse**. The firmware file has a PKT extension.
 2. Click **Update** to begin the firmware upload.
 3. A progress indicator is displayed as the file is transferred to temporary storage on the advanced management module (AMM). Remain on this window until the transfer is complete.
 4. Verify that the type of file that is shown on the Confirm Firmware Update window is what you intended to update. Click **Continue** to begin the process. If not, click **Cancel**.
 5. A progress indicator is displayed as the firmware update progresses. Remain on this window until the process is complete, at which point a status window is displayed to indicate whether the update was successful.

Note: Only supported blades are available for selection.

The **update** command loads a pkt file to flash either the AMM, blade service processor, or I/O module from the command line.

The command has the following syntax:

```
update {-a|-activate|-img|-r|-u|-v}
```

where:

- a Display firmware info
- activate Activate the specified firmware image on I/O modules that support this
- img Image index to update, on I/O modules that support updating images
- r Automatically reboot AMM if firmware update succeeds
- u Remote location of firmware to update. Must specify the filename.
- v Verbose mode

Use one of the following protocols: tftp, ftp, ftps, http, or https to retrieve the firmware image for flashing. An example of a qualified location is `tftp://192.168.0.1/tmp/<Filename>.pkt`.

Figure 5-35 shows flashing the firmware and rebooting the AMM.

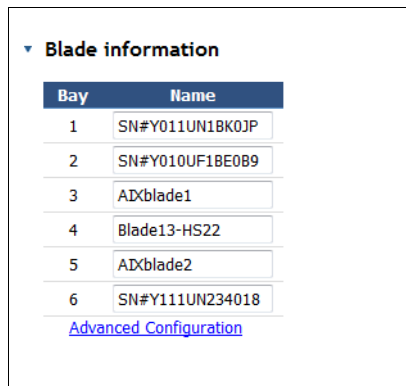
```
system> update -v -u tftp://192.168.192.1/CNETCMUS.pkt -T mm[1]
IPv6 address(es) have been configured for one or more
interfaces/protocols/services on this AMM. Note that if you update the
firmware to a level which does not support IPv6, all IPv6 connectivity will
be lost, and services/interfaces for which an IPv6 address was configured
may not function properly. You will be required to reconfigure these
services/interfaces.
100% transferred (53099016/53099016)
Transfer completed successfully
Flashing firmware to target device
Starting flash packet preparation.
Flash preparation - packet percent complete 26.
Flash preparation - packet percent complete 70.
Flash preparation - packet percent complete 86.
Flash preparation - packet percent complete 96.
Flash preparation - packet percent complete 98.
Flash operation phase starting.
Flashing - packet percent complete 34.
Flashing - packet percent complete 50.
Flashing - packet percent complete 82.
Update of AMM Main Application firmware was successful.
The new firmware will become active after the next reset of the MM.
system> Connection closed.
```

Figure 5-35 The update command

Note: Updating to older firmware levels might cause the loss of certain functions.

5.4.4 Configuration

The Configuration window, shown in Figure 5-36, allows you to perform a number of useful tasks that are related to blade configuration. These tasks include setting a boot sequence for a blade.



The screenshot shows a web-based configuration window titled "Blade information". It contains a table with two columns: "Bay" and "Name". The table lists six blades with their respective bay numbers and names. Below the table is a link labeled "Advanced Configuration".

Bay	Name
1	SN#Y011UN1BK0JP
2	SN#Y010UF1BE0B9
3	ADxblade1
4	Blade13-HS22
5	ADxblade2
6	SN#Y111UN234018

[Advanced Configuration](#)

Figure 5-36 Sample blade configuration information window

There are five subheadings on this window:

- ▶ “Blade Information”
- ▶ “Blade Policy Settings” on page 368
- ▶ “Service Processor’s Ethernet over USB” on page 368
- ▶ “Management Network Configuration” on page 370
- ▶ “Boot Sequence” on page 372
- ▶ “Boot Mode” on page 373
- ▶ “Concurrent KVM Configuration” on page 374

Blade Information

You can use this window to enter a name for the blades that are installed in the chassis. Enter the new name in the name column next to the bay number where the blade is installed as shown in Figure 5-37. Click **Save** when done.

▼ Blade information

Bay	Name
1	<input type="text" value="Blade_Slot_1"/>
2	<input type="text" value="Blade_Slot_2"/>
3	<input type="text" value="ADXblade1"/>
4	<input type="text" value="Blade_Slot_4"/>
5	<input type="text" value="ADXblade2"/>
6	<input type="text" value="Blade_Slot_6"/>

[Advanced Configuration](#)

Figure 5-37 Blade information

The **config** command config displays and configures general settings:

```
config {-name|-contact|-loc|-uuid|-tm|-sn}
```

where:

-contact	Quote-delimited AMM contact (47 characters maximum)
-loc	Quote-delimited AMM location (47 characters maximum)
-name	Blade or AMM name (15 characters maximum)
-uuid	Universally unique identifier (32 hex digits, no spaces)
-tm	Type/Model (7 alphanumeric characters)
-sn	Serial number (7 alphanumeric characters)

Figure 5-38 shows examples of use.

```
system> config -T blade[1]
-name SN#Y011UN1BK0JP
system> config -name HS22_Blade_1 -T blade[1]
OK
system> config -T blade[1]
-name HS22_Blade_1
```

Figure 5-38 The config command

Running the command against a target displays the general settings. Running **config** without a target displays the settings for the current working environment.

Note: Changing **-uuid**, **-tm**, or **-sn** is not recommended. Change these values only if you are certain they were not programmed correctly on the hardware. Invalid Machine Type/Model or Serial No can cause a failure to call home. If you change the UUID on an existing system to a random new value, IBM Director treats it as a new system, distinct from the one identified by the old UUID.

There is also an Advanced Configuration link, which displays a window, Figure 5-39, where you can record data specific to the chassis bay, which is known as Blade Bay Data (BBD).

The BBD is written to the blade currently inserted in that bay. If you replace the existing blade with a new blade, the new blade gets this bay data and any existing data that the new bay might have had is overwritten.

Blade Bay Data ?

Bay	Bay Data Status	Blade Bay Definition
1	BSMP	This is the blade in bay 1
2	Supported	
Blade Bay Data	ported	
4	Unsupported	
5	Unsupported	
6	BSMP	

Figure 5-39 Blade Bay Data window: Data about the specified chassis bay

Up to 60 characters are available. This data is accessible to software that runs on the blade and can be used, for example, as part of a deployment procedure to decide what function this blade performs. The data is stored in SMBIOS as an OEM Type 11 string with the format “\$Bdstring” where *string* is the BBD defined in the management module.

The status column shows whether the blade server currently inserted supports this bay data. The following are the possible values:

- ▶ Blade not present: There is no blade installed in the bay.
- ▶ Unsupported: The management processor on the blade does not support the BBD functions. You might be able to upgrade the IMM or BMC firmware to a version that supports BBD. POWER blades are not supported.
- ▶ BSMP: The management processor (also known as Blade Systems Management Processor or BSMP) of the blade supports BBD, but BIOS has

not read the current BBD definition. This is an operational state. The operating system that is running on the blade can read the BBD from the BMC.

BIOS has not read the BBD either because it must be rerun or the BIOS firmware level that is installed does not support BBD. First, try rerunning BIOS by powering off and on, restarting, or removing and reinstalling the blade. If that does not work, load the latest BIOS firmware to see if it supports BBD.

- ▶ Supported: The blade fully supports BBD. The latest BBD definition is in both the BMC and BIOS SMBIOS structure.
- ▶ Discovering: This is displayed for the short time while a blade is being discovered by the AMM.

If the text fields are disabled, you are logged in to the AMM with insufficient privileges. Write operations require Blade Configuration authority.

The **baydata** command displays and configures bay data:

```
baydata {-b|-clear|-data}
```

where:

- b Blade bay number
- clear Clears bay data for the specified bay or all bay data if no bay is specified
- data Quote-delimited user data (60 characters maximum)

Figure 5-40 shows the bay data for blade 1 being changed.

```
system> baydata -b 1

Bay  Status      Definition
1    Supported
system> baydata -b 1 -data "This is the blade in bay 1"
OK
system> baydata -b 1

Bay  Status      Definition
1    BSMP        This is the blade in bay 1
```

Figure 5-40 The baydata command

Blade Policy Settings

Blade Policy Settings allow you to enable or disable the following settings:

- ▶ Local power control
- ▶ Local KVM control
- ▶ Remote KVM control
- ▶ Local media tray control
- ▶ Remote media tray control
- ▶ Multiple concurrent remote video sessions per blade
- ▶ Wake on LAN
- ▶ Auto-power on mode

Figure 5-41 illustrates the Blade Policy Settings window.

Note: These settings apply to all blade bays (including the empty bays).

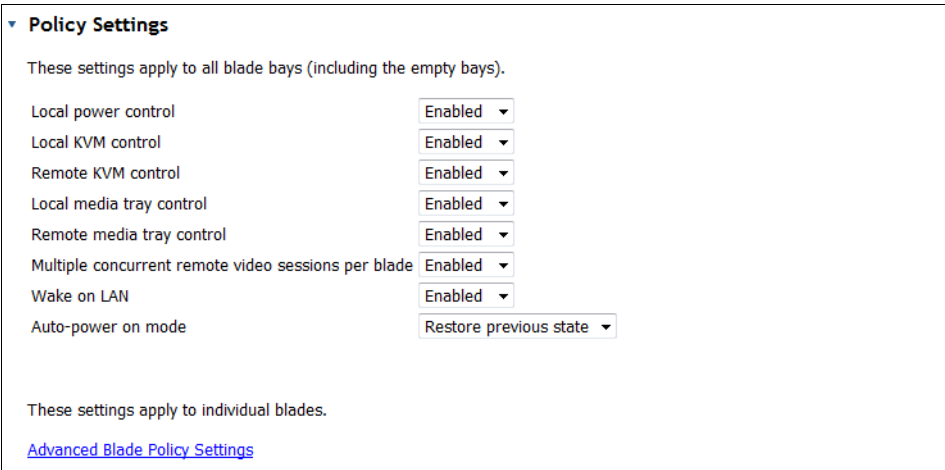


Figure 5-41 Blade Policy Settings window

For more information about changing the Blade Policy Settings from the command line, see Table 5-3 on page 338.

Service Processor’s Ethernet over USB

This window allows the user to view the status of, enable, or disable a blade SP’s command interface on Ethernet-over-USB. Not all blades support this feature.

The normal operational state for this interface is enabled, but it can be useful to temporarily disable it for some maintenance tasks. See Figure 5-42.

Service Processor's Ethernet over USB interface

Use this section to enable or disable commands on Ethernet-over-USB.

Blade selection and status

Click the checkboxes in the first column to select one or more blades, then click Enable or Disable.

<input type="checkbox"/>	Bay	Name	Status
<input type="checkbox"/>	1	SN#Y011UN1BK0JP	Enabled
<input type="checkbox"/>	2	SN#Y010UF1BE0B9	Enabled
<input type="checkbox"/>	4	Blade13-HS22	Enabled
<input type="checkbox"/>	6	SN#Y111UN234018	Enabled

Status refresh may take a moment.

Refresh

Enable or disable commands on Ethernet-over-USB

Enable

Disable

Figure 5-42 Service Processor's Ethernet over USB interface

The **ethoverusb** command displays and configures a blade SP's command interface on Ethernet-over-USB:

ethoverusb {-s}

where:

-s Enable or disable a blade SP's command interface on Ethernet-over-USB (enabled, disabled)

Management Network Configuration

The settings on this window apply to the internal network between the AMM and the Blade System Management Processors (BSMP or BMC). See Figure 5-43.

Blade Configuration

Information and PolicyManagement NetworkBoot SequenceBoot ModeConcurrent KVMOpen Fal

General options

VLAN ID

4095

Enable management network auto-discovery☐

Interface management

The links in this table will allow users to configure management network interface(s) on some blades. Note that only ce support this configuration.

Bay	Name
1	SN#Y011UN1BK0JP
2	SN#Y010UF1BE0B9
3	ADXblade1
4	Blade13-HS22
5	ADXblade2
6	SN#Y111UN234018

Figure 5-43 Management Network configuration window

The window allows you to adjust the following settings:

- ▶ VLAN ID
This is the virtual LAN ID for the internal management network between the AMM and the blade BSMPs. The range of valid VLAN IDs is 3 - 4095. To change this setting from the command line, use the **ifconfig** command with the **-v** flag:

```
ifconfig -ethx -v vlan_id
```


where x is the NIC number and -v vlan_id from 3 - 4095, inclusive. If you enter a value outside this range, an error is displayed.
- ▶ Enable management network auto-discovery
This control allows you to choose whether management network auto-discovery is enabled or not. When management network auto-discovery is enabled, the AMM determines the communication channel based on the expansion cards installed on a blade and I/O modules installed in the chassis. The communication path is given higher preference on high speed I/O

Modules over low speed I/O Modules, and is done automatically. The user cannot select the management communication path.

► Blade Network Configuration

This section displays a table that shows all the blades in the chassis. To change the network configuration for a blade, click the blade name link. Another window opens where the settings can be changed and saved. Note that only certain blade types support this configuration. Like changing the VLAN ID, use the **ifconfig** command to change the Blade Network Configuration from the command line as shown in Figure 5-44.

```
eth0      eth0
-up/down Enabled
-c dhcp
-i 169.254.2.55
-s 255.255.255.0
-g 0.0.0.0
-v 0
-b 00:21:5E:BF:97:2C
-ipv6 enabled
-ipv6static enabled
-id 2
-i6 ::
-p6 0
-g6 ::
-dhcp6 enabled
-sa6 enabled
Link-local address: fe80::221:5eff:febf:972c
Link-local address prefix length: 64
Stateless auto-config IP Addresses      Prefix Length
-----
fe80::221:5eff:febf:972c                  64
system> ifconfig -eth0 -up -ipv6 disabled -T blade[3]
OK
```

Figure 5-44 Enabling the blade management network from the CLI

In the example, eth0 is enabled and IPv6 is disabled for Blade 3. The management network uses DHCP as the default configuration.

Note: The **ifconfig** command is responsible for IP addressing of all the management interfaces in the chassis. It has many options that go beyond the scope of this book. For more information, see the *IBM BladeCenter Advanced Management Module: Command-Line Interface Reference Guide* at:

<http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kplaupdf.pdf>

Boot Sequence

The Boot Sequence window, shown in Figure 5-45, is useful for setting the boot sequence for either an individual blade or all of the blades.

Blade Configuration						
Information and Policy Management Network Boot Sequence Boot Mode Concurrent KVM Open Fab						
Follow the links in the Name column to edit the boot sequence settings of individual blades.						
Bay	Name	1 st Device	2 nd Device	3 rd Device	4 th Device	
1	SN#Y011UN1BK0JP	UEFI	CDROM	USB Floppy	Hard Drive 0	
2	SN#Y010UF1BE0B9	UEFI	CDROM	USB Floppy	Hard Drive 0	
3	AIXblade1	Hard Drive 0	No device	No device	No device	
4	Blade13-HS22	Hypervisor	Hard Drive 0	CDROM	USB Floppy	
5	AIXblade2	Hard Drive 0	No device	No device	No device	
6	SN#Y111UN234018	CDROM	USB Floppy	Hard Drive 0	Network	

Figure 5-45 Blade Boot Sequence window

To change the boot sequence of one specific blade (or all blades), click the name of the blade in Figure 5-45. The window shown in Figure 5-46 is displayed. Specify the order and optionally select **Apply to all blades** if you want to set this boot sequence to all currently installed blades.

Bay 3 - AIXblade1: Blade Boot Sequence ?

1st device

Hard drive 0

2nd device

CD-ROM

3rd device

Hard drive 1

4th device

Network

☐ Apply to all blades

Figure 5-46 Boot sequence for a specific blade

The **bootseq** command also displays and configures the blade boot sequence.

```
bootseq {-all}{bootSequence}
```

where:

-all	Applies settings to all blades
-T blade[X]	Applies settings to blade number X

The **bootseq -T** parameter has the following options:

usb	Media tray for non-POWER-based blades only
usbdisk	USB device (not supported by all blades)
iscsi	iSCSI boot device
iscsicrt	iSCSI Critical
nw	Network
nodev	No device
hd0	Hard disk drive 0
hd1	Hard disk drive 1
hd2	Hard disk drive 2
hd3	Hard disk drive 3
hd4	Hard disk drive 4
cd	CD-ROM
hyper	Hypervisor
legacy	Legacy only
uefi	Unified Extensible Firmware Interface

Note: All blades do not support all boot options. A maximum of four devices can be selected. If less than four are listed, the rest are set to nodev.

Boot Mode

This displays a table that shows all the blades in the chassis. To change the boot mode for a blade, click the blade name link as shown in Figure 5-47.

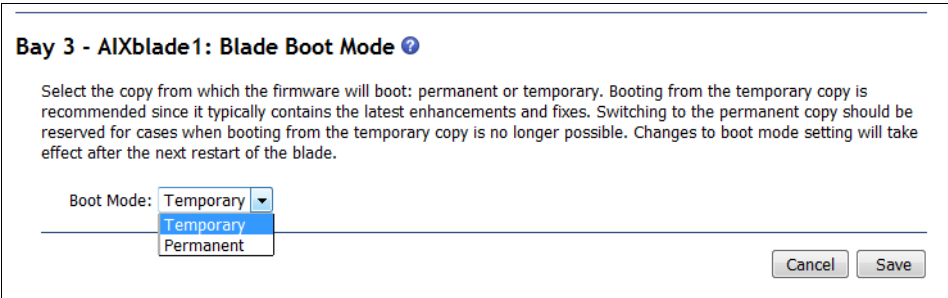


Figure 5-47 Blade Boot Mode

This setting allows you to boot from temporary or permanent firmware. Changes to the boot mode take effect after the next restart of the blade. You can also change this setting by using the **bootmode** command:

```
bootmode {-p {temp|perm}}
```

Concurrent KVM Configuration

Clicking Concurrent KVM Configuration at the top of the Configuration window shows Figure 5-48. Here, you can enable or disable a cKVM daughter card if one is installed.

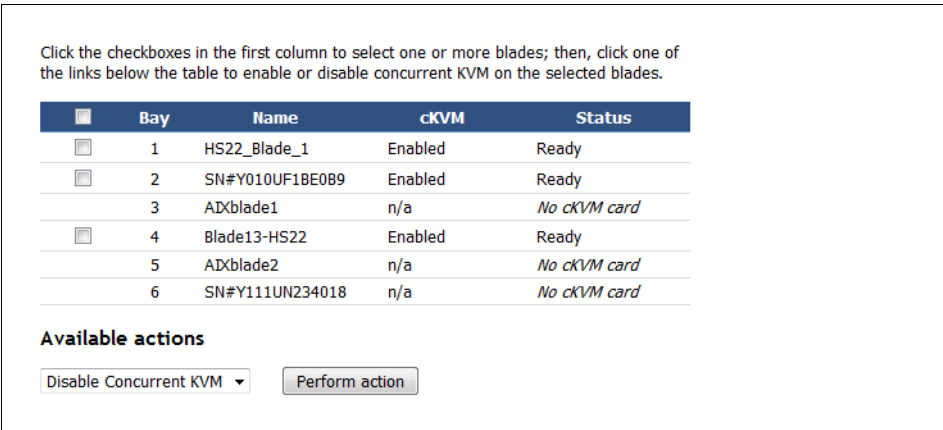


Figure 5-48 Concurrent KVM configuration pane

5.4.5 Serial Over LAN

The Serial Over LAN (SOL) window allows you to enable SOL for individual blades. This is useful for blades without local consoles, such as the PS700. You can enable SOL on individual blades and set various parameters. For more information, see “Connecting to blades without video cards” on page 358.

5.5 I/O module tasks

You can use the I/O Module Tasks window to run a number of tasks. These include powering I/O modules on or off, enabling external ports (which are disabled by default), and configuring the IP address of the I/O modules for external management.

This section includes the following topics:

- ▶ 5.5.1, “I/O Module Power/Restart” on page 375
- ▶ 5.5.2, “Configuration” on page 376
- ▶ 5.5.3, “Updating I/O module firmware” on page 379

5.5.1 I/O Module Power/Restart

The I/O Module Power/Restart window is shown in Figure 5-49.

I/O Module Power/Restart ?

Select one or more module(s) using the checkboxes in the first column, select the desired action below the table, and then click "Perform action" to p

<input type="checkbox"/>	Bay	Type	Manufacturer	MAC Address	IP Address	Pwr	Unique ID	Type	ID	Stacking Mode
<input type="checkbox"/>	1	Intelli. Copper PM	IBM (BNT)	n/a	n/a	On	n/a		n/a	n/a
<input type="checkbox"/>	2	Intelli. Copper PM	IBM (BNT)	n/a	n/a	On	n/a		n/a	n/a
<input type="checkbox"/>	3	SAS Conn Mod	IBM (n/a)	00:14:5E:C3:2B:BB	View	On	n/a		n/a	n/a
<input type="checkbox"/>	4	SAS Conn Mod	IBM (n/a)	00:14:5E:C3:2C:2E	View	On	n/a		n/a	n/a

[†] If this notation is shown next to an IP address, it means the address is the external stack management address.

Available actions

Power On Module(s) ▾

Perform action

I/O Module Advanced Setup ?

Select a module I/O module 1 ▾

Fast POST

Disabled ▾

External ports

Enabled ▾

Figure 5-49 I/O Module Power/Restart pane

You can perform a number of functions from this window, most of which are self-explanatory. For more information, click the online help, which is displayed as a question mark (?).

The last setting in Figure 5-49 is of particular note. The external ports of an I/O module are disabled by default. You must enable them before inserted cables (for example, Ethernet cables) will function. This action is required for security purposes. It ensures that you do not mistakenly enable unauthorized access. You can also use the **ifconfig** command from the command line with the **-ep** flag:

```
ifconfig -ep <enabled/disabled> -T switch[1-4]
```

Note: When you are using Copper pass-thru modules (CPM), the SOL console function shows “SOL is not ready” for any blades if the CPM in switch bay 1 does not have the external ports enabled, and ports 1-6 up and linked.

5.5.2 Configuration

The I/O Module Configuration window allows you to manually configure the IP addressing information for each I/O module that is installed in the chassis. This capability might be useful if you did not use the Configuration Wizard for the initial installation process. You can also perform other tasks, such as enabling the I/O module ports for external management or resetting the I/O module settings to the factory default.

You see the information in Figure 5-50 for each I/O module bay.

Note: Only static IP addresses are supported on I/O modules. Dynamic Host Configuration Protocol (DHCP)-assigned addresses are not supported.

Current IP Configuration

Configuration method: Static
IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

To change the IP configuration for this I/O module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

New Static IP Configuration

Configuration status: Enabled
IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

[Advanced Options](#)
[Zone Configuration Management](#)

Save

Figure 5-50 IP address configuration window for the I/O modules

Subnet requirement: You access the I/O module’s internal IP address through the AMM’s external Ethernet port IP address. Therefore, both the AMM’s IP address and the I/O module’s IP address must be on the same subnet.

When you use the IBM SAS RAID Controller Module (RSSM), assign an IP address to the SAS switch interface and the RAID controller. To configure the I/O module IP address from the command line, use the **ipconfig** command:

```
ifconfig {-i|-g|-s|-ir|-gr|-sr} -T switch[1-4]
```

where:

-i	IPv4 address
-g	Gateway
-s	Subnet mask
-ir	IP address for RAID controller
-gr	Gateway for RAID controller
-sr	Subnet mask for RAID controller

Copper pass-thru module: When you use copper pass-thru modules with the RSSM, connect ports 7 and 14 to the same subnet as the AMM to access the RAID controller interfaces.

Advanced configurations for the I/O module

As seen in Figure 5-50 on page 376, each I/O module window has an **Advanced Configuration** link. Clicking this link presents you with the following options:

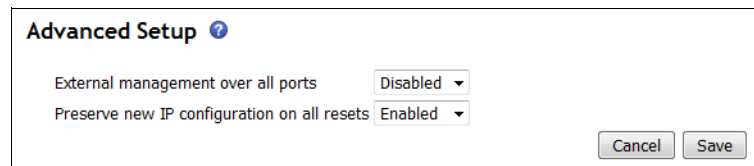
► POST Results

This window displays the results for the latest power-on self-test (POST) that this I/O module ran.

► Advanced Setup

This section, shown in Figure 5-51, allows you enable or disable the ability to run management tasks by using the I/O module's web interface through the external ports. When this field is set to disabled, only the management module ports can be used to change the configuration on this module.

You can also decide whether you want the IP address configuration to be preserved when the module is reset to factory defaults.



Advanced Setup ?

External management over all ports Disabled ▾

Preserve new IP configuration on all resets Enabled ▾

Cancel Save

Figure 5-51 Advanced Setup options

► Restore Factory Defaults

To restore the module configuration to its factory defaults, click **Restore Defaults** as shown in Figure 5-52. You are asked to confirm this action. Doing so causes the module to be reset and go through POST.

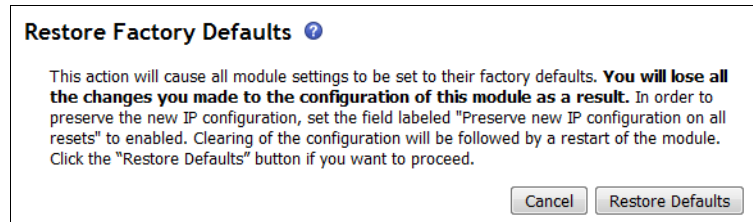


Figure 5-52 Restore Factory Defaults window

To restore factory defaults from the command line, use the **clear** command:

```
clear -cnfg
```

Valid targets are mm[1] and switch[1-4].

► Send Ping Requests

You can test the internal path between the management module and the I/O module by sending it ping requests, as shown in Figure 5-53.

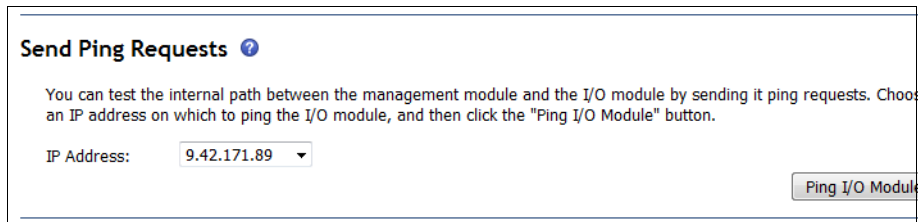


Figure 5-53 Send Ping Requests interface

The command-line interface also supports the **ping** command:

```
ping {-i | no argument}
```

where:

- i The '-i' option can take one of three arguments:
 - An IPv4 or IPv6 address to ping.
 - No argument. This must be targeted to an I/O module such as `switch[3]`, and prints an indexed table of IP addresses for the target I/O module.

- An index from the table of IP addresses. This must also be targeted to an I/O module, and looks up the associated IP address for the specified index.
- no argument Pings the associated IP address that is assigned to the module.

Figure 5-54 shows the use of the **ping** command.

```
system> ping -T switch[1]
Reply from 9.42.171.89: bytes=32 time<40ms
Reply from 9.42.171.89: bytes=32 time<108ms
Reply from 9.42.171.89: bytes=32 time<309ms
Reply from 9.42.171.89: bytes=32 time<57ms
```

Figure 5-54 The ping command

► Start Telnet/Web Session

You can use these buttons to start a Telnet (port 23) or web browser (or https) session with the I/O module.

The Java 1.4 Plug-in is required for the Telnet session. You are given the option to download and install the plug-in if necessary. For best results, use Sun JRE 1.4.2_08 or higher.

5.5.3 Updating I/O module firmware

The Update I/O Module Firmware window allows you to update the firmware for the I/O modules that are installed in your chassis. Updating firmware is done one module at a time.

Not all I/O modules support updating firmware through this interface. You will only see a list of the modules that support this type of update. See Figure 5-55.

Figure 5-55 Interface for updating I/O module firmware

Refer to Figure 5-35 on page 363 for instructions on updating the I/O Module Firmware by using the **update** command.

5.6 Storage tasks

You can use the Storage Configuration window, which is shown in Figure 5-56, to select and apply one of the user-defined configurations that you created using Storage Configuration Manager, or one of the predefined zone configurations if you are using a SAS module.

Storage Configuration ?

Use the following links to jump down to different sections on this page.

[I/O Modules](#)

I/O Modules ?

Zone Configuration

Select any link shown under the "I/O Module Type" column to change the zone configuration for your installed I/O Modules. If no link is displayed, you be powered off, in a fault state, the IP address of the I/O Module is not on the same subnet as the AMM or it may not have completed its initialization. If a SAS RAID Controller Module and SAS Connectivity Module are installed in slot 3 and 4 of BCS chassis, AMM must prevent one of them from powering on, otherwise it would be conflict with the Storage Module access and possibly corruption of data.

Bay	I/O Module Type	Active Zone Configuration	Zone Config. Type	
3	SAS Conn Mod	Predefined Config 06	Pre-defined	Chassis: BCS. SAS modules: 2. Disks per Blade: 4. Zoned Blade
4	SAS Conn Mod	Predefined Config 06	Pre-defined	Chassis: BCS. SAS modules: 2. Disks per Blade: 4. Zoned Blade

Figure 5-56 Zone configuration settings overview

To select and implement a zone configuration, complete these steps:

1. Click the **Storage Module** link, which is in the I/O Module Type column, of the I/O module that you want to change the zone configuration for.
2. Figure 5-57 is displayed. Select the zone configuration that you want to apply.
3. Select **Activate Selected Configuration** to commit the change.

Note: You must configure the same zone configuration type for both I/O modules. Having different zone configurations per I/O module is not supported.

Zone Configuration Management for I/O Modules ?

☒ Show the zone configuration that is most appropriate for my current number of blades and SAS I/O Modules

☐ Show all possible zone configurations available. I will choose one myself (recommended for advanced users)

☐ Do not change the zone configuration at this time

The table below displays zone configurations stored on the given I/O Module. Please select the desired zone configuration from the list and activate it. The activate button would be helpful in refreshing the status once the zone is applied. If you have multiple SAS RAID Controller Modules or SAS Connectivity Modules in working order, a check box will be provided that allows you to easily apply the same configuration to each I/O Module. The default setting is to apply the configuration to each. If you uncheck the check box, information for both I/O Modules will be presented and you can select a zone configuration from the list. It is highly recommended that you select the same zone configuration for both I/O Modules.

☒ Apply the same zone configuration to both I/O Modules

I/O Module 3 (SAS Conn Mod) ?

The table below lists zone configurations that is most appropriate for my current number of blades and SAS I/O Modules. **Note:** The currently active configuration will match the recommended configuration in your current setup.

Select	Active?	Name	Type	Intended # of Blades	Intended # of SAS Modules	Max Disks per Blade	Configuration Store	Date
<input checked="" type="radio"/>		Predefined Config 02	Pre-defined	6	2	1	6	04/24/2012 02:00
<input type="radio"/>	✓	Predefined Config 06	Pre-defined	3	2	2	10	04/24/2012 02:00

Activate Selected Configuration

Figure 5-57 Zone configuration settings (each I/O module must have the same zone configuration)

For more information about the available zone configuration options, see Chapter 3, “Getting started using the BladeCenter S chassis” on page 99.

5.7 Management module control

There are a number of management windows under management module control:

- ▶ 5.7.1, “General Settings” on page 382
- ▶ 5.7.2, “Login profiles” on page 386
- ▶ 5.7.3, “Alerts” on page 394
- ▶ 5.7.4, “Managing alerts from the command line” on page 398
- ▶ 5.7.5, “Passive air filter reminder” on page 400
- ▶ 5.7.6, “Serial port” on page 400
- ▶ 5.7.7, “Port assignments” on page 401
- ▶ 5.7.8, “Network interfaces” on page 402
- ▶ 5.7.9, “Network protocols” on page 404
- ▶ 5.7.10, “Miscellaneous services” on page 411
- ▶ 5.7.11, “Configuring services from the CLI” on page 411
- ▶ 5.7.12, “Chassis Internal Network (CIN)” on page 414
- ▶ 5.7.13, “Security” on page 415
- ▶ 5.7.14, “File management” on page 416
- ▶ 5.7.15, “Update AMM firmware” on page 418
- ▶ 5.7.16, “Configuration management” on page 418
- ▶ 5.7.17, “Restart AMM” on page 425
- ▶ 5.7.18, “License Manager” on page 426

5.7.1 General Settings

The AMM General Settings window allows you to run the following tasks:

- ▶ “AMM Information”
- ▶ “AMM Date and Time”
- ▶ “Network Time Protocol (NTP)” on page 385
- ▶ “Trespassing Warning” on page 385

AMM Information

Enter AMM information, such as the name you want to give to the BladeCenter S, the contact name and information of a support member, or the physical location of the device. An example is shown in Figure 5-58 on page 383. Click **Save** to commit the changes. Refer to the **config** command shown in Figure 5-38 on page 365 to change the AMM information from the command line.

AMM Date and Time

To set the AMM date and time settings, complete these steps:

1. Click **Set MM Date and Time**.
2. The window shown in Figure 5-58 is displayed. Enter the date and time.
3. Select the correct time zone by clicking the menu and selecting the relevant time zone.
4. Select **Automatically adjust daylight saving changes** if your region uses this.

MM Date and Time ?

Date (mm/dd/yyyy) 02 / 27 / 2013

Time (hh:mm:ss) 14 : 40 : 41

GMT offset -5:00 - Eastern Standard Time (Eastern USA, Ontario, Quebec) ▼

☒ Automatically adjust for daylight saving changes

Network Time Protocol (NTP) ?

NTP auto-synchronization service Disabled ▼

Cancel Save

Figure 5-58 MM Date and Time settings with NTP disabled

The **clock** command is used to change the date and time settings from the command line.

`clock [-options]`

where:

-d	Date (mm/dd/yyyy)
-t	Time (hh:mm:ss)
-g	GMT offset
-dst	Daylight saving time (on off special case)

For a GMT offset of +2:00, use one of the following values for **-dst**:

ee	Eastern Europe
gtb	Great Britain
egt	Egypt
fle	Finland
off	Off

For a GMT offset of +9:30, use one of the following values for **-dst**:

sa	South Australia
other	Other locations
off	Off

For a GMT offset of +10:00, use one of the following values for **-dst**:

ea	Eastern Australia
tanv	Tasmania, Australian Capital Territory, New South Wales, and Victoria
vlad	Vladivostok
off	Off

For a GMT offset in set {-9:00, -8:00, -7:00, -6:00, -5:00}, use one of these values for **-dst**:

uc	US and Canada
other	Other locations
off	Off

For a GMT offset of -4:00, use one of the following values for **-dst**:

can	Canada
other	Other locations
off	Off

The following example configures the time and date for a management module in the Eastern Time Zone with Daylight Savings for the US and Canada enabled:

```
clock -d 03/03/2013 -t 12:01:00 -g -5:00 -dst uc -T mm[1]
```

Network Time Protocol (NTP)

You can configure the AMM to keep its time automatically synchronized with an available Network Time Protocol (NTP) server. The NTP options are shown in Figure 5-59.

Network Time Protocol (NTP) ?

NTP auto-synchronization service: Enabled

NTP server fully qualified hostname or IP address: time1

NTP update frequency: 1400 Minutes

NTP v3 authentication: Enabled

Key index: 0

Key type: M - MD5

Key:

If the NTP auto-synchronization service is enabled, the AMM clock will be synchronized with the NTP server when you save your settings.

NTP is disabled.

Cancel Save

Figure 5-59 NTP time settings

Note: To enter host names, the DNS protocol must be configured. Otherwise, enter IP address information. For more information about configuring the AMM to use a DNS server, see “Domain Name System (DNS)” on page 404.

Trespassing Warning

The last setting on the General Settings window, MM Trespassing Warning, allows you to specify a message to any user who logs in to the AMM. Select **Enabled** in the menu, enter the message that you want the users to receive in the box, and click **Save** to commit the change. The **trespass** command sets this message from the command line:

```
trespass {-twd|-twe|-tw}
```

where:

- twd Reset the trespass warning to default value
- twe Trespassing warning enable (on, off)
- tw Quote-delimited trespassing warning message that is limited to 1600 characters

Tip: This message is displayed for all users, and can be any sort of informational message that you require, not just to dissuade unauthorized users.

5.7.2 Login profiles

The Login Profiles window is broken down into two sections, Login Profiles (Figure 5-60) and Account Security Management. With the Login Profiles window, you can create user accounts and define roles for those accounts. Account Security Management allows you to define how the user account authenticates to the AMM.

Creating login profiles

To create a basic user account within the Login Profiles section, complete these steps:

1. Select one of the available ~ *not used* ~ links in the Login ID column as shown in Figure 5-60. The AMM supports a maximum of twelve accounts.

Management Module Login Configuration ?

Use the following links to jump down to different sections on this page.

[Login Profiles](#)
[Group Profiles](#)
[Account Security Management](#)

Login Profiles ?

To configure a login profile, click a link in the "Login ID" column.

	Login ID	Role	Active Sessions	Last Login	Password Compliant	Days Until Password Expires	Dormant	State	Action
1	USERID	S	3	02/27/13 14:23:28	Yes	n/a		Active	
2	MIKE	S	0	11/30/10 13:56:03	Yes	n/a		Active	
3	~ not used ~								
4	~ not used ~								
5	~ not used ~								
6	~ not used ~								
7	~ not used ~								
8	~ not used ~								
9	~ not used ~								
10	~ not used ~								
11	~ not used ~								
12	~ not used ~								

Figure 5-60 Login Profiles pane

2. Enter a new account name and password.
3. In the **Maximum simultaneous active sessions** menu, select a number to determine the maximum concurrent active sessions that the AMM allows for this user. Values are 0-20, where 0 means unlimited.
4. Click **SSH Public Key Authentication** → **Add New Key** if you want to access Secure Shell (SSH) or Secure SMASH without using a password.
5. Select a Role that provides the user with the appropriate access. The choices are shown in Figure 5-61 on page 388:
 - Supervisor: No restrictions on the functions that the user is able to run. You can optionally specify which devices in the chassis (the chassis, specific blades, and specific I/O modules) the user can administer. The default is for all devices.
 - Operator: An operator role has only read-only access, and cannot run any save, modify, clear, or state-affecting operations.
 - Custom: Allows you to define custom roles and access scopes to assign to users.

SSH Public Key Authentication

This user currently has no keys.

Role

☒ Supervisor (requires Scope selection)
 ☐ Operator (readonly, all scopes)
 ☐ Custom (requires Roles and Scopes)

To move an item from one column to another, click the item or use either the enter key or the space bar when the item has focus.

Unassigned roles

Chassis operator
Chassis user account management
Chassis log administration
Chassis configuration
Chassis administration
Blade operator
Blade remote presence
Blade configuration
Blade administration
I/O module operator
I/O module configuration
I/O module administration

Assigned roles

Access Scope

To move an item from one column to another, click the item or use either the enter key or the space bar when the item has focus.

Unassigned

Assigned

Chassis
Blade 1
Blade 2
Blade 3
Blade 4
Blade 5
Blade 6
I/O Module 1
I/O Module 2
I/O Module 3
I/O Module 4

Figure 5-61 Supervisor Role Selection pane

The following roles are available for the Custom role selection:

- Chassis operator: The user can browse the status and properties of chassis components (AMM, chassis cooling devices, midplane, power modules, and media tray). This role can back up the AMM configuration.
- Chassis user account management: The user can add, modify, and delete user login profiles. Changing global login settings requires Chassis configuration authority.

388 Implementing the IBM BladeCenter S Chassis

- Chassis log administration: The user can clear the AMM event log and change log policy settings.
 - Chassis configuration: The user can modify and save any chassis configuration parameter except user profiles and event log settings. Examples include general AMM settings, AMM port assignments, AMM network interfaces, AMM network protocols, and AMM security. This user can restore AMM factory defaults if the user also has Chassis administration permissions. This user can also change the global login settings and the SOL configuration.
 - Chassis administration: This user can run AMM firmware updates, modify chassis LEDs, restore AMM factory defaults if the user also has Chassis configuration permissions, and restart the AMM.
 - Blade operator: This user can browse the status and properties of blades.
 - Blade remote presence: This user can access the Remote Control Web window and the functions that are provided on the window: Remote console (KVM) and remote disk. The CLI **console** command that starts an SOL session to a blade also requires this authority.
 - Blade configuration: This user can modify and save blade configuration parameters. These include parameters in the Blade Configuration web window and blade SOL parameters on the Serial Over LAN web window.
 - Blade administration: This user can power on and off and restart blades, activate standby blades, update firmware, and modify blade LEDs.
 - I/O module operator: This user can browse the status and properties of I/O modules, and can ping the I/O modules.
 - I/O module configuration: This user can modify the I/O module IP address and configure I/O module Advanced Management parameters.
 - I/O module administration: This user can power on and off and restart I/O modules, update I/O module firmware, and enable and disable the Fast POST and External Ports of an I/O module. To be able to start the I/O module telnet or web UI, or restore factory defaults, supervisor access is required for that I/O module. This means that both Switch Configuration and Administration roles must be assigned.
6. Click **Configure SNMPv3 Access** to use this access profile to access the AMM by using SNMP.
 7. Click **Save** to commit the changes.

To delete an existing user profile, click the name of the profile to edit it, and then click **Reset to Defaults** at the bottom of the window. You are prompted to confirm the action.

Managing login profiles from the command line

In addition to the Web Login Profiles interface, you use the command-line interface for all user management features with the **users** command:

```
users {-curr} | {-ts} | {<- [1-12]> { {-clear} | {-disable} | {-enable} | {-unlock} |  
{-n|-p|-op|-a|-cn|-ap|-pp|-ppw|-at|-i|-ms} } | -pk {<-key_index>|all}  
{ {-e} | {-remove} | { {-add} | {-upld|-dnld} {-i|-l} | {-af|-cm} } }
```

where:

Login profiles options:

-clear	Deletes a user (you can delete an empty user)
-curr	Displays currently logged in users
-ts	Terminates a user session
-disable	Disables a user's account
-enable	Enables a disabled user's account
-unlock	Unlocks a locked user's account
-n	User name (limited to 15 characters, must be unique)
-p	Password (limited to 15 characters)
-op	Old password, only necessary for users without account management authority to change own password
-a	role-based security level (operator, rbs:<role list>:<scope list>).
-cn:	Context name (limited to 31 characters, must be unique)
-ap:	Authentication protocol (md5, sha, none)
-pp:	Privacy protocol (des, aes, none)
-ppw:	Privacy password (limited to 31 characters)
-at:	Access type (get, set, trap)
-i:	IP address or host name (limited to 63 characters)
-ms:	Maximum simultaneous sessions that are allowed for the specified user (0 - 20 sessions)
-pk	Public key operations.

For the **-a** parameter, the roles are as follows:

super	Supervisor
co	Chassis Operator
cam	Chassis Account Management
clm	Chassis Log Management

cc	Chassis Configuration
ca	Chassis Administration
bo	Blade Operator
brp	Blade Remote Presence
bc	Blade Configuration
ba	Blade Administration
so	I/O Module Operator
sc	I/O Module Configuration
sa	I/O Module Administration

For the **-a** parameter, the scopes are as follows:

bX	Blade number X
bX-bY	Blades numbered X through Y
sX	I/O Module number X
sX-sY	I/O Modules numbered X through Y
cX	Chassis number X (X must be 1)

Note: <role list> and <scope list> are pipe '|' separated lists

The **-pk** parameter has the following SSH public keys options:

-e	Displays the entire key in OpenSSH format. This option takes no arguments, and must be used exclusive of other options.
-remove	Removes the specified key for the specified user. If the <-key_index> is 'all', it removes all keys for the specified user. This option takes no arguments, and must be used exclusive of other options.
-add:	Adds a public key for the specified user. This option is followed by the key in OpenSSH format, and must be used exclusive of other options.
-upld:	Used to upload a public key in OpenSSH format. This option must be used with the -i and -l options, and exclusive of other options. To replace a key with a new key, you must specify a key index. To add a key to the end of the list of current keys, do not specify an index.
-dnld:	Used to download the specified public key to a computer that is running a TFTP server. This option must be used with the -i and -l options, and exclusive of other options.
-i:	IP address of the TFTP server when uploading or downloading a key file.
-l:	File name of the key file when uploading or downloading through TFTP.

- af: Accept connections from host, in the format: from="<list>", where <list> is a comma-separated list of host names and IP addresses (limited to 511 characters, valid characters include alphanumeric, comma, asterisk, question mark, exclamation point, period, hyphen, colon, and percent)
- cm: Comment (limited to 255 characters, must be quote-delimited)

Note: When you are using the SSH public key options, the **-pk** option must be used after the user index.

Figure 5-62 shows changing the USERID supervisor account to “administrator” and adding a read only account named “Operator” that allows basic management functionality, but does not allow the user to change or reset the Management Module.

```
system> users -1 -n administrator -p passwd -a super -ms 20 -T mm[1]
OK
system> users -3 -n Operator -p passwd -a
rbs:ba|co|clm|bo|brp|ba|so:c1|b1|b2 -ms 10 -T mm[1]
OK
```

Figure 5-62 Creating and changing users from the command line

Account Security Management

Account Security Management allows you to globally define how the user account authenticates to the AMM as seen in Figure 5-63 on page 394. You can set the following options. Click **Save** to commit any changes you make.

- **User authentication method:** There are four options you can choose from:
 - Local Only: The user ID and password are verified by searching the list of users that are locally configured under Local Login Profiles.
 - LDAP Only: The users are authenticated through a remote LDAP server.
 - Local first, then LDAP: The AMM supports both authentication methods, but Local authentication is attempted first.
 - LDAP first, then Local: The AMM supports both authentication methods, but LDAP authentication is attempted first.

Select the appropriate method from the menu.

- **Web inactivity session timeout:** Use this field to indicate how long, in minutes, the AMM waits before disconnecting an inactive web session. Select the **no time-out** option to disable this feature. Select the **User picks time-out**

option (the default) if the time-out instead must be selected by the user during the login process.

- ▶ **CLI inactivity session timeout:** Use this field to indicate how long in seconds the AMM waits before disconnecting an inactive command-line interface session started from a Telnet or SSH client. If there is no traffic from the client for this many seconds, the AMM closes the Telnet or SSH connection. A value of 0 means that there is no timeout. The default timeout is 120 seconds (two minutes).
- ▶ **Number of simultaneous active sessions for LDAP users:** Use this field to indicate how many concurrent active sessions the AMM allows for each user who logs in using the LDAP authentication method. The minimum value is 1, and the maximum value is 20. A value of 0 means that there is no session limit for LDAP users.
- ▶ **Account security level:** There are three levels for the account security settings. Select the level that you want. Refer to the descriptions on the AMM for details.

Account Security Management ?

User authentication method

Local only

Web inactivity session timeout

User picks timeout

CLI inactivity session timeout (seconds)

0

Number of simultaneous active sessions for LDAP users

0

Do not log new authentication events for the same user for

5 minutes

Ignore client IP address when tracking user authentication events

☐

Account security level:

Security Level	Details
<input checked="" type="radio"/> Legacy security settings	No password required No password expiration No password re-use restrictions No password change frequency restrictions Account is locked for 2 minutes after 5 login failures Simple password rules No account inactivity monitoring
<input type="radio"/> High security settings	Password required Factory default 'USERID' account password must be changed on next login Force user to change password on first logi Passwords expire in 90 days Password re-use checking enabled (last 5 passwords kept in history) Minimum 24 hour interval between password changes Account is locked for 60 minutes after 5 login failures Complex password rules with 2 degrees of difference from previous password Alert on account inactivity after 120 days Accounts disabled after 180 days of inactivity
<input type="radio"/> Custom security settings	<div>Edit Security Settings</div>

Figure 5-63 Account Security Management options

5.7.3 Alerts

The management module Alerts Configuration window (Figure 5-64 on page 395) allows you to specify which events (from lists of critical, warning, and information alerts) are monitored, which event notifications are sent to whom, how event notifications are sent (SNMP, email, or IBM Director), whether to include the event log with the notification, and other alert parameters.

To successfully configure alerting, complete these steps:

1. Create one or more remote alert recipients.
2. Edit the global remote alert settings.
3. Set the alerts to monitor and be sent to the recipients you have configured.

Remote alert recipients

Remote alert recipients are users or systems (for example, IBM Director or an SNMP listener) that receive alerts from the AMM (Figure 5-64).

Management Module Alerts Configuration ?

Use the following links to jump down to different sections on this page.

[Remote Alert Recipients](#)
[Global Remote Alert Settings](#)
[Monitored Alerts](#)
[Passive Air Filter Reminder](#)

Remote Alert Recipients ?

To configure a remote alert recipient, click a link in the "Description" column.

Index	Description	Notification Method	Status
1	~ not used ~		
2	~ not used ~		
3	~ not used ~		
4	~ not used ~		
5	~ not used ~		
6	~ not used ~		
7	~ not used ~		
8	~ not used ~		
9	~ not used ~		
10	~ not used ~		
11	Win2008R2-04	IBM Director (comprehensive)	Receives all alerts
12	Win2008R2-02.davis.local.com	IBM Director (comprehensive)	Receives all alerts

Generate Test Alert

Figure 5-64 Remote Alert Recipients list

To create a remote recipient alert, complete these steps:

1. Click one of the ~ not used ~ links in the Remote Alert Recipients pane as seen in Figure 5-64 on page 395. The window shown in Figure 5-65 is displayed.

Remote Alert Recipient 1 ?

1. If you enable a SNMP over LAN recipient, you also need to complete the SNMP section on the [Network Protocols](#) page.
2. If you enable an E-mail over LAN recipient, you also need to complete the SMTP section on the [Network Protocols](#) page.
3. IPv6 is currently disabled. Any IPv6 configuration entered will not take effect until IPv6 is enabled.

By entering an email or SNMP address not assigned to your company, you are consenting to share hardware serviceable even the owner of that email or SNMP address not assigned to your company. In sharing this information, you warrant that you are with all import/export laws.

Status: Enabled

Name: John Smith

Notification method: E-mail over LAN

E-mail address (userid@hostname or userid@ip): jsmith45@us.ibm.com

Receives critical alerts only: ☐

Reset to Defaults Cancel

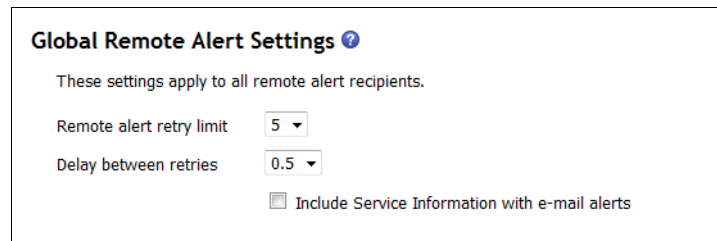
Figure 5-65 Recipient Alert configuration window

2. Select the **Receives critical alerts only** check box if you want this recipient to receive enabled critical alerts only. If this check box is not selected, the recipient receives all enabled alerts.
3. Set the **Status** to Enabled by selecting **Enabled** from the menu. This setting allows the recipient to receive alerts.
4. Create a useful name for the alert by entering a name in the Name box.
5. Select the Notification method by selecting the relevant choice from the menu. The following options are available:
 - **SNMP over LAN:** For this to work correctly, you must configure SNMP on the Network Protocols window. For more information about the configuration of SNMP, see 5.7.9, “Network protocols” on page 404.
 - **E-mail over LAN:** For this to work correctly, you must configure SMTP on the Network Protocols window. For more information about the configuration of SMTP, see the 5.7.9, “Network protocols” on page 404.
 - **IBM Director (comprehensive):** Enter the host name or IP address of the IBM Director server on your network. A recipient that uses the IBM Director (comprehensive) notification method receives all alerts that are generated by the AMM, regardless of whether the type of alert is enabled.

6. Click **Save** to commit the changes.
7. The Alerts main pane reopens. Generate a test by clicking **Generate Test Alert** to ensure that the alerting structure you have created works.

Global Remote Alert Settings

Use the Global Remote Alert Settings window (Figure 5-66) to specify whether you want the event log information included in the email alert that is sent. Select **Include event log with e-mail alerts** to enable this feature. You can also adjust the remote alert retry limit and the delay between retries.

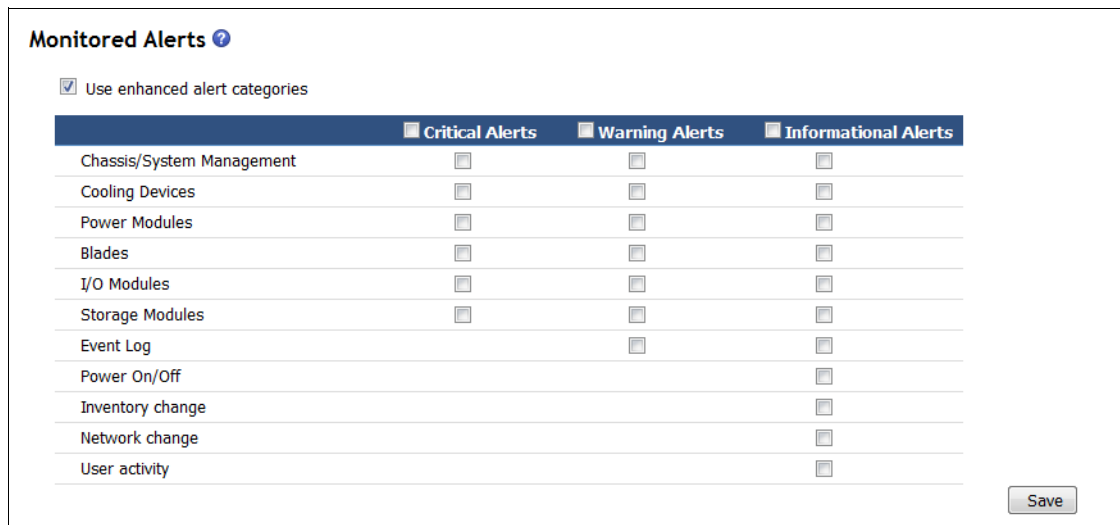


The screenshot shows the 'Global Remote Alert Settings' window. It has a title bar with a question mark icon. Below the title, it says 'These settings apply to all remote alert recipients.' There are two dropdown menus: 'Remote alert retry limit' set to '5' and 'Delay between retries' set to '0.5'. At the bottom, there is a checkbox labeled 'Include Service Information with e-mail alerts' which is currently unchecked.

Figure 5-66 Global Remote Alert Settings window

Monitored alerts

Monitored alerts (Figure 5-67) are user-selectable by category to allow the users to receive messages about the event through SNMP or email asynchronously.



The screenshot shows the 'Monitored Alerts' window. It has a title bar with a question mark icon. Below the title, there is a checkbox labeled 'Use enhanced alert categories' which is checked. Below this is a table with three columns: 'Critical Alerts', 'Warning Alerts', and 'Informational Alerts'. The table lists various alert categories with checkboxes for each. A 'Save' button is located at the bottom right.

	Critical Alerts	Warning Alerts	Informational Alerts
Chassis/System Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cooling Devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Power Modules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blades	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I/O Modules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Storage Modules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Event Log		<input type="checkbox"/>	<input type="checkbox"/>
Power On/Off			<input type="checkbox"/>
Inventory change			<input type="checkbox"/>
Network change			<input type="checkbox"/>
User activity			<input type="checkbox"/>

Figure 5-67 Monitored Alerts window

The specific alerts that you select here apply to all configured alert recipients. If the alert is recoverable, an informational alert is sent in the same category to indicate that a recovery has occurred. To enable monitored alerts, completed these steps:

1. Select the check box next to the alert types that you want to receive.
2. Click **Save**.

5.7.4 Managing alerts from the command line

You can use the **alertentries** and **monalerts** commands to configure alerts from the command line. First, you must configure an alert recipient and then configure which alerts are generated.

The **alertentries** command has the following syntax:

```
alertentries {{-[1-12]} {-del}|{-n|-status|-f|-t|-e|-i}}|{-test}
```

where:

-del	Deletes the specified alert entry (you can delete an empty alert recipient)
-n	Name (limited to 31 characters)
-status	Alert recipient status (on or off)
-f	Filter (critical or none)
-t	Type (snmp, email, or director)
-e	Email address (used with -t email)
-i	IP address/host name (used with -t director)
-test	Generates a test alert. Note: This option must be used by itself.

The **monalerts** command has the following syntax:

```
monalerts {-ec|-ca|-cb|-ciom|-cstg|-ccsm|-ccd|-cpm|  
-wa|-wb|-wiom|-wstg|-wscm|-wel|-wcd|-wpm|  
-ia|-ib|-iiom|-istg|-icsm|-ipon|-iinv|-iel|-inc|-iua|-icd|-ipm}
```

where:

-ec:	Enabled enhanced alerts categories with the command monalerts -ec enabled. Do not use the legacy alert categories. They will be removed in a subsequent release. Either begin using the enhanced alert categories or upgrade your existing alert categories to the enhanced format.
-------------	--

Critical Alerts:

-ca:	All critical alerts (enabled, disabled)
-cb:	Critical blade alerts (enabled, disabled)
-ciom:	Critical I/O module alerts (enabled, disabled)
-cstg:	Critical storage alerts (enabled, disabled)
-ccsm:	Critical chassis or system management alerts (enabled, disabled)
-ccd:	Critical cooling device alerts (enabled, disabled)
-cpm:	Critical power module alerts (enabled, disabled)

Warning Alerts:

-wa:	All warning alerts (enabled, disabled)
-wb:	Warning blade alerts (enabled, disabled)
-wiom:	Warning I/O module alerts (enabled, disabled)
-wstg:	Warning storage alerts (enabled, disabled)
-wscsm:	Warning chassis or system management alerts (enabled, disabled)
-wel:	Warning event log (enabled, disabled)
-wcd:	Warning cooling device alerts (enabled, disabled)
-wpm:	Warning power module alerts (enabled, disabled)

Informational Alerts:

-ia:	All informational alerts (enabled, disabled)
-ib:	Informational blade alerts (enabled, disabled)
-iiom:	Informational I/O module alerts (enabled, disabled)
-istg:	Informational storage alerts (enabled, disabled)
-icsm:	Informational chassis or system management alerts (enabled, disabled)
-ipon:	Informational Power on/off (enabled, disabled)
-iinv:	Informational inventory changes (enabled, disabled)
-iel:	Informational Event log (enabled, disabled)
-inc:	Informational Network change (enabled, disabled)
-iua:	Informational User activity (enabled, disabled)
-icd:	Informational cooling device alerts (enabled, disabled)
-ipm:	Informational power module alerts (enabled, disabled)

Note: **-ec** is executed first, followed by **-ca**, **-wa**, and **-ia**, and then the remaining options.

In Figure 5-68, alert recipient `snmp_server` is created, enabled, set to receive all critical alerts through `snmp` traps, and sends them to `monitorsrv.ibm.com`. Then, the AMM is configured to send all critical alerts to configured users.

```
system> alertentries -3 -status on -n snmp_server -f critical -t snmp -i
monitorsrv.ibm.com -T mm[1]
IPv6 is currently disabled. Any IPv6 configuration entered will not take
effect until IPv6 is enabled.
OK
system> monalerts -ca enabled -cb enabled -ccd enabled -ccsm enabled -ciom
enabled -cpm enabled -cstg enabled -T mm[1]
OK
```

Figure 5-68 Configuring alerts

5.7.5 Passive air filter reminder

The IBM BladeCenter Airborne Contaminant Filter must be cleaned or replaced regularly. Figure 5-69 shows how to configure a reminder alert to change the filter every one, three, or six months.

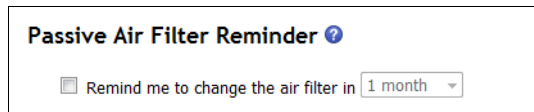
A screenshot of the 'Passive Air Filter Reminder' window. It has a title bar with the text 'Passive Air Filter Reminder' and a help icon. Below the title bar, there is a checkbox labeled 'Remind me to change the air filter in' followed by a dropdown menu currently set to '1 month'.

Figure 5-69 Passive Air Filter Reminder window

5.7.6 Serial port

Use the Serial Port field (Figure 5-70) to specify the data transfer rate of your serial port connection. Click the menus to adjust the settings.

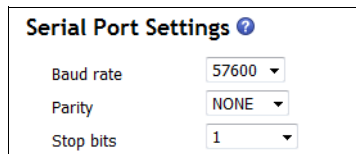
A screenshot of the 'Serial Port Settings' window. It has a title bar with the text 'Serial Port Settings' and a help icon. Below the title bar, there are three settings: 'Baud rate' with a dropdown menu set to '57600', 'Parity' with a dropdown menu set to 'NONE', and 'Stop bits' with a dropdown menu set to '1'.

Figure 5-70 Serial Port settings

5.7.7 Port assignments

You can use this window (Figure 5-71) to change the port numbers for the displayed services and protocols if you need to. You cannot configure a port to a number that is already in use. You must restart the AMM for the changes to take effect.

Open Ports ?

Protocol	Ports
TCP	21, 22, 23, 80, 427, 3900, 6090, 50022
UDP	67, 69, 161, 427

Changes to the Port Assignments below may not appear immediately in the Open Ports list. You may need to refresh the page.

Port Assignments ?

You can change the port number for the following services/protocols.
Note that you cannot configure a port to a number that is already in use.

HTTP	<input type="text" value="80"/>
HTTPS	<input type="text" value="443"/>
Telnet	<input type="text" value="23"/>
SSH	<input type="text" value="22"/>
SNMP Agent	<input type="text" value="161"/>
SNMP Traps	<input type="text" value="162"/>
FTP	<input type="text" value="21"/>
FTP Data	<input type="text" value="20"/>
TFTP	<input type="text" value="69"/>
Remote Presence	<input type="text" value="3900"/>
TCP Command Mode	<input type="text" value="6090"/>
Secure TCP Command Mode	<input type="text" value="6091"/>
SLP	<input type="text" value="427"/>
SMASH CLP	<input type="text" value="50023"/>
Secure SMASH CLP	<input type="text" value="50022"/>

Changes to port numbers will take effect immediately. Note that changing a port number will affect ongoing operations using the service at that port.

Figure 5-71 Port Assignments window

5.7.8 Network interfaces

The Network Interfaces window (Figure 5-72) allows you to configure the host name, IP address, and network interface connectivity settings of the AMM's external network interface.

The screenshot shows the 'Management Module' configuration window. At the top, there's a 'Hostname' field with 'BC6MM' and an empty 'Domain name' field. Below these is a checkbox for 'Register this interface with DNS'. A link for 'Advanced Ethernet Setup' is present. The 'IPv4' section is expanded, showing 'DHCP' set to 'Disabled - Use static IP configuration'. A warning message states: '*** Currently the static IP configuration is active for this interface. *** This static configuration is shown below.' Under 'IPv4 Static IP Configuration', there are fields for 'IP address' (9.42.170.210), 'Subnet mask' (255.255.254.0), and 'Gateway address' (9.42.170.1). The 'IPv6' section is also expanded, showing 'Link local address:' as empty, 'IPv6 static IP configuration' as 'Disabled', 'DHCPv6' as 'Enabled', and 'Stateless Auto-configuration' as 'Enabled'. A warning message at the bottom states: '⚠️ IPv6 is currently disabled. Any IPv6 configuration entered will not take effect until IPv6 is enabled.' A 'Save' button is at the bottom right.

Figure 5-72 Network interface settings for the AMM external Ethernet interface

External Network Interface (eth0)

Use the DHCP field to specify whether you want the TCP/IP settings for the AMM external network interface to be set through a DHCP server on your network. The following options are available to you:

- **Disabled - Use static IP configuration:** You must enter a static IP address in the Static IP Configuration window if you select this option. This is the preferred method of configuration.

- ▶ **Enabled - Obtain IP config from DHCP server:** This option allows the network interface to accept an IP address from a DHCP server.
- ▶ **Try DHCP server. If it fails, use static IP config:** Select this option if you want to try a DHCP server and revert to the static IP configuration if the DHCP server cannot be reached.

Select the relevant option from the menu and click **Save**.

Management module

Use this section to provide the host name and IP address settings for the AMM external network interface if you chose to use a static address.

The **Advanced Ethernet Setup** link, shown in Figure 5-73, allows you to configure the data rate and duplex settings on the AMM network interface. The default settings are **Auto** for both Data rate and Duplex. You can also override the burned-in MAC address by entering a locally administered address (LAA).

Advanced Ethernet Setup ?

Data rate: Auto

Duplex: Auto

Maximum transmission unit (bytes): 1500

Locally administered MAC address*: 00:00:00:00:00:00

Burned-in MAC address: 00:14:5E:E1:60:50

***Note:** The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.

Cancel Save

Figure 5-73 AMM external network interface Advanced Ethernet Setup

The **IP Configuration Assigned by DHCP Server** link shows you the currently assigned IP address of the AMM if you elected to use DHCP to get an address.


To configure the AMM IP address from the command line, use the **ifconfig** command.

Requirement: The **-eth0** flag is required for configuring the AMM from the CLI.

5.7.9 Network protocols

The Network Protocols window allows you to configure a number of options related to the network protocols used within the AMM. The options that are highlighted in bold are addressed:

- ▶ **Domain Name System (DNS)**
- ▶ **File Transfer Protocol (FTP)**
- ▶ Lightweight Directory Access Protocol (LDAP)
- ▶ Network Time Protocol (NTP)
- ▶ Remote Control
- ▶ Secure Shell (SSH) Server
- ▶ Service Location Protocol (SLP)
- ▶ **Simple Mail Transfer Protocol (SMTP)**
- ▶ **Simple Network Management Protocol (SNMP)**
- ▶ SMASH Command Line Protocol (CLP)
- ▶ SSL Client Configuration for LDAP Client
- ▶ SSL Server Configuration for Web Server
- ▶ Syslog Protocol
- ▶ TCP Command Mode Protocol
- ▶ Telnet Protocol
- ▶ Trivial File Transfer Protocol (TFTP)
- ▶ **Web Access (HTTP/HTTPS)**

This topic describes several of the common network protocols used. For information about the protocols that are not described, see the online help by clicking the help icon  next to the main heading.

Domain Name System (DNS)

Use this field to specify whether you use a DNS server on your network to translate host names into IP addresses. To allow use of a DNS server, completed these steps:

1. Click the menu and select **Enabled**.
2. Specify the IP address of a DNS server on your network (you can enter a total of three DNS servers).
3. Click **Save**. A restart of the AMM is required for this setting to take effect.

Note: If you are changing a number of settings on the Management Module Network Protocols window, select **Save All Settings** after you make all the necessary changes to the network protocols.

Figure 5-74 shows the DNS window.

Domain Name System (DNS) ?

DNS

Disabled

Preferred DNS Servers

IPv6

Send DDNS updates to these servers

☐

	IPv4	
Primary	0.0.0.0	0::0
Secondary	0.0.0.0	0::0
Tertiary	0.0.0.0	0::0

Figure 5-74 DNS server settings

Note: This setting affects all other settings on the AMM. If you want to use host names for alerting, SMTP, SNMP, and so on, you must configure DNS first.

File Transfer Protocol (FTP)

Use this field to specify whether the FTP server is enabled on the AMM as shown in Figure 5-75. To implement this setting, complete these steps:

1. Click the menu and select **Enabled**.
2. Set the FTP idle timeout if required. This is the FTP server inactivity timeout in seconds. If there is no traffic from an FTP client for this many seconds, the AMM closes the connection. A value of 0 means that there is no timeout. The default value is 5 minutes (300 seconds).
3. Click **Save** to commit the change.

File Transfer Protocol (FTP) ?

FTP server

Enabled

FTP idle timeout (seconds)

300

Trivial File Transfer Protocol (TFTP) ?

TFTP server

Enabled

Figure 5-75 FTP settings

Lightweight Directory Access Protocol (LDAP)

The AMM supports both local and remote authentication. Local refers to the authentication of users who are configured as one of the local user profiles defined on the Login Profiles page. The term “remote” refers to the use of LDAP servers to authenticate users who are not defined locally on the AMM.

Figure 5-76 shows the LDAP configuration. Enter the fully qualified host name or IP address of the LDAP server. For more information, see the (?) Help section.

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization

☐ Use LDAP Servers for Authentication Only (with local authorization)

☐ Use DNS to find LDAP Servers

☒ Use Pre-Configured Servers

Server	Fully Qualified Hostname or IP Address	Port
1.	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>
4.	<input type="text"/>	<input type="text"/>

Active Directory Settings

Enhanced role-based security

Disabled ▾

Group filter

Group Search Attribute

Login Permission Attribute

Miscellaneous Parameters

Root DN

Binding method

Anonymously ▾

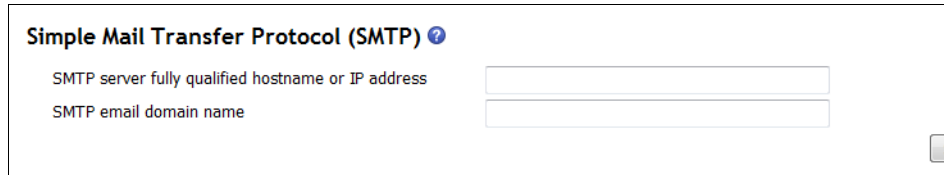
Enable or disable SSL: [LDAP section of the Security page.](#)

Save

Figure 5-76 LDAP settings

Simple Mail Transfer Protocol (SMTP)

Use this field (Figure 5-77) to specify either the IP address or, if DNS is enabled and configured, the host name of the SMTP server. Click **Save** to commit the change.

A screenshot of a web form titled "Simple Mail Transfer Protocol (SMTP)" with a help icon. The form contains two input fields: "SMTP server fully qualified hostname or IP address" and "SMTP email domain name". A "Save" button is located at the bottom right of the form.

Simple Mail Transfer Protocol (SMTP) ?

SMTP server fully qualified hostname or IP address

SMTP email domain name

Save

Figure 5-77 Simple Mail Transfer Protocol settings

Simple Network Management Protocol (SNMP)

This window (Figure 5-78) allows you to specify whether you want to send traps to the SNMP trap receivers configured in the community list, or to allow an SNMP manager to send get and set requests to the SNMP agent type specified.

Simple Network Management Protocol (SNMP) ?

SNMP traps*

Enabled

* If you enabled SNMP traps, you must also define an alert recipient from the Alerts page, and one of the SNMP agents, below, must be enabled and configured.

SNMPv1 agent†

Enabled

† If you enabled the SNMPv1 agent, you must also define at least one community below.

Community Name	Access Type	Fully Qualified Hostnames or IP Addresses‡
public	Get	1. 0.0.0.0 2. 3.
	Get	1. 2. 3.
	Get	1. 2. 3.

‡ The value 0.0.0.0 is not a valid trap destination IP address, so it is ignored for sending traps. One of the remaining IP addresses of that community may be configured with an explicit trap destination IP address.

SNMPv3 agent§

Enabled

§ If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles in order for the interaction between the SNMPv3 manager and SNMPv3 agent to work properly. You can configure these settings at the bottom of the individual login profile pages which can be reached via the Login Profiles page. Click the link for the login profile to configure, scroll to the bottom of the page and then click the "Configure SNMPv3 User" link.

Save

Figure 5-78 Simple Network Management Protocol configuration window

The following options are available for configuration:

- ▶ SNMPv1 agent: Use this field to specify whether you want to send traps to the SNMPv1 trap receivers configured in the community list or to allow a SNMPv1 manager to send get and set requests to the SNMPv1 agent. To enable the SNMPv1 agent, all of the following criteria must be met:
 - The AMM contact is specified.
 - The AMM location is specified.
 - At least one Community name is specified.

- At least one valid IP address is specified for that Community.
- In order for SNMPv1 trap receivers to receive traps, both SNMP traps and the SNMPv1 agent must be enabled.
- ▶ **SNMPv3 agent:** Use this field to specify whether you want to send traps to SNMPv3 trap receivers configured under Login Profiles, or to allow a SNMPv3 manager to send get and set requests to the SNMPv3 agent. To enable the SNMPv3 agent, all of the following criteria must be met:
 - The AMM contact is specified.
 - The AMM location is specified.

After the SNMPv3 agent is enabled, you can configure login profiles for SNMPv3 through the Login Profiles window. Click the link for the login profile to configure, scroll to the bottom of the window, and click **Configure SNMPv3 User**. A new window with SNMPv3 specific fields to configure is displayed. For SNMPv3 users to receive traps, both SNMP traps and the SNMPv3 agent must be enabled.

- ▶ **SNMP traps:** Use this field to convert all alert information into the AMM Management Information Base (MIB) SNMP format for those alerts to be sent to an SNMP trap receiver. To allow conversion of alerts to SNMP format, click the menu and select **Enabled**.

Note: Alert recipients whose notification method is SNMP will not receive alerts unless both SNMP traps and SNMP agent are enabled.

- ▶ **SNMPv1 Communities:** Use these fields to define the administrative relationship between SNMPv1 agents and SNMPv1 managers. You must define at least one Community to enable the SNMPv1 agent. Each Community definition consists of three parameters (Community Name, Access Type, and one or more Host Names or IP Addresses). Ensure that the SNMPv1 agent field is set to **Enabled**.

To set up a Community:

- In the Community Name field, enter the Community's authentication name string. Each name must be unique.
- In the Access Type field, select an access type. The **Trap** option allows all hosts in the community to receive traps. The **Get** option allows all hosts in the community to receive traps and query MIB objects. The **Set** option allows all hosts in the community to receive traps, query, and set MIB objects.
- In the Host Names or IP address field, enter the host names or IP addresses of the hosts that are allowed in the community. If an IP address of 0.0.0.0 is configured for the first host name in the first community, any

hosts can query MIB objects (if the Access Type is GET) or can query and set MIB objects (if the Access Type is SET). The value 0.0.0.0 is not a valid trap destination IP address, so it is ignored for sending traps. One of the remaining IP addresses of that community can be configured with an explicit trap destination IP address.

Web Access (HTTP/HTTPS)

You can use this menu to specify whether you want to allow web access to the AMM as shown in Figure 5-79. This field is **Enabled** by default. If you set this field to **Disabled**, you are no longer able to access the AMM management functions by using a web browser. You need to use one of the other access methods, such as SNMP access or command-line interface access through Telnet, SSH, or direct serial connection.

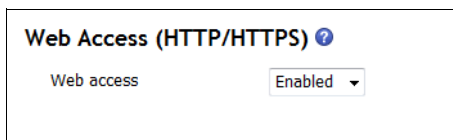
A screenshot of a web-based configuration interface. At the top, the title 'Web Access (HTTP/HTTPS)' is displayed in bold black text, followed by a small blue circular help icon. Below the title, the text 'Web access' is shown on the left, and a dropdown menu is on the right. The dropdown menu is currently set to 'Enabled' and has a small downward-pointing arrow on its right side.

Figure 5-79 Web Access settings

5.7.10 Miscellaneous services

Figure 5-80 shows some of the other services you can configure, including Telnet, TCP, SLP, CLP, syslog, and Remote control settings.

The screenshot displays a web-based configuration interface for miscellaneous services. It is divided into three sections, each with a title, a help icon, and a 'Save' button.

- Telnet Protocol**: Contains a 'Telnet mode' dropdown menu set to 'Enabled'.
- TCP Command Mode Protocol**: Contains three input fields: 'Command mode' (1), 'Secure command mode' (0), and 'Command mode inactivity timeout' (300). Each field is followed by a unit label: 'connections' for the first two and 'seconds' for the last.
- Service Location Protocol (SLP)**: Contains three input fields: 'SLP' (Enabled), 'Address type' (Multicast), and 'Multicast address' (239.255.255.253).

Figure 5-80 Miscellaneous services

5.7.11 Configuring services from the CLI

The **ports** command allows you to view and configure open ports, and enable or disable services from the command line.

```
ports {-options} | {{-open} | {-reset}} | {{protocol} <-[port_index]>}  
{-speed | -state}
```

where:

- open: Displays the currently opened ports
- reset: Reset all ports to default values
- speed: Port speed on I/O modules that support port configuration. Possible values for this option are displayed with the port information, and are in the format of {multiplier}{units}{duplex mode}. Examples: 100mh stands for 100 Mbps half-duplex, and 10gf stands for 10 Gbps full-duplex
- state: Operational state on I/O modules that support port configuration. Valid state is either “on” or “off”.

The protocol entry must be one of the following protocols with a configurable port number (1-65535):

-ftpp	FTP port.
-ftpdp	FTP Data port.
-http	HTTP port.
-https	HTTPS port.
-rpp	Remote presence port.

Note: -rpp is a consolidated network port to provide Remote Presence Network Services of KVM, Remote disk, Remote disk on card, and Storage Description Service.

-slpp	SLP port.
-smashsp	Secure SMASH CLP over SSH port.
-smashtp	SMASH CLP over Telnet port.
-snmpap	SNMP agent port.
-snmptp	SNMP traps port.
-sshp	SSH port.
-stcmp	Secure TCP Command Mode port.
-tcmp	TCP Command Mode port. IBM Director requires this be 6090.
-telnetp	Telnet port.
-tftpp	TFTP port. The default value is 69. Changing -tftpp to a non-default value causes firmware update through TFTP server failure if the AMM is being used as the TFTP server.

Notes:

- ▶ You cannot configure a port to a number that is already in use.
- ▶ Changes to port numbers take effect immediately.
- ▶ Changing port numbers affects ongoing operations that are using the service at that port.

Port settings to turn on/off a port/service:

-ftpe	FTP.
-httpse	HTTPS.
-rpe	Remote presence.

-kvme	KVM.
-ntpe	NTP.
-rde	Remote disk.
-rdoce	Remote disk on card.
-slpe	SLP.
-smashse	Secure SMASH CLP over SSH.
-smashte	SMASH CLP over Telnet.
-snmplae	SNMPv1 agent. To enable the SNMPv1 agent, the following criteria must be met: <ul style="list-style-type: none"> - AMM contact is specified - AMM location is specified - At least one Community name is specified - At least one valid IP address is specified for that Community
-snmp3ae	SNMPv3 agent. To enable the SNMPv3 agent, the following criteria must be met: <ul style="list-style-type: none"> - AMM contact is specified - AMM location is specified
-snmppte	SNMP traps.
-sshe	SSH.
-stcme	Secure TCP Command Mode (on/off or 0-20 connections). On a write, the maximum number of connections can be set explicitly (0-20). It can also be turned on (1 connection) or off (0 connections). On a read, "off" means 0 connections, and "on" means 1 or more connections. The total session count of TCP Command Mode (TCM) and Secure TCM (STCM) is limited to 20.
-tcme	TCP Command Mode (on/off or 0-20 connections). On a write the maximum number of connections can be set explicitly (0-20), or it can be turned on (1 connection) or off (0 connections). On a read, "off" means 0 connections, and "on" means 1 or more connections. The total session count of TCM and STCM is limited to 20.
-telnete	Telnet.
-tftpe	TFTP.

To set Port timeouts, use these parameters followed by a number in secs (0 - 4,294,967,295):

-ftpt	FTP timeout
-tcmt	TCP Command Mode timeout
-telnett	Telnet port timeout

Figure 5-81 turns on FTP and sets the timeout at ten minutes, turns off Telnet, changes the port that is used for Secure SMASH CLP over SSH to port 19, and enables SSH and SNMP.

```
system> ports -ftpe on -ftpt 36000 -tftpe on -telnete off -smashsp 19 -sshe  
on -snmppte on -T mm[1]  
Ok
```

Figure 5-81 Configuring ports from the CLI

5.7.12 Chassis Internal Network (CIN)

The Chassis Internal Network (CIN) provides internal connectivity between blade server ports and the internal AMM management port. This capability allows a user to access the Management Module from a blade server, for example, by opening a WEB, CLI or SNMP session. The communication path is two-way, such that the AMM can also use services on the blade, such as, LDAP, SMTP, DNS, and NTP.

Figure 5-82 displays the CIN configuration.

Chassis Internal Network (CIN) ?

Use the following links to jump down to different sections on this page.

[Enable Chassis Internal Network \(CIN\)](#)

[Chassis Internal Network \(CIN\) Configuration](#)

Enable Chassis Internal Network (CIN) ?

Chassis Internal Network Disabled ▾

Save

Chassis Internal Network (CIN) Configuration ?

Index	CIN VLAN ID	CIN IP Address	Action
1	not used	n/a	n/a
2	not used	n/a	n/a
3	not used	n/a	n/a
4	not used	n/a	n/a
5	not used	n/a	n/a
6	not used	n/a	n/a
7	not used	n/a	n/a
8	not used	n/a	n/a
9	not used	n/a	n/a
10	not used	n/a	n/a
11	not used	n/a	n/a
12	not used	n/a	n/a
13	not used	n/a	n/a
14	not used	n/a	n/a

Save

Refresh

Figure 5-82 Chassis Internal Network window

5.7.13 Security

Select **Security** to view or change the Secure Sockets Layer (SSL) settings for the web server and LDAP client, and to view or change the SSH server settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates that are provided by a certificate authority (CA). You can also enable or disable (the default) SSH, select the SSH version to use (advanced management module only), and generate and manage the SSH server key.

You can also enable or disable data encryption for sensitive data, such as passwords and keys. When enabled, the only way to disable data encryption is by restoring the AMM to its factory default configuration. If data encryption is

enabled, loading an AMM firmware update that does not support data encryption causes all configuration settings to revert to their factory default configuration. Figure 5-83 shows the Management Module Security window.

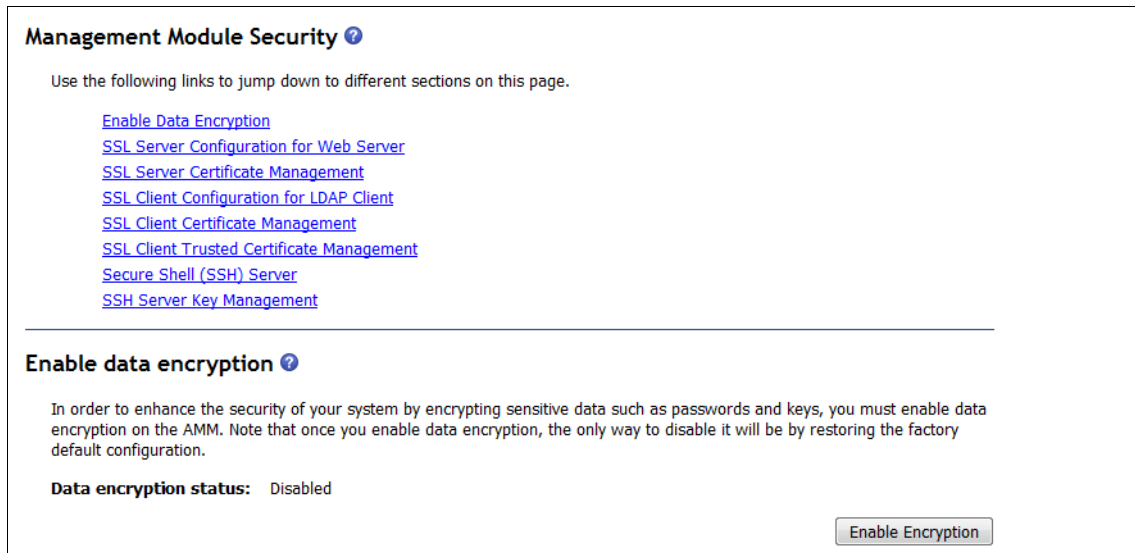


Figure 5-83 Management Module Security window

For more information about the use of various security methods available within the AMM, see the online help or the *IBM BladeCenter Advanced Management Module User's Guide* at:

<http://ibm.com/support/entry/portal/docdisplay?lnodocid=MIGR-5073887>

5.7.14 File management

Use this page to view or delete files in the AMM local storage file system. Only one directory level is displayed at a time. Click the directory name to navigate down to that directory level. Click **Up one Level** to return to the previous directory. Files can be deleted at any level in the directory tree. Select the file name, then click **Delete Selected Files**. A user must have Supervisor or Chassis Administrator access to delete a file.

Figure 5-84 shows the File Management window.

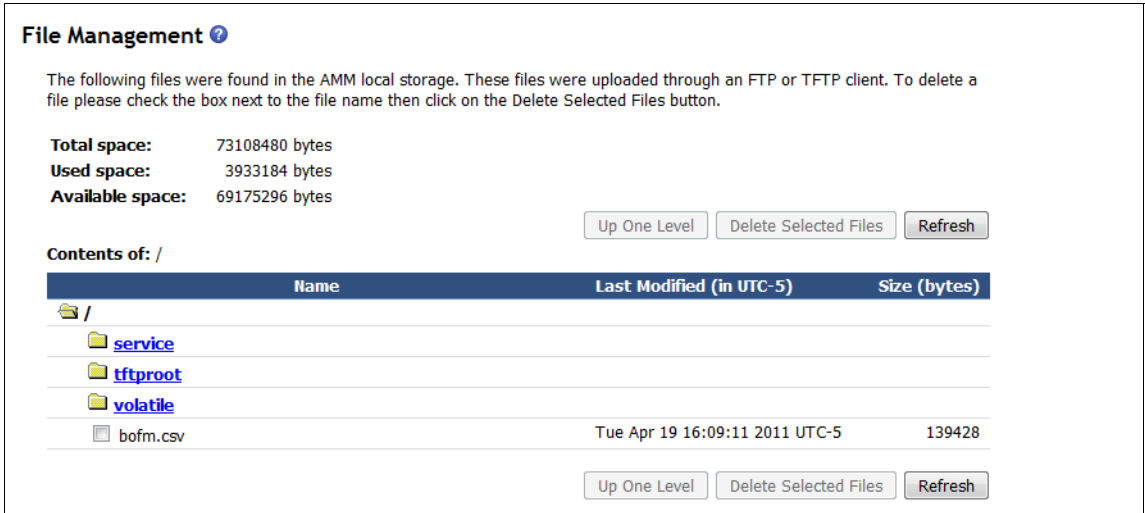


Figure 5-84 File Management window

The total, used, and available space in the file system is shown at the top of the file table. You can store files on the AMM for future use. For example, you can store firmware updates for the storage or network modules and use the AMM as a TFTP server for updating. For more information, see 5.7.15, “Update AMM firmware” on page 418.

5.7.15 Update AMM firmware

Use this window, which is shown in Figure 5-85, to update the firmware of the AMM.

Update MM Firmware ?

To update firmware on the MM, select the firmware file and click "Update". The new firmware will require a reboot of the MM to become active. So, if you want the new firmware to become active immediately, click the "Update & Reboot" button.

To update firmware on the MM, and then automatically reboot the MM, select the firmware file and click "Update & Reboot". This option will also bypass all dialogs until the update completes.

If there is a standby MM installed, the firmware on the standby MM will be automatically updated to the same level.

Please do not navigate away from this page for any reason until the flash is complete. Doing so may interfere with the completion of the flash and/or the automatic reboot.

Firmware file

☐ Remote file

Browse...

Update **Update & Reboot**

Figure 5-85 Update MM Firmware window

To update the AMM firmware, complete these steps:

1. Download the firmware from the IBM Support site.
2. Click **Browse**. Find the firmware file in your computer's file system. It has a PKT extension.
3. To begin the transfer process, click **Update**.
4. After the transfer is complete, you are asked to verify the firmware update. Click **Continue** or **Cancel**.
5. Remain on this window until the process is complete, at which point a status window is displayed to indicate whether the update was successful.
6. Restart the AMM so that the new firmware takes effect.

To update the AMM firmware from the CLI, see the section about the **update** command in 5.4.3, "Updating blade firmware" on page 362.

5.7.16 Configuration management

This window allows the user to back up and restore the management module configuration, and restore the factory default configuration:

- ▶ "Restoring defaults" on page 419
- ▶ "Backing up the configuration to file" on page 420

- ▶ “Restoring the configuration from file” on page 421
- ▶ “Saving the configuration to chassis” on page 423
- ▶ “Restoring the configuration from the chassis” on page 423
- ▶ “Starting the Configuration Wizard” on page 425

Restoring defaults

The Restore Defaults pane, which is shown in Figure 5-86, allows you to set all configuration settings to the factory defaults.



Figure 5-86 Restore Defaults configuration pane

There are two restore options available:

- ▶ **Restore Defaults:** This action causes all configuration settings to be set to factory defaults. If the AMM external network interface is configured with a static IP address, you must reconfigure it to restore connectivity. Clearing the configuration is followed by a restart of the AMM. A user must have Supervisor or both Chassis administration and Chassis configuration permissions to run this restore operation.
- ▶ **Restore Defaults Preserve Logs:** This action causes all configuration settings to be set to factory defaults. The logs are preserved with this action. If the AMM external network interface is configured with a static IP address, you must reconfigure it to restore connectivity. Clearing the configuration is followed by a restart of the AMM. Again, a user must have Supervisor or both Chassis administration and Chassis configuration permissions to run this restore operation.

Backing up the configuration to file

Use the Backup Configuration to File pane, which is shown in Figure 5-87, to download a copy of your current AMM configuration to the system on which this web interface is running. This action creates a backup of your current AMM configuration. This backup can be used to restore your AMM subsystem if the configuration is accidentally changed or corrupted. It also can be used as a base image that you can modify to configure multiple MMs with similar configurations. Any of the chassis access roles allows a user to run this operation.

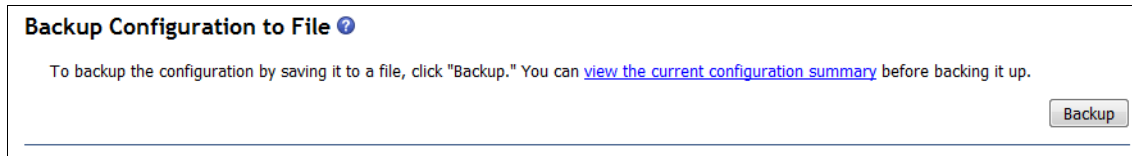


Figure 5-87 Backup Configuration window

To back up your current configuration, complete the following steps:

1. Click **View the current configuration summary** in the Backup MM Configuration pane. Figure 5-88 shows the configuration summary page.

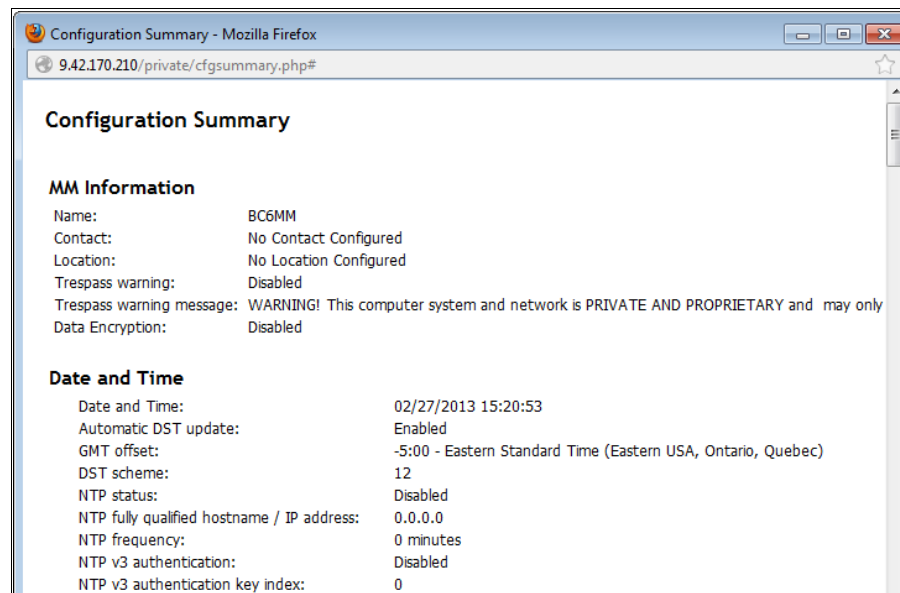


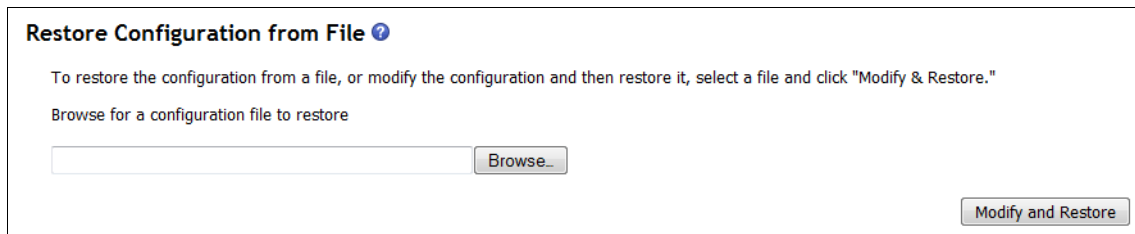
Figure 5-88 Configuration Summary window

2. Verify that the displayed settings are the ones that you want to save and then click **Close**.

3. To back up this configuration, click **Backup**.
4. Click **Save this file to disk** and click **OK**.
5. Enter the file name you want and choose the location where the file must be saved, then click **Save**.

Restoring the configuration from file

Use the Restore Configuration from File pane, which is shown in Figure 5-89, to restore a saved configuration from a file. You can restore the saved configuration in full, or you can modify key fields in the saved configuration before you restore them to your AMM.



Restore Configuration from File ?

To restore the configuration from a file, or modify the configuration and then restore it, select a file and click "Modify & Restore."

Browse for a configuration file to restore

Browse...

Modify and Restore

Figure 5-89 Restore Configuration from File pane

Modifying the configuration before restoring it is helpful when you are setting up multiple AMMs with similar configurations. This process allows you to quickly specify parameters that require unique values, such as names and IP addresses without having to reenter common, shared information. A user must have Supervisor access to run this restore operation.

To restore a saved configuration without modification, complete the following steps:

1. Click **Browse**. Click the configuration file and then click **Open**. The file (including the full path) is displayed in the box beside the **Browse** button.
2. Click **Restore**. A configuration summary window is displayed. Verify that this is the configuration that you want to restore. If it is not, click **Cancel**. To proceed with restoring this file to the AMM, click **Restore Configuration**.
3. After you receive a confirmation that the restore process is complete, go to the **Restart MM** window and click **Restart**.
4. Click **OK** in the window that is displayed to confirm that you want to restart your AMM.
5. Click **OK** in the window that is displayed to close the current browser window.
6. To log in to the AMM again, open your browser to the location of your AMM and follow your regular login process.

To modify and then restore a saved configuration, complete the following steps:

1. Click **Browse**. Click the configuration file and then click **Open**. The file (including the full path) is displayed in the box beside the **Browse** button.
2. Click **Modify and Restore**. This opens an editable configuration summary window. Initially, only the fields that allow changes are shown. Figure 5-90 shows an example configuration. To change between this view and the complete configuration summary view, click **Toggle View** at the top or bottom of the window.

Restore Configuration

MM Information

Name: BC6MM

Contact: No Contact Configured

Location: No Location Configured

~~~~~ Section(s) Hidden ~~~~~

External Network Interface

Interface: Enabled

Hostname: BC6MM

Domain Name:

AMM IPv4 Configuration

DHCP: Disabled - Use static IP configuration

Static IPv4 Configuration

IP address: 9.42.170.210

Subnet mask: 255.255.254.0

Gateway address: 9.42.170.1

AMM IPv6 Configuration

IPv6 Support: Disabled

IPv6 Static Address Assignment: Disabled

DHCPv6: Enabled

Stateless Auto-configuration: Enabled

Static IPv6 Configuration

IPv6 Static Address: 0000:0000:0000:0000:0000:0000:0000:0000

Prefix Length: 0

Default Route: 0000:0000:0000:0000:0000:0000:0000:0000

Data rate: Auto

Figure 5-90 Restore Configuration window

3. To modify the contents of any field, click in the corresponding text box and enter the wanted data.
4. Verify that the displayed configuration is what you want to restore.
5. Click **Restore Configuration**. A progress indicator is displayed as the firmware on the AMM flashes. Remain on this window until the transfer is

complete. A confirmation window is displayed to verify whether the update was successful.

6. After you receive a confirmation that the restore process is complete, go to the **Restart MM** window and click **Restart**.
7. Click **OK** in the window that is displayed to confirm that you want to restart your AMM.
8. Click **OK** in the window that is displayed to close the current browser window.
9. To log in to the AMM again, open your browser to the location of your AMM and follow your regular login process.

**Note:** An alert window might appear if the configuration file that you are attempting to restore was created by a different type of AMM or was created by the same type of AMM with older firmware (and thus fewer capabilities). This alert message includes a list of AMM capabilities that need to be manually configured after the restoration is complete. Some capabilities require configurations on more than one window.

## Saving the configuration to chassis

The Save Configuration to Chassis pane is shown in Figure 5-91. This action causes the configuration settings to be copied from the AMM to the midplane of the chassis. A user must have Supervisor access to run this backup operation. Click **Save** to commit the change.

### Save Configuration to Chassis ?

This action will cause the configuration settings to be saved from AMM to the BladeCenter chassis.  
To save the configuration settings to the BladeCenter chassis with default format, click "Save".

Save

---

### Restore Configuration from the Chassis ?

☒ Automatically copy configuration from the chassis to the AMM if it is inserted into a new chassis.

This action will cause the configuration settings to be restored to the AMM from the BC6MM chassis.  
To restore the configuration from the chassis, click "Restore".

Restore

Figure 5-91 Save/Restore configuration

## Restoring the configuration from the chassis

The AMM automatically reads configuration settings from the midplane every time that the AMM is inserted into a new chassis. Click to clear the check box in Figure 5-91 to disable this behavior on the Restore Configuration from the

Chassis pane. Click **Restore** to force the configuration settings to be copied from the midplane of the chassis to the AMM. After this operation, a restart of the AMM is required for the new settings to take effect.

Use the **write** and **read** commands to save and load configuration files from the command-line interface.

The syntax of the **write** command is as follows:

```
write -config {-i {-l} {-p}}
```

where:

|         |                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------|
| -config | Save destination (chassis, file)                                                                             |
| -i      | IP address of TFTP server to save the config file to                                                         |
| -l      | Optional file name to save the config file as (default is asm.cfg)                                           |
| -p      | Quote-delimited passphrase, required when encryption is enabled and saving to a file (maximum of 1600 chars) |

The syntax of the **read** command is as follows:

```
read -config {-i|-l|-p}|{-auto}
```

where:

|         |                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------|
| -config | Where to read the configuration from (chassis, file)                                                              |
| -auto   | Automatically read the configuration from the chassis every time the AMM is put into a new chassis (on, off)      |
| -i      | IP address of the TFTP server                                                                                     |
| -l      | File name of the configuration file                                                                               |
| -p      | Quote-delimited passphrase, required when encryption is enabled in the configuration file (maximum of 1600 chars) |

Figure 5-92 shows writing the configuration file to the chassis and then to a TFTP server, and reading it back to the AMM.

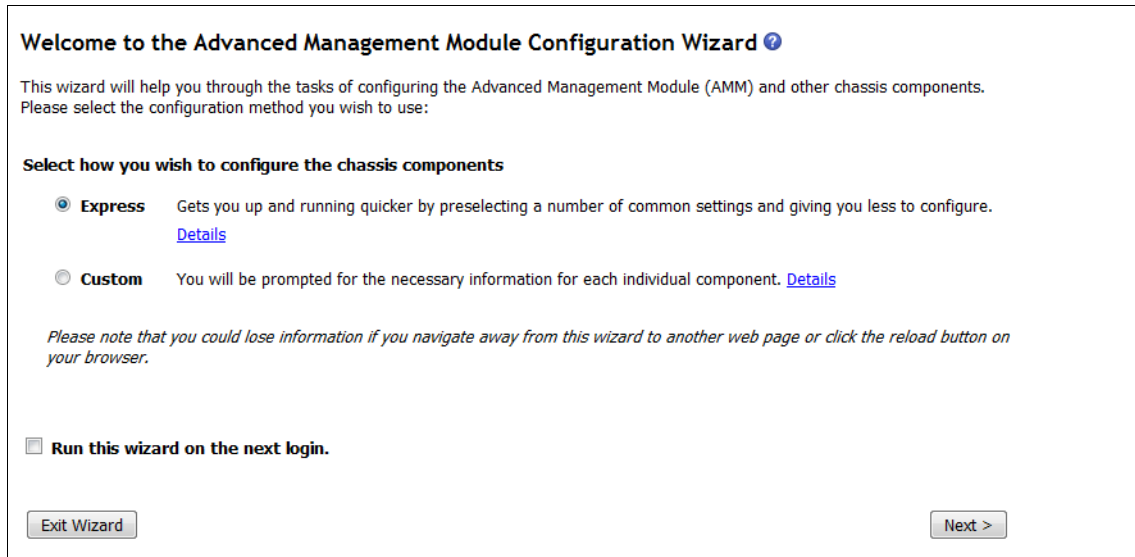
```
system> write -config chassis -T mm[1]
OK
Configuration settings were successfully saved to the chassis
system> write -config file 9.42.171.25 -T mm[1]
OK
system> read -config file -i 9.42.171.25 -l asm.cfg -T mm[1]
OK
```

*Figure 5-92 The write and read commands*

## Starting the Configuration Wizard

The Start Configuration Wizard pane (Figure 5-93) can be run at any time, and is used to get your BladeCenter up and running quickly. It allows you to configure the most important settings in the shortest amount of time.

For more information about using this wizard, see Chapter 3, “Getting started using the BladeCenter S chassis” on page 99.



**Welcome to the Advanced Management Module Configuration Wizard** ?

This wizard will help you through the tasks of configuring the Advanced Management Module (AMM) and other chassis components. Please select the configuration method you wish to use:

**Select how you wish to configure the chassis components**

☒ **Express** Gets you up and running quicker by preselecting a number of common settings and giving you less to configure. [Details](#)

☐ **Custom** You will be prompted for the necessary information for each individual component. [Details](#)

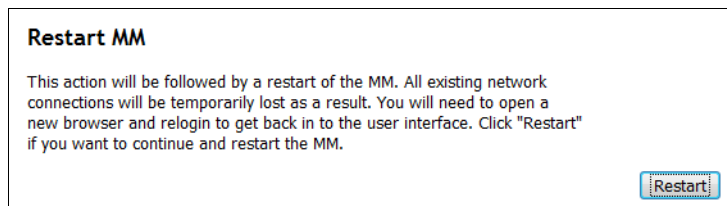
*Please note that you could lose information if you navigate away from this wizard to another web page or click the reload button on your browser.*

☐ **Run this wizard on the next login.**

Figure 5-93 Advanced Management Module Configuration Wizard

### 5.7.17 Restart AMM

You can use the Restart MM pane (Figure 5-94) to restart the AMM when required for necessary changes or if you are experiencing problems with the AMM. All network connections to the AMM are lost when the AMM restarts. Click **Restart** to begin the process.



**Restart MM**

This action will be followed by a restart of the MM. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. Click "Restart" if you want to continue and restart the MM.

Figure 5-94 AMM Restart window

The **reset** command restarts the AMM from the command line. For more information, see 5.4.1, “Blade Power/Restart” on page 349.

## 5.7.18 License Manager

Figure 5-95 shows the License Manager window, which can be used to manage license information for either a single chassis or any number of chassis within a data center.

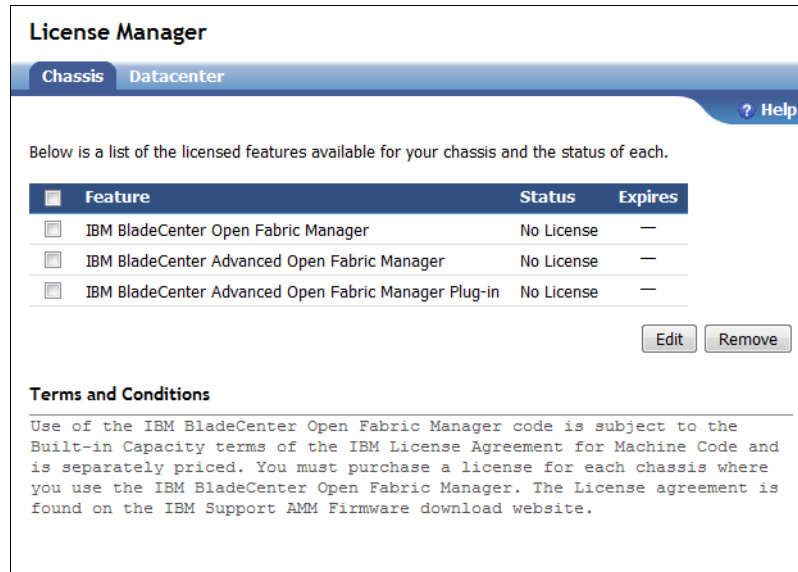


Figure 5-95 License Manager window

Features, such as Open Fabric Manager, can be used on your chassis after you install a valid License Key for the feature. A License Key is a seven character lowercase alphanumeric string that is unique for the combination of feature, chassis, and license type. For more information about how to obtain License Keys for features that you purchased, see:

<https://licensing.datacentertech.net>

## 5.8 Service tools

The following service tools are available:

- ▶ 5.8.1, “AMM Service Data” on page 427
- ▶ 5.8.2, “Blade Service Data” on page 429



- ▶ 5.8.3, “AMM Status” on page 431
- ▶ 5.8.4, “Service Advisor” on page 433

## 5.8.1 AMM Service Data

The AMM Service Data tool is used by the help desk to diagnose issues. To save this data to your local computer, complete these steps:

1. Click **Save AMM Service Data**.
2. Click **Save** when prompted for a location to save the file.
3. Select a location to save the file and click **Save** again.

A sample of AMM service data is shown in Figure 5-96.

### AMM Service Data ?

The support team will use the AMM service data provided by this page.

Save AMM Service Data

---

You can [send service information using e-mail](#) to report possible problems. Service information, which will include the contents of the service.txt file, will be sent in the e-mail as an attachment.

Service.txt

```

Time: 02/27/2013 15:25:00
UUID: A5EC 61FE C777 11DC 8DE9 924D 6B61 CA9E
MAC Address 00:14:5E:E1:60:50

MM Information
  Name: BC6MM
  Contact: No Contact Configured
  Location: No Location Configured
  IP address: 9.42.170.210

Date Time Information
  GMT offset: -5:00 - Eastern Standard Time (Eastern USA, Ontario, Quebec)
  Adjust for DST: Yes
  NTP: Disabled
  NTP Hostname/IP: N/A

System Health: Good

CHASSIS (BladeCenter-S) in Chassis slot: 01
TopoPath is "/CHASSIS[1]".
  Description      : BladeCenter-S
  Name             : modular01
  Width           : 1
  Sub Type        : BladeCenter Extreme (BCS)

```

Figure 5-96 AMM Service Data window

The **displaysd** command generates the AMM Service Data from the command line:

```
displaysd {-mmstat} | {-save|-i}
```

where:

|         |                                               |
|---------|-----------------------------------------------|
| -mmstat | Displays connectivity status and BIST results |
| -save   | Saves the service data to the specified file. |

**Note:** Save data with an extension of .tgz to allow support personnel to identify the file.

-i                      IP address of TFTP server to save the service data file to

The example shown in Figure 5-97 generates the AMM Service Data and saves it as a file named sdc.tgz. It is then uploaded to the TFTP server 9.67.22.176.

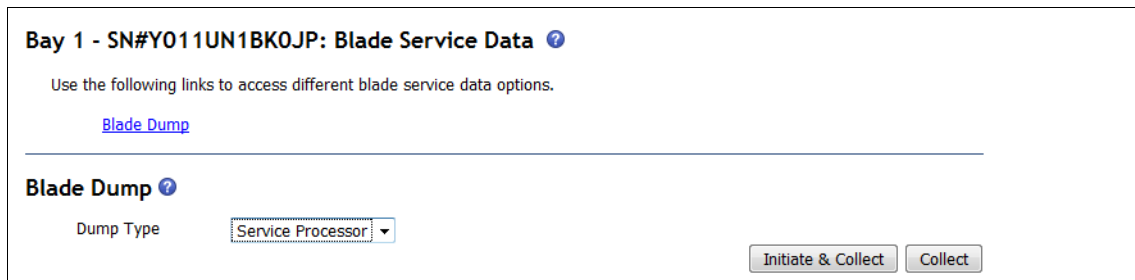
```
system> displaysd -T system:mm[1]
SPAPP Capture Available
Time: 10/04/2005 21:47:43
UUID: Not Available
*
*
*
system> displaysd -T system:mm[1] -save sdc.tgz -i 9.67.22.176
OK
system>
```

*Figure 5-97 The displaysd command*

## 5.8.2 Blade Service Data

This section allows the user to manage various blade memory dumps, and to view blade system reference codes (SRCs), if the blade supports these functions. Figure 5-98 shows an example for the HS22 blades.

Select the Dump type from the menu. Types include **Service Processor**, **Service Data**, **Platform**, and **Partition**. Not all types are supported by all blades. After you select the type of dump that you want to run, select **Initiate & Collect** or click **Collect**. If you choose the first option, the blade initiates a new memory dump and overwrites any existing one. **Collect** just copies the existing file to the /service directory on the AMM.



Bay 1 - SN#Y011UN1BK0JP: Blade Service Data ?

Use the following links to access different blade service data options.

[Blade Dump](#)

---

**Blade Dump** ?

Dump Type Service Processor ▼

Initiate & Collect Collect

Figure 5-98 Blade Service Data window

In addition, on supported blade types like the PS700, you can view SRC and boot codes from the blade as shown in Figure 5-99. See the individual product guides for assistance with these codes.

Bay 3 - AIXblade1: Blade Service Data ?

Use the following links to access different blade service data options.

[Blade Dump](#)  
[System Reference Codes](#)

Blade Dump ?

Dump Type

Service Processor ▾

Initiate

System Reference Codes ?

Follow the links in the System Reference Code column to obtain additional detailed data relating to the particular code.

| Unique ID | System Reference Code | Timestamp           |
|-----------|-----------------------|---------------------|
| 000000ff  | <a href="#">0c33</a>  | 2013-02-27 20:35:27 |
| 000000fe  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000fd  | <a href="#">2028</a>  | 2013-02-27 20:35:27 |
| 000000fc  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000fb  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000fa  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000f9  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000f8  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000f7  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000f6  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000f5  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000f4  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000f3  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000f2  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000f1  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |
| 000000f0  | <a href="#">0539</a>  | 2013-02-27 20:35:27 |
| 000000ef  | <a href="#">0538</a>  | 2013-02-27 20:35:27 |

Figure 5-99 Blade Service Data on Power Systems blade servers

### 5.8.3 AMM Status

The AMM Status pane, which is shown in Figure 5-100, displays basic information, such as name, serial number, and firmware version of the AMM.

AMM Status ?

The following MMs are present in the chassis.

| Property    | MM                                      |
|-------------|-----------------------------------------|
| Name        | BC6MM                                   |
| MAC Address | 00:14:5E:E1:60:50                       |
| UUID        | 489B 768D 1D79 11DD 84F8 0014 5EE1 6050 |
| Serial No.  | YK16808561S7                            |
| Build ID    | BPET54V                                 |

Use the following links to jump down to different sections on this page.


[MM Connectivity Status](#)  
[MM Built-in Self Test \(BIST\) Results](#)

Figure 5-100 AMM Status information

### AMM connectivity status

The MM Connectivity Status pane, which is shown in Figure 5-101, displays connectivity status between the MMs and various chassis components. The Last Update field shows when the status data was collected.

MM Connectivity Status ?

Status: 

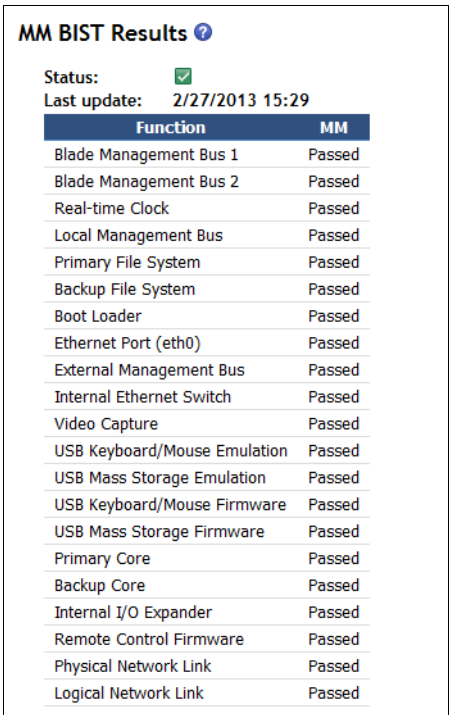
Last update: 2/27/2013 15:29

| Module                   | MM            |
|--------------------------|---------------|
| Blade 1                  | Communicating |
| Blade 2                  | Communicating |
| Blade 3                  | Communicating |
| Blade 4                  | Communicating |
| Blade 5                  | Communicating |
| Blade 6                  | Communicating |
| I/O Module 1             | Communicating |
| I/O Module 2             | Not Installed |
| I/O Module 3             | Communicating |
| I/O Module 4             | Communicating |
| Power Module 1           | Communicating |
| Power Module 2           | Communicating |
| Power Module 3           | Communicating |
| Power Module 4           | Communicating |
| Chassis Cooling Device 1 | Not Installed |
| Chassis Cooling Device 2 | Communicating |
| Chassis Cooling Device 3 | Not Installed |
| Chassis Cooling Device 4 | Communicating |
| Storage Module 1         | Communicating |
| Storage Module 2         | Communicating |

Figure 5-101 MM Connectivity Status pane

## AMM BIST results

The MM BIST Results pane, which is shown in Figure 5-102, displays built-in self test (BIST) results for the MMs.



The screenshot shows a window titled "MM BIST Results" with a status indicator (a green checkmark) and a last update timestamp of "2/27/2013 15:29". Below this is a table with two columns: "Function" and "MM". The table lists 20 functions, all of which have a "Passed" status in the "MM" column.

| Function                     | MM     |
|------------------------------|--------|
| Blade Management Bus 1       | Passed |
| Blade Management Bus 2       | Passed |
| Real-time Clock              | Passed |
| Local Management Bus         | Passed |
| Primary File System          | Passed |
| Backup File System           | Passed |
| Boot Loader                  | Passed |
| Ethernet Port (eth0)         | Passed |
| External Management Bus      | Passed |
| Internal Ethernet Switch     | Passed |
| Video Capture                | Passed |
| USB Keyboard/Mouse Emulation | Passed |
| USB Mass Storage Emulation   | Passed |
| USB Keyboard/Mouse Firmware  | Passed |
| USB Mass Storage Firmware    | Passed |
| Primary Core                 | Passed |
| Backup Core                  | Passed |
| Internal I/O Expander        | Passed |
| Remote Control Firmware      | Passed |
| Physical Network Link        | Passed |
| Logical Network Link         | Passed |

Figure 5-102 Displaying connectivity issues between the AMM and the components

### 5.8.4 Service Advisor

Service Advisor is built into your advanced management module and monitors for hardware problems 24 hours a day, 7 days a week.

If you are not using an approved service provider for your warranty support, you can send the event to IBM support by enabling and configuring Service Advisor. A ticket is opened for each service event that is received. For each ticket opened, an IBM support representative contacts the person who is specified on the contact panel. The response time depends on several factors, such as your level of support and call volume.

If you are using an approved service provider for hardware warranty support, you can configure Service Advisor and specify the FTP site that is provided by your service provider. Figure 5-103 shows an example of the Service Advisor page.

Service Advisor ?

Service Advisor resides on your Advanced Management Module (AMM) and monitors your BladeCenter chassis for hardware events. Upon detecting a hardware event Service Advisor captures the event, error logs, and service data and can automatically report the event to IBM support or (depending upon your service agreement) an approved service provider. To send the serviceable event to IBM support you must enable and configure Service Advisor. For each serviceable call home event IBM receives a service ticket will be opened and a follow-up call will be made. To send this data to your service provider (or your own internal support organization) you must specify an FTP site (FTP/TFTP Server of Service Data).

[View Terms and Conditions](#)

You can change Service Advisor status and view/change your settings .

Report to IBM Support: **Disabled**

Report to FTP/TFTP Server: **Disabled**

Your current settings for IBM Support are valid.

Service Advisor Activity Log

Service Advisor Settings

Help

Refresh

Display For

Both IBM Support and FTP/TFTP Server

| Corrected                |      | IBM Support  |     | FTP/TFTP Server | Event ID   | Event Severity | Event Source | Date/Time         | Message                             |
|--------------------------|------|--------------|-----|-----------------|------------|----------------|--------------|-------------------|-------------------------------------|
|                          | Send | Assigned Num |     |                 |            |                |              |                   |                                     |
| <input type="checkbox"/> | NO   | Failed       | N/A | Disabled        | 0x00016802 | Info           | CHASSIS      | 11/23/10 15:50:30 | Test Call Home generated by USERID. |
| <input type="checkbox"/> | NO   | Failed       | N/A | Disabled        | 0x00016802 | Info           | CHASSIS      | 11/23/10 15:34:44 | Test Call Home generated by USERID. |
| <input type="checkbox"/> | NO   | Failed       | N/A | Disabled        | 0x00016802 | Info           | CHASSIS      | 11/23/10 15:27:46 | Test Call Home generated by USERID. |
| <input type="checkbox"/> | NO   | Failed       | N/A | Disabled        | 0x00016802 | Info           | CHASSIS      | 11/23/10 15:27:00 | Test Call Home generated by USERID. |
| End of Log.              |      |              |     |                 |            |                |              |                   |                                     |

You can use the [Call Home Exclusion List](#) to specify specific call home events not to be reported.

Figure 5-103 Service Advisor

The Service Advisor Activity Log lists the five most recent events that were generated by Service Advisor and sent to IBM support or approved service provider. To prevent the same event from being sent repeatedly, Service Advisor provides a timeout interval of 120 hours (five days) before another event can be sent for the same failed component. However, you can reset the timeout interval by marking an event as corrected. After you mark an event as corrected, Service Advisor will send out a new serviceable event the next time a hardware server event is detected, even if it was previously reported.

Click **Service Advisor Settings** to enable or disable the Service Advisor.



# Abbreviations and acronyms

|               |                                     |             |                                                 |
|---------------|-------------------------------------|-------------|-------------------------------------------------|
| <b>AAS</b>    | Advanced Administrative System      | <b>DVS</b>  | Digital Video Surveillance                      |
| <b>AC</b>     | alternating current                 | <b>ECC</b>  | error correction code                           |
| <b>AMD</b>    | Advanced Micro Devices              | <b>EDA</b>  | Electronic Design Automation                    |
| <b>AMM</b>    | advanced management module          | <b>ETSI</b> | European Telecommunications Standards Institute |
| <b>BBD</b>    | Blade Bay Data                      | <b>FC</b>   | Fibre Channel                                   |
| <b>BBU</b>    | battery-backup-unit                 | <b>FTP</b>  | file transfer protocol                          |
| <b>BC</b>     | BladeCenter                         | <b>GB</b>   | gigabyte                                        |
| <b>BC-S</b>   | BladeCenter-S                       | <b>GMT</b>  | Greenwich Mean Time                             |
| <b>BIOS</b>   | basic input/output system           | <b>HA</b>   | high availability                               |
| <b>BIST</b>   | built-in self test                  | <b>HBA</b>  | host bus adapter                                |
| <b>BMC</b>    | baseboard management controller     | <b>HDD</b>  | hard disk drive                                 |
| <b>BSMP</b>   | Blade System Management Processor   | <b>HH</b>   | half-high                                       |
| <b>CA</b>     | certificate authority               | <b>HMC</b>  | Hardware Management Console                     |
| <b>CD</b>     | compact disk                        | <b>HPC</b>  | high-performance computing                      |
| <b>CD-ROM</b> | compact disc read-only memory       | <b>HT</b>   | Hyper-Threading                                 |
| <b>CLI</b>    | command-line interface              | <b>I/O</b>  | input/output                                    |
| <b>CLP</b>    | Command Line Protocol               | <b>IBM</b>  | International Business Machines Corporation     |
| <b>CPU</b>    | central processing unit             | <b>ID</b>   | identifier                                      |
| <b>DC</b>     | domain controller                   | <b>IM</b>   | Integrated Mirroring                            |
| <b>DCOM</b>   | distributed component object model  | <b>IME</b>  | Integrated Mirroring Enhanced                   |
| <b>DHCP</b>   | Dynamic Host Configuration Protocol | <b>IP</b>   | Internet Protocol                               |
| <b>DIMM</b>   | dual inline memory module           | <b>IPTV</b> | Internet Protocol Television                    |
| <b>DLT</b>    | Digital Linear Tape                 | <b>ISO</b>  | International Organization for Standardization  |
| <b>DNS</b>    | Domain Name System                  | <b>IT</b>   | information technology                          |
| <b>DRS</b>    | Distributed Resource Scheduler      | <b>ITSO</b> | International Technical Support Organization    |
| <b>DSM</b>    | disk storage module                 | <b>JRE</b>  | Java Runtime Environment                        |
|               |                                     | <b>KB</b>   | kilobyte                                        |

|             |                                            |               |                                                     |
|-------------|--------------------------------------------|---------------|-----------------------------------------------------|
| <b>KVM</b>  | keyboard, video, mouse                     | <b>RMU</b>    | Remote Management Unit                              |
| <b>LAA</b>  | locally administered address               | <b>SAN</b>    | storage area network                                |
| <b>LAN</b>  | local area network                         | <b>SAS</b>    | serial-attached SCSI                                |
| <b>LDAP</b> | Lightweight Directory Access Protocol      | <b>SATA</b>   | Serial Advanced Technology Attachment               |
| <b>LED</b>  | light-emitting diode                       | <b>SCM</b>    | supply chain management                             |
| <b>LTO</b>  | Linear Tape-Open                           | <b>SCSI</b>   | Small Computer System Interface                     |
| <b>LVD</b>  | Low Voltage Differential                   | <b>SDK</b>    | software development kit                            |
| <b>MAC</b>  | Media Access Control                       | <b>SDRAM</b>  | synchronous dynamic random access memory            |
| <b>MB</b>   | megabyte                                   | <b>SES</b>    | SCSI Enclosure Services                             |
| <b>MIB</b>  | Management Information Base                | <b>SFF</b>    | small form factor                                   |
| <b>MIO</b>  | Memory and I/O                             | <b>SIMD</b>   | single-instruction multiple-data                    |
| <b>MPE</b>  | Multiprocessor Expansion                   | <b>SIO</b>    | Storage and I/O                                     |
| <b>NAS</b>  | network-attached storage                   | <b>SLES</b>   | SUSE Linux Enterprise Server                        |
| <b>NEBS</b> | Network Equipment Building System          | <b>SLP</b>    | Service Location Protocol                           |
| <b>NGN</b>  | next-generation network                    | <b>SMASH</b>  | Systems Management Architecture for Server Hardware |
| <b>NOS</b>  | network operating system                   | <b>SMBIOS</b> | system management BIOS                              |
| <b>NTP</b>  | Network Time Protocol                      | <b>SMP</b>    | symmetric multiprocessing                           |
| <b>OCP</b>  | Operator Control Panel                     | <b>SMTP</b>   | Simple Mail Transfer Protocol                       |
| <b>OEM</b>  | original equipment manufacturer            | <b>SNMP</b>   | Simple Network Management Protocol                  |
| <b>OPM</b>  | Optical Pass-thru Module                   | <b>SOL</b>    | Serial over LAN                                     |
| <b>OS</b>   | operating system                           | <b>SSH</b>    | Secure Shell                                        |
| <b>PC</b>   | personal computer                          | <b>SSL</b>    | Secure Sockets Layer                                |
| <b>PCI</b>  | Peripheral Component Interconnect          | <b>SSP</b>    | Serial SCSI Protocol                                |
| <b>PKT</b>  | packet                                     | <b>TB</b>     | terabyte                                            |
| <b>POST</b> | power-on self-test                         | <b>TCP</b>    | Transmission Control Protocol                       |
| <b>PXE</b>  | Preboot Execution Environment              | <b>TCP/IP</b> | Transmission Control Protocol/Internet Protocol     |
| <b>RAID</b> | redundant array of independent disks       | <b>TFTP</b>   | Trivial File Transfer Protocol                      |
| <b>RAS</b>  | remote access services; row address strobe | <b>TOE</b>    | TCP offload engine                                  |
| <b>RDM</b>  | Remote Deployment Manager                  | <b>UI</b>     | user interface                                      |
| <b>RHEL</b> | Red Hat Enterprise Linux                   |               |                                                     |

|            |                              |
|------------|------------------------------|
| <b>UPS</b> | uninterruptible power supply |
| <b>URL</b> | Uniform Resource Locator     |
| <b>USB</b> | Universal Serial Bus         |
| <b>VAC</b> | volts alternating current    |
| <b>VLP</b> | very low profile             |
| <b>VNC</b> | Virtual Network Computing    |
| <b>VPD</b> | vital product data           |
| <b>XDR</b> | extreme data rate            |
| <b>XM</b>  | extended memory              |



# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

## IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 441. Note that some of the documents referenced here might be available in softcopy only.

Related publications from IBM Redbooks:

- ▶ *IBM BladeCenter Interoperability Guide*, REDP-BCIG
- ▶ *IBM BladeCenter Products and Technology*, SG24-7523
- ▶ *IBM BladeCenter S*, TIPS0977
- ▶ *xREF: IBM x86 Server Reference*, REDP-XREF

## Other publications

These publications are also relevant as further information sources. They are available from this website:

- ▶ BladeCenter Information Center  
<http://publib.boulder.ibm.com/infocenter/bladectr/documentation/>
- ▶ Installation and User's Guide - IBM BladeCenter S  
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5073635>
- ▶ Office Enablement Kit Installation and User's Guide  
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5073634>
- ▶ Planning Guide - IBM BladeCenter S  
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5073632>
- ▶ Problem Determination and Service Guide  
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5076785>

These other publications are available from the BladeCenter support site:

<http://www.ibm.com/systems/bladecenter/support/>

- ▶ *IBM BladeCenter Advanced Management Module User's Guide*
- ▶ *IBM BladeCenter Advanced Management Module for BladeCenter and BladeCenter H Installation Guide*
- ▶ *IBM Management Module Command Line Interface Reference Guide*
- ▶ *IBM BladeCenter S 6 Disk Storage Module*
- ▶ *IBM BladeCenter S Power Supply Modules*
- ▶ *IBM BladeCenter S Serial Pass-Thru Module*
- ▶ *IBM BladeCenter SAS Connectivity Module Installation and User's Guide*
- ▶ *IBM BladeCenter SAS Expansion Card Installation and User's Guide*

## Online resources

These websites are also relevant as further information sources:

- ▶ BladeCenter Power Configurator  
<http://www.ibm.com/systems/bladecenter/powerconfig/>
- ▶ IBM BladeCenter forum hosted on IBM developerWorks  
[http://www.ibm.com/developerworks/forums/dw\\_forum.jsp?forum=819&cat=53](http://www.ibm.com/developerworks/forums/dw_forum.jsp?forum=819&cat=53)
- ▶ IBM BladeCenter home page  
<http://www.ibm.com/bladecenter>
- ▶ IBM Director downloads  
<http://www.ibm.com/systems/management/director/downloads.html>
- ▶ ServerProven  
<http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html>

## How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this website:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)







# Implementing the IBM BladeCenter S Chassis

(0.5" spine)  
0.475" <-> 0.875"  
250 <-> 459 pages







# Implementing the IBM BladeCenter S Chassis



**Describes the features and components of the BladeCenter S chassis**

**Guides you through the quick start wizards**

**Explains how to configure the integrated storage**

IBM BladeCenter remains an innovative solution to running business solutions. IBM BladeCenter builds on the IBM commitment to integrating server, storage, and networking functionality with technology exchange and heterogeneous management. IBM BladeCenter offers the ease, density, availability, affordability, and scalability that are central to the blade technology promise.

IBM BladeCenter S combines the power of blade servers with integrated storage. It can hold up to six blade servers and up to 12 shared hot-swap 3.5-inch disk drives in just 7U of rack space.

BladeCenter S is the ideal solution for a branch office or distributed environment where servers, switches, and shared storage are all in one unit, or in environments where only 110V power is available.

This IBM Redbooks publication was written for a technical audience with limited or no experience with IBM BladeCenter solutions. After reading it, you should be able to successfully implement the BladeCenter S, customized to your specific needs.

## **INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

### **BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)