

# Hardware Management **Console V7 Handbook**



ibm.com/redbooks



International Technical Support Organization

# Hardware Management Console V7 Handbook

October 2007

**Note:** Before using this information and the product it supports, read the information in "Notices" on page xi.

#### First Edition (October 2007)

This edition applies to Version 7, Release 3, Modification 10 of Hardware Management Console (product number 5639-N47).

**Note:** This book is based on a pre-GA version of a product and might not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-on versions of this book for more current information.

© Copyright International Business Machines Corporation 2007. 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	ci ii
Preface	ii
The team that wrote this bookxi	v
Become a published author	v
Comments welcome x	v
Chapter 1 HMC overview	1
1.1 HMC concepts	2
1 1 1 User interface	2 2
1 1 2 User tasks and roles	3
1.2 HMC type	4
1.2.1 Deskton HMC	5
1.2.2 Back mounted HMC	5
1.2.3 HMC version matrix to support POWER servers	5
1.3 HMC connectivity	7
1.3.1 Local HMC	R
1.3.2 Redundant HMC	a
1 4 Enhancements in HMC Version 7	9
1.4.1 Web browser based user interface	9
1.4.2 System Planning Tool	0
1 4 3 Customizable Data Replication	D.
1 4 4 Custom groups	n.
1 4 5 New System Beference Code look-up	n.
1 4 6 Processor compatibility	1
1.4.7 Host Ethernet Adapter.	2
1.4.8 Donating dedicated LPARs.	3
1.4.9 Processor recovery and partition availability priority	3
1.4.10 Barrier Synchronization Register	3
1.4.11 Capacity on Demand enhancement	4
	-
Chapter 2. Basic operation	7
2.1 Using the Web browser based user interface	B
2.1.1 Starting the HMC 18	В
2.1.2 Session preservation1	9
2.1.3 Components of the Web browser based user interface	1
2.2 Systems Management - Servers	2
2.2.1 Servers	3

2.2.2 Properties	27
2.2.3 Operations.	27
2.2.4 Configuration	31
2.2.5 Connection	34
2.2.6 Hardware (Information)	36
2.2.7 Updates	38
2.2.8 Serviceability	39
2.2.9 Capacity on Demand.	39
2.3 System Managements - Partitions	39
2.3.1 Operations	39
2.3.2 Configuration	42
2.3.3 Dynamic Logical Partitioning.	44
2.4 Systems Management - Frames	45
2.4.1 Properties	46
2.4.2 Operations	46
2.4.3 Configuration	47
2.4.4 Connections	48
2.4.5 Hardware (Information)	49
2.4.6 Serviceability	49
2.5 HMC Management	50
2.5.1 View HMC Events	51
2.5.2 Shut Down or Restart	52
2.5.3 Schedule Operations.	52
2.5.4 Format Media	53
2.5.5 Back up HMC Data	53
2.5.6 Restore HMC Data	54
2.5.7 Save Upgrade Data	54
2.5.8 Change Network Settings	54
2.5.9 Test Network Connectivity	55
2.5.10 View Network Topology	55
2.5.11 Tip of the Day	57
2.5.12 View License	57
2.5.13 Change User Interface Settings	58
2.5.14 Change Date and Time	59
2.5.15 Launch Guided Setup Wizard	59
2.5.16 Locking the HMC screen	59
2.5.17 Opening a 5250 console	60
2.5.18 Open Restricted Shell Terminal	60
2.5.19 Launch Remote HMC	60
2.5.20 Change User Password	61
2.5.21 Manage User Profiles and Access	61
2.5.22 Manage Task and Resource roles	61
2.5.23 Manage Users and Tasks	61
5	

2.5.24 Manage Certificates 61
2.5.25 Remote Command Execution
2.5.26 Remote Virtual Terminal 62
2.5.27 Remote Operation 62
2.5.28 Change Language and Locale62
2.5.29 Create Welcome Text
2.5.30 Manage Data Replication 63
Chapter 3. Installing the HMC
3.1 Cabling the HMC
3.2 Configuring the HMC using the HMC Guided Setup wizard79
3.2.1 The HMC Guided Setup wizard checklist
3.2.2 Using the HMC Guided Setup wizard
3.3 Connecting managed systems to the HMC130
Chapter 4. System plans and the HMC
4.1 System plans
4.2 Using the HMC graphical user interface
4.2.1 Importing a system plan to the HMC
4.2.2 Exporting a system plan from the HMC
4.2.3 Creating a system plan on the HMC
4.2.4 Viewing a system plan on the HMC
4.2.5 Removing system plan on the HMC
4.3 System plans deployment
4.3.1 Deployment validation process
4.3.2 Deploy a system plan using the graphical wizard
4.3.3 System plans management using restricted shell (CLI)
Chapter 5. HMC security and user management
5.1 Certificate management
5.1.1 Creating a new certificate
5.1.2 Modifying existing certificates
5.1.3 Advanced options for modifying existing certificates
5.2 HMC user management
5.2.1 Changing the user password
5.2.2 Managing user profiles and access.
5.2.3 Customizing user task roles and managed resource roles 190
Chapter 6. Network configuration and the HMC
6.1 Types of HMC network configurations
6.2 Configuring HMC network settings 196
6.2.1 HMC Identification
6.2.2 LAN Adapters
6.2.3 Name Services

6.2.4 Routing
6.3 Testing network connectivity 206
6.3.1 Ping
6.3.2 Interfaces
6.3.3 Address
6.3.4 Routes
6.3.5 ARP
6.3.6 Sockets
6.3.7 TCP
6.3.8 UDP
6.3.9 IP
6.4 Viewing network topology 216
Chapter 7. Partitioning
7.1 Partitioning concepts
7.1.1 Host Ethernet Adapter 221
7.1.2 Shared pool usage of dedicated capacity
7.1.3 Partition availability priority 225
7.2 Creating logical partitions
7.2.1 Creating an AIX or a Linux partition
7.3 Managing partition data
7.3.1 Restore
7.3.2 Initialize
7.3.3 Backup
7.3.4 Delete
Chapter 8. Dual HMC and redundancy
8.1 Redundant HMC configurations
8.2 Redundant remote HMC 256
8.3 Redundant HMC configuration considerations
Chapter 9. Virtual I/O
9.1 Understanding virtual I/O
9.1.1 POWER Hypervisor for virtual I/O
9.1.2 Virtual I/O Server
9.2 Virtual SCSI
9.2.1 Client/server communications
9.2.2 Adding a virtual SCSI server adapter
9.3 Virtual Ethernet
9.3.1 Virtual LAN overview
9.3.2 Virtual Ethernet connection
9.3.3 Adding virtual Ethernet

9.4 Shared Ethernet Adapter	267
Chapter 10. Command line interface.   10.1 CLI enhancements   10.1.1 Host Ethernet Adapter.   10.1.2 Partition Availability Priority.   10.1.3 Shared pool usage of dedicated   10.1.4 Partitioning support for barrier synchronization register   10.1.5 System planning   10.1.6 HMC dump commands   10.1.7 Partition processor compatibility modes   10.1.8 Utility Capacity on Demand   10.1.9 i5/OS only enhancements   10.1.10 Other changes in CLI that are not related to specific features   10.2 Most common command line options and usage	271 272 278 281 285 288 288 288 289 292 295 297 298
Chapter 11. Firmware maintenance.   11.1 Critical Console Data backup   11.1.1 Manual back up of Critical Console Data   11.1.2 Scheduled Critical Console Data backup   11.2 Restoring Critical Console Data   11.2.1 Restoring data from DVD   11.2.2 Restoring data that was archived to a remote FTP or NFS server   11.3 HMC firmware maintenance   11.3.1 How to determine the HMC software version   11.3.2 Which firmware or fix level is correct for your system   11.3.3 Obtaining HMC updates and recovery software   11.3.4 Obtaining and applying HMC code from an FTP server   11.3.5 Applying HMC code from CD or DVD   11.3.7 Upgrading the HMC machine code   11.3.7 Upgrading HMC from Version 6 to Version 7   11.4 Managed system firmware updates   11.4.1 Firmware overview   11.4.2 Obtaining system firmware	303 304 305 309 309 309 310 311 312 316 318 320 320 324 326 327 328
Chapter 12. Service Management 12.1 Service Management area of the HMC 12.2 Management tasks 12.2.1 Service events 12.2.2 Remote access 12.2.3 Managing HMC service data 12.3 Connectivity 12.3.1 Manage Systems Call-Home 12.3.2 Manage Outbound Connectivity	331 332 333 342 344 351 352 353

12.3.3 Manage Inbound Connectivity	. 359
12.3.4 Manage Customer Information	. 361
12.3.5 Manage eService Registration	. 363
12.3.6 Manage Serviceable Event Notification	. 368
12.3.7 Manage Connection Monitoring	. 370
12.3.8 Manage POWER4 Service Agent	. 371
Chapter 13. Capacity on Demand	. 373
13.1 Advantages of CoD	. 374
13.2 Permanent types of CoD	. 3/5
	. 375
13.2.2 Mobile CoD	. 3/5
12.2.1 Trial CoD	. 3// 070
12.2.2 Op/Off CoD	. 3/0 970
13.3.2 OI//OII COD	. 3/0 202
13.3.5 Reserve Capacity	202
13.3.4 Ounity CoD	200
13.4 CoD Web site pavigation	385
13.4 1 Acquiring activation codes	387
13.4.2 Bequesting trial activation	3007
13.5 Entering enablement and activation codes on the HMC	395
13.5.1 Entering an activation enablement or deactivation code	395
13.5.2 Activating and managing Utility CoD	396
13.5.3 Activating and managing Beserve CoD	402
13.5.4 Activating and managing On/Off CoD	406
13.5.5 Activating and managing Trial CoD	413
13.5.6 Advanced System Management CoD interface	. 419
Chapter 14. Advanced System Management Interface	. 423
14.1 Connecting to ASMI	. 424
14.1.1 Connection to ASMI using the HMC	. 424
14.1.2 Connecting to ASMI through a Web browser	. 425
14.1.3 Accessing the ASMI using an ASCII terminal	. 426
14.2 Log in to ASMI	. 426
14.2.1 ASMI login restrictions	. 428
14.3 Power and restart control	. 429
14.3.1 Power On/Off System	. 429
14.3.2 Auto Power Restart.	. 430
14.3.3 Immediate Power Off	. 431
14.3.4 System Reboot	. 431
14.4 System Service Aids	. 432
14.4.1 Error/Event Logs	. 433

14.4.2 System Dump	. 433
14.4.3 Service Processor Dump	. 435
14.4.4 Reset Service Processor.	. 436
14.4.5 Factory Configuration	. 436
14.5 System Information	. 438
14.5.1 Vital Product Data	. 438
14.5.2 Power Control Network Trace	. 439
14.5.3 Previous Boot Progress Indicator	. 439
14.5.4 Progress Indicator History	. 440
14.5.5 Real-time Progress Indicator	. 441
14.6 System Configuration	. 442
14.6.1 System Name	. 443
14.6.2 Configure I/O Enclosures	. 443
14.6.3 Time of Day	. 446
14.6.4 Firmware Update Policy	. 447
14.6.5 PCI Error Injection Policy	. 447
14.6.6 I/O Adapter Enlarged Capacity	. 447
14.6.7 Hardware Management Consoles	. 448
14.6.8 Virtual Ethernet Switches	. 448
14.6.9 Floating Point Unit Computation Test	. 449
14.6.10 Hardware Deconfiguration	. 450
14.6.11 Program Vital Product Data	. 456
14.7 Network Services	. 461
14.7.1 Network Configuration	. 462
14.7.2 Network Access	. 464
14.8 Performance Setup	. 465
14.8.1 System Memory Page Setup	. 466
14.9 On Demand Utilities	. 466
14.9.1 CoD Order Information	. 467
14.9.2 CoD Activation	. 469
14.9.3 CoD Recovery	. 469
14.9.4 CoD Command	. 469
14.9.5 Viewing Information about CoD Resources	. 470
14.10 Login Profile	. 470
14.10.1 Change Password	. 470
14.10.2 Retrieve Login Audits	. 471
14.10.3 Change Default Language	. 471
14.10.4 Update Installed Languages	. 472
14.10.5 User Access Policy	. 472

Appendix A. An example of backing up HMC Critical Console Data 475 Using the HMC option to back up Critical Console Data
Appendix B. Introduction to IBM Director.485Overview of IBM Director486IBM Director components.487IBM Director capabilities.488IBM Director Server Tasks488IBM Director Agent features489IBM Director extensions for System p.490
Appendix C. Moving existing System i LPAR profiles to HMC493Saving LPAR profiles using System i Navigator494Importing LPAR profiles to HMC499
Related publications505IBM Redbooks505Other publications505Online resources506How to get IBM Redbooks publications507Help from IBM507
Index

# **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 about 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

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

Redbooks (logo) 🤣 🛽	GPFS™
i5/OS®	HACMP™
z/VM®	IBM®
Asset ID™	POWER™
AIX 5L™	POWER Hypervisor™
AIX®	POWER4™
BladeCenter®	POWER5™
Electronic Service Agent <sup>™</sup>	POWER6™
General Parallel File System™	Redbooks®

ServeRAID<sup>™</sup> System i<sup>™</sup> System p<sup>™</sup> System p5<sup>™</sup> System x<sup>™</sup> System z<sup>™</sup> Tivoli® Virtualization Engine<sup>™</sup>

The following terms are trademarks of other companies:

InfiniBand, and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

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

# Preface

The IBM® Hardware Management Console (HMC) provides systems administrators a tool for planning, deploying, and managing IBM System p<sup>™</sup> and IBM System i<sup>™</sup> servers. This IBM Redbooks® publication is designed for system administrators to use as a desk-side reference when managing partition-capable System i and System p servers using the HMC.

The major functions that the HMC provides are server hardware management and virtualization (partition) management. You can find information about virtualization management in the following documents:

- Advanced POWER Virtualization on IBM System p5: Introduction and Configuration, SG24-7940
- Virtualization and Clustering Best Practices Using IBM System p Servers, SG24-7349
- Logical Partitions on System i5: A Guide to Planning and Configuring LPAR with HMC on System i, SG24-8000
- ► LPAR Simplification Tools Handbook, SG24-7231

In this book, we discuss how to:

- ► Configure the HMC
- Manage software levels on the HMC
- ► Use service functions on the HMC
- Update firmware of managed systems
- ► Move profiles from System i servers that previously did not connect to a HMC
- Use System Planning Tool deployments

In addition, we explain how to use the new HMC graphical user interface and the new HMC commands that are available with HMC Version 7, Release 3.

# The team that wrote this book

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

**Stephen Hochstetler** is an IT Specialist. He writes extensively and teaches IBM classes worldwide on all areas of Linux®, System p, and Tivoli®. Before joining the ITSO, Stephen worked in Tivoli Services as a network management specialist.

JunHeum Min is an SSR in IBM Korea. He has four years of experience in System p and support on AIX® systems. His areas of expertise include AIX Problem Determination, GPFS<sup>™</sup>, HACMP<sup>™</sup> and Virtualization on System p5<sup>™</sup>. JunHeum holds a degree in Computer Science and a Master's degree in Cryptography from the University of Sogang in Seoul, Korea.

**Matt Robbins** is a System p5 Technical Sales Specialist in Dallas, Texas. He has more than 10 years of experience working with System p5 and AIX. His areas of expertise include UNIX®, TCP/IP, and designing On Demand solutions for internet security and Web servers. Matt attended the University of North Texas as a student of computer science.

**Nancy Milliner** is an HMC Development Support Specialist in Austin, Texas. She has five years of experience in Linux Performance as well as several years of hands-on experience with HMC. Her areas of expertise include Linux networking and performance analysis. Nancy holds a degree in Computer Science from Texas Woman's University.

**Narend Chand** is a System Service Representative in New Zealand. He has 13 years experience working with system p5. His areas of expertise include supporting system p5 and i5, problem analysis, and account management. Narend graduated from Auckland University of Technology in Electronics and Computer Technology.

**Syamsul Hidayat** is a System i System Service Representative in Indonesia. He has two years of experience in the i5 field. His areas of expertise include i5 servers, HMC, and FSP. Syamsul holds a degree in Electrical Engineering from the University of Indonesia.

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

- Gary Anderson, IBM Austin
- Shamsundar Ashok IBM Austin
- Anton Blanchard, IBM Austin
- Mark Dewalt, IBM Austin
- Bob Foster, IBM Austin
- Chris James, IBM Austin
- ► Stephanie L Jensen, IBM Austin
- ► Taijung Kim, IBM Korea
- ► Bryan M Logan, IBM Rochester
- Mark Manges, IBM Rochester
- Minh Nguyen IBM Austin
- ► Brian Tolan, IBM Endicott
- ► Christine Wang, IBM Austin

# Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

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 in one of the following ways:

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

ibm.com/redbooks

► Send your comments in an e-mail 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

# 1

# **HMC** overview

The content of this book focuses on the Hardware Management Console (HMC), a member of the IBM Systems Director platform management family. IBM Systems Director provides IT professionals with the tools that they need to better coordinate and manage all of their virtual and physical resources in the data center.

The cost of managing the IT infrastructure has become the largest and fastest-growing component of overall IT spending for many organizations. Virtualization helps to address this cost through the consolidation of physical resources; however, virtualization also adds complexity to the system by creating a sharp increase in the number of managed virtual resources.

IT professionals are seeking more advanced capabilities and tools for managing both their physical and virtual systems across multiple architectures and environments. As virtualization becomes reality in today's IT infrastructures, the IBM Systems Director family can help businesses realize their full potential by providing a unified approach to platform management designed to lower IT operational costs and increase productivity. We discuss the HMC functions that manage the System p and System i servers in this book.

In this chapter, we tell you about the HMC concepts, the types of HMC, HMC connectivity, and enhancements in HMC Version 7.

For more detailed information about HMC, refer to the following sources:

- Operations Guide for the Hardware Management Console and Managed Systems, SA76-0085
- Hardware Information Center

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp

# 1.1 HMC concepts

With the HMC, a system administrator can perform logical partitioning functions, service functions, and various system management functions using either the Web browser based user interface or the command line interface (CLI). The HMC uses its connection to one or more systems (referred to in this book as *managed systems*) to perform various functions, including:

Creating and maintaining logical partitions in a managed system

The HMC controls logical partitions in managed systems. We explain these tasks in detail in Chapter 7, "Partitioning" on page 219.

Displaying managed system resources and status

We explain these tasks in Chapter 2, "Basic operation" on page 17.

Opening a virtual terminal for each partition

The HMC provides virtual terminal emulation for AIX and Linux logical partitions and virtual 5250 console emulation for i5/OS® logical partitions.

Displaying virtual operator panel values for each partition

You can see the operator panel messages for all partition within managed systems in HMC.

Powering managed systems on and off

We explain these tasks in Chapter 2, "Basic operation" on page 17.

Performing DLPAR operation

With the HMC, you can perform DLPAR operations that change the resource allocation (such as processor, memory, physical I/O, and virtual I/O) dynamically for the specified partition. We explain these tasks in detail in Chapter 7, "Partitioning" on page 219.

Managing Capacity on Demand operation

We explain these tasks in Chapter 13, "Capacity on Demand" on page 373.

Managing virtualization features

We explain these tasks in Chapter 7, "Partitioning" on page 219.

Managing platform firmware installation and upgrade

We explain these tasks in Chapter 11, "Firmware maintenance" on page 303.

Acting as a service focal point

You can use the HMC as a service focal point for service representatives to determine an appropriate service strategy and to enable the Service Agent to call home to IBM. We explain these tasks in Chapter 12, "Service Management" on page 331.

# 1.1.1 User interface

HMC Version 7 uses a Web browser based user interface. This interface uses a tree-style navigation model that provides hierarchical views of system resources and tasks using drill-down and launch-in-context techniques to enable direct access to hardware resources and task management capabilities. It provides views of system resources and provides tasks for system administration. For more information about using the Web browser based user interface, see 2.1, "Using the Web browser based user interface" on page 18.

The remote interface has changed in this release to also use a browser interface instead of a WebSM interface.

# 1.1.2 User tasks and roles

Each HMC user can be a member of a different role. Each of these roles allows the user to access different parts of the HMC and to perform different tasks on the managed system. HMC roles are either *predefined* or *customized*. When you create an HMC user, you must assign that user a task role. Each task role allows the user varying levels of access to tasks that are available on the HMC interface.

You can assign managed systems and logical partitions to individual HMC users, allowing you to create a user that has access to managed system A but not to managed system B. Each grouping of managed resource access is called a *managed resource role*.

Table 1-1 lists the predefined HMC roles, which are the default on the HMC.

User name	Role	Description
hmcoperator	Operator	The operator is responsible for daily system operation.
hmcsuperadmin	Super Administrator	The super administrator acts as the root user or manager of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.
hmcpe	Product Engineer	A product engineer assists in support situations but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.
hmcservicerep	Service Representative	A service representative is an employee who is at your location to install, configure, or repair the system.
hmcviewer	Viewer	A viewer can view HMC information, but cannot change any configuration information.

Table 1-1 Predefined HMC roles

# 1.2 HMC type

The HMC runs as an embedded application on an Intel® based workstation that can be a desktop or rack mounted system. The embedded operating system and applications take over the entire system, and no other applications are allowed to be loaded.

Whether you opt for a desktop or rack mounted version is a personal choice. Customers with space in their rack mounted systems would probably opt for the rack mounted version with the slide-away keyboard and display. The following options are available:

- ► 7042-C06 is a desktop HMC.
- ► 7042-CR4 is a rack mounted HMC.

All 7310 models are supported. The new machine type of the V7 HMC has the same hardware base with 7310-C06/CR4 as previous HMC versions. However,

the current POWER5<sup>™</sup> HMC must be upgraded to POWER6<sup>™</sup> HMC by order FC 0962.



Figure 1-1 is a picture of the IBM 7042 C06/CR4 HMC.

Figure 1-1 IBM 7042 Hardware Management Console

# 1.2.1 Desktop HMC

The supported desktop models are the 7042-C06 and older versions 7310 models. The older 7315 models are not supported by V7 of the HMC.

On the desktop you can connect a keyboard and mouse to either the standard keyboard, mouse PS/2 style connectors, or USB ports. You cannot connect any other devices to the HMC. Printers are not supported off the parallel port.

# 1.2.2 Rack mounted HMC

The supported rack mounted models are the 7042-CR4 and older versions 7310 models. The older 7315 models are not supported by V7 of the HMC. Figure 1-1 shows the HMC 7042-CR4 system unit as a standard 1 U unit and also the display and keyboard mounted in a standard 1 U pull-out tray. This model is a great choice for a dark machine room, where space is restricted.

You can find detail hardware information at this site:

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp

### 1.2.3 HMC version matrix to support POWER servers

The HMC has several versions to support the different type of power processors (POWER4<sup>™</sup>, POWER5, and new POWER6). In this book, we focus on new

HMC supported POWER6. POWER5 servers must be at least GA7 SF240 firmware level to be managed by the new version of HMC.

Table 1-2 shows the interoperability between HMC and POWER™ processors.

HMC Version	Supported managed system
Version 7 and later	POWER6 and POWER5 <sup>a</sup>
Version 4 and later, 5 and later, 6 and later	POWER5
Version 3 and later	POWER4

Table 1-2 HMC and POWER Processors interoperability

a. POWER5 servers must be at least GA7 SF240 firmware level.

You can find detailed information about HMC versions at:

http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html

# 1.3 HMC connectivity

You can control your managed system through HMC directly or remote clients without installing any application. Figure 1-2 illustrates how HMCs might be implemented in your network.



Figure 1-2 Implementations of HMCs

To provide flexibility and availability, you can implement HMCs as a local HMC or a redundant HMC, as shown in left side of Figure 1-3. To save space and to centralize multiple system management control points, you can configure multiple managed systems using a single HMC, as shown in right side of Figure 1-3.



Figure 1-3 HMC connectivity option

## 1.3.1 Local HMC

A *local HMC* is one that is located physically close to the system that it manages and that is connected by either a private or public network. An HMC in a *private network* is a DHCP server for the service processors of the systems it manages. An HMC can also manage a system over a *public network* where the managed system's service processor IP address has been assigned manually using the Advanced System Management Interface (ASMI) or assigned by a DHCP server on the public network. For convenience of service personnel, an HMC is typically kept in close proximity to the servers that it manages.

# 1.3.2 Redundant HMC

A *redundant HMC* manages a system that is already managed by another HMC. When two HMCs manage one system, they are peers, and each can be used to control the managed system. If both HMCs are connected to the server using private networks, each HMC must be a DHCP server set up to provide IP addresses on two unique, non-routing IP ranges.

For best redundancy, redundant HMCs are kept on separate subnetworks and attach to different server support network ports.

# 1.4 Enhancements in HMC Version 7

HMC Version 7 includes several new functions that support new POWER6 technology features. The HMC also configures and manages IBM System p and System i systems based on the POWER5 technology.

In this section, we introduce the new functions of HMC Version 7 and POWER6. Several new functions in this version of the HMC for System i and System p come from System z<sup>™</sup> HMC technology.

#### 1.4.1 Web browser based user interface

To access remotely an HMC running HMC Version 4, 5, or 6, a special client program (WebSM) was required. WebSM is no longer required with HMC Version 7. Remote access to an HMC running Version 7 requires only a standard (and supported) Web browser.

Highlights of the new Web based user interface include:

- Persistent GUI session across login
- The ability to manage both POWER5 and POWER6

The differences in the GUI include:

- Simplified operations
- Reorganized panels
- More descriptive GUI settings
- Redesigned panels

For more information about the Web browser based user interface, see 2.1, "Using the Web browser based user interface" on page 18.

# 1.4.2 System Planning Tool

The System Planning Tool (SPT) is a tool for designing logically partitioned systems and is the replacement for the LPAR Validation Tool (LVT). SPT creates a system plan that is saved as a sysplan file. That system plan can be just one system or it can contain multiple systems, each with a unique system name.

A system plan, also referred to as *sysplan*, is a representation or data model of the resources that are included in the system and how they are allocated to each partition. When you create the sysplan in SPT, the file will reflect the intended LPAR configuration for a target server. This sysplan includes details on partition allocations of memory, processors, and the I/O hardware required for each partition.

For additional information about the SPT, see Chapter 4, "System plans and the HMC" on page 133.

### 1.4.3 Customizable Data Replication

Customizable Data Replication allows another HMC to obtain customized console data from or send data to this HMC. For more information, see 2.5.30, "Manage Data Replication" on page 63.

### 1.4.4 Custom groups

Custom groups provide a mechanism for you to group system resources together in a single view or a way to organize the systems or partitions into smaller business or workload entities. For more information, see 2.2.4, "Configuration" on page 31.

# 1.4.5 New System Reference Code look-up

There is a single repository for all System Reference Code (SRC) and Progress Code for POWER6 systems. The SRC is a sequence of data words (codes) that:

- Identifies a system status
- Describes a detected hardware, Licensed Internal Code (LIC), or software failure
- Describes the unit that is reporting the failure and its location

SRCs can be viewed on a system's control panel, as a system console message, or from the following three panels on the HMC:

- Managed Serviceable Events overview display
- ► The Reference code column of the Server display
- ► The Reference Code History display

For POWER6 servers, the HMC provides active Web links to the SRC repository. Clicking on these links displays the additional SRC information.

For more information, see 12.2.1, "Service events" on page 333.

# 1.4.6 Processor compatibility

POWER6 systems support running in one of the following modes:

► POWER5 compatible

The POWER5 Compatible mode provides an application compatible execution mode on the POWER6 processor. In this mode, all new features of the POWER6 processor are disabled.

POWER6 Architecture

The POWER6 Architecture mode provides an execution mode compatible with Version 2.05 of the POWER Processor Architecture.

POWER6 Enhanced

The POWER6 Enhanced mode provides additional instructions not recognized by version 2.05 of the POWER Processor Architecture.

LPARs running on the same POWER6 system can run in different modes.

All POWER6 LPARs default to POWER6 Architecture mode. You can see and modify that mode in the command line interface. The GUI allows display of current LP compatibility mode but does not allow modification. The current status is shown in the Partition Properties window as shown in Figure 1-4.

🖲 https://hmc2.itsc.austin.ibm.com - HMC: Partition Properties : do 🖃 🗖 🔀					
Partition Properties : doc @ 9117-MMA-SN10FFE0B-L9					
General Hardwar	e Virtual Adapters	Settings	Other		
Processors Memory I/O					
Processing U	nits				
Minimum :	1.0				
Assigned :	2.0				
Maximum :	4.0				
Allow proces	sor pool utilization aut	thority			III
Processor Sha	aring				
Allow when p	artition is Inactive.			2	
Allow when p	artition is active.				
11					
11					
Processor Co	mpatibility Mode	_			
Compatibility M	ode: POWER6				
OK Cancel H	elp				~
Done				hmc2,itsc,austin,ibm,com	

Figure 1-4 Processor capability mode

# 1.4.7 Host Ethernet Adapter

A Host Ethernet Adapter (HEA) allows multiple logical partitions to share a single special physical Ethernet adapter. Unlike most other types of I/O devices, you can never assign the HEA itself to a logical partition. Instead, virtual subsets called *logical HEAs* or *LHEAs* are defined on the physical HEA. These LHEAs can then be assigned to logical partitions. This allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge on VIOS or another logical partition.

For more information, see 7.1.1, "Host Ethernet Adapter" on page 221.

# 1.4.8 Donating dedicated LPARs

POWER6 allows dedicated processors in LPAR to donate its idle processor cycles to the shared processor pool instead of being wasted as cycles in the dedicated partition as like shared processors LPAR. You can enable this function in the HMC. We explain how you can set up this function using HMC in 7.1.2, "Shared pool usage of dedicated capacity" on page 223.

### 1.4.9 Processor recovery and partition availability priority

The POWER6 processor supports enhanced RAS capabilities. One of enhanced RAS capacities make firmware checkpoint the state of a failed processor. The checkpoint state can be resumed on another good processor. This function is called *Processor Recovery*.

Sometimes, this causes a loss of entitled capacity for one or more Shared Processor LPARs. At that time, firmware notifies those partitions of the loss of capacity. To determine which LPARs prefer to be stolen capacity, you can set the *Partition Availability Priority* of LPAR using HMC.

All processor recovery actions as well as loss of entitled capacity are logged in the system error log.

# 1.4.10 Barrier Synchronization Register

POWER6 extends the Barrier Synchronization Register (BSR) support that was present in POWER5. BSR can now be partitioned and assigned in granules to individual LPARS. This BSR provides a low latency array of storage bytes to be used as synchronization points for parallel programming jobs.

When the BSR capability is enabled in HMC, as shown in Figure 1-5 on page 14, the managed system includes processors with BSR arrays and supports the use of the BSR arrays on the processors.

If an operating system supports the use of BSR arrays, a parallel-processing application running on that operating system can use a BSR array to perform barrier synchronization, which is a method for synchronizing the threads in the parallel-processing application. If you use logical partitions, BSR arrays can be assigned to logical partitions.

🧐 https://hmc2.itsc.austin.ibm.com - 9117-MMA-SN10FFE0B-L9 - M 🖃 🗖 🔯									
9117-MMA-SN10FFE0B-L9									
Ge	eneral	Processors	Memory	1/0	Power-On	Сара	bilities	Advanced	
				-7 -	Parameters				
Capabilities									
	Capability					Value			
i	5/OS Capable					True			
	5250 Application Capable					False			
	CoD Capable					True			
	Processor Capable					True			
	Memory Capable					True			
	Micro-partitioning Capable					True			
	Virtual I/O Server Capable					True			
	Logical Host Channel Adapter Capability					True			П
	Logical Host Ethernet Adapter Capability					True			
	Huge Page Capable					True			
	Barrier Synchronization Register (BSR) Capab					True			
	Service Processor Failover Capable					True			
	Shared Ethernet Adapter Failover Capable				apable	True			
	Redundant Error Path Reporting Capable				pable	True			
	GX Plus Capable					False			
	Partitio	n processor	compatibil	ity mo	de capable	True			
	Partitio	n Availability	Priority Ca	apable	9	True			
	Electro	nic Error Rep	orting Ca	pable		True			
Active Partition Processor Sharing Capable									
OK Cancel Help									
https://hmc2,itsc,austin,ibm,com/hmc/content?taskId=61&refresh,,, hmc2,itsc,austin,ibm,com 🔗									

Figure 1-5 BSR capable

# 1.4.11 Capacity on Demand enhancement

The Capacity on Demand (CoD) can be configured with inactive processor and memory resources that can be enabled dynamically and non-disruptively to the system. The CoD offering provides flexibility and improved granularity in processor and memory upgrades and is a useful configuration option to support future growth requirements. CoD also eliminates the need to schedule downtime to install additional resources at a given point in time.

This CoD was introduced in POWER5 products. Throughout this book, we introduce two new types of CoD and some enhancements:

- Mobile CoD
- ► Utility CoD

We explain these tasks in Chapter 13, "Capacity on Demand" on page 373.

# 2



This chapter describes how to use the Web browser based user interface to perform tasks on the HMC or on your managed resources.

# 2.1 Using the Web browser based user interface

HMC Version 7 is migrated to a new framework, the System z HMC framework. All existing management functions and commands remain unchanged. However, there are new user interface improvements and changes due to the new framework.

A major change is the Web browser based user interface. With this interface, you do not have to install an application to access the HMC remotely, and you can connect to the HMC using your browser. Firefox and Internet Explorer® are supported.

## 2.1.1 Starting the HMC

First, start the HMC by setting both the display and system units to the on position. You should then see the initialization window that includes the IBM logo and copyright information.

After finishing the initialization step, the Welcome window displays as shown in Figure 2-1. This page includes the link to log on, to view the online help, and the summarized HMC status information.



Figure 2-1 HMC Welcome window
To log on to the HMC, click **Log on and launch the Hardware Management Console web application** from the Welcome window. The Logon window opens as shown in Figure 2-2.

<u>F</u> ile <u>E</u>	dit <u>V</u> iew	Hi <u>s</u> tory	<u>B</u> ookmarks	S <u>p</u> lit	<u>T</u> ools	<u>H</u> elp		0
<b>0 (</b>	Hardwar	e Manag	ement Con	isole (	V7R31	0.0) L	.ogon	
Please	enter a u	serid and	password b	elow a	nd click	"Logo	n".	
Useri	id: h	scroot						
Pass	word: 🛛	*****						
Logor	n Canc	el Heli	2					

Figure 2-2 HMC Logon window

The HMC is supplied with a predefined user ID, *hscroot*, and the default password *abc123*. Both the user ID and password are case sensitive and must be entered exactly as shown. When you update your password, you can no longer keep it six characters. The minimum length for a password is now seven characters.

# 2.1.2 Session preservation

With HMC Version 7, you can remain in the GUI session across logins, as shown in Figure 2-3. If you want to preserve your session, then you should choose **Disconnect** and click **OK**.

Choose to Logoff or Disconnect
Would you like to log off the console, or disconnect from it? If you log off, your session is ended. If you disconnect, your session is preserved and your tasks continue to run. You can reconnect to the session at a later time and continue working.
<ul> <li>● Log off</li> <li>● Disconnect</li> </ul>
OK Cancel

Figure 2-3 HMC Log off or disconnect

After disconnecting from the session, you can reconnect to the session by selecting the session that you want to connect. As shown in Figure 2-4, session ID 7 has are two running jobs. When you reconnect that session, the jobs that you were doing previously are displayed. You also see that there are three disconnected sessions for the userid *hscroot*. This situation is a typical situation when all users log in with the same user ID (for example, *hsroot*). The disconnect feature provides another reason to use separate user IDs for each user.

<u>F</u> ile <u>E</u> r	dit <u>V</u> iew H	i <u>s</u> tory <u>B</u> ook	marks	S <u>p</u> lit	<u>T</u> ools	<u>H</u> elp				$\diamond$
Choo The foll to one reconne You car	ose a Disconnected Session ollowing disconnected sessions are available to user "hscroot". You can choose to either reconnect e of these sessions, or start a new session. To reconnect, select the session to which you wish to nect, then click " <b>Reconnect</b> ". To create a new session, click " <b>New Session</b> ". an also delete a disconnected session by selecting the session you wish to delete, and then clicking te".									
If you'd	rather cance	el connecting	g, click "	Cance	г.					
Select	Session Id	Disconnect	t Time			Creation Ti	me			Running Tasks
۲	7	May 15,	2007	1:30:	37 PM	May 15,	2007	1:29:33	PM	2
0	6	May 15,	2007	1:29:	28 PM	May 15,	2007	1:29:16	PM	0
0	5	May 15,	2007	1:29:	06 PM	May 15,	2007	1:27:38	PM	0
Recon	nect New :	Session D	elete	Cance						

Figure 2-4 Reconnecting the previous session

# 2.1.3 Components of the Web browser based user interface

The HMC workplace window is comprised of several major components as shown in Figure 2-5:

- ► The Banner
- The Task bar
- The Navigation pane
- The Work pane
- The Status bar



Figure 2-5 HMC workplace window

#### Banner

The *Banner*, across the top of the workplace window, identifies the product and logo. It is optionally displayed and is set by using the **Change User Interface Setting** task.

### Task bar

The *Task bar*, located below the Banner, displays the names of any tasks that are running, the user ID you are logged in as, online help information, and the

ability to logoff or disconnect from console. It provides the capability of an active task switcher. You can move between tasks that were launched and have not yet been closed. However, the task switcher does not pause or resume existing tasks.

### **Navigation pane**

The *Navigation pane*, in the left portion of the window, contains the primary navigation links for managing your system resources and the HMC. These include:

- ► Welcome
- Systems Management
- System Plans
- HMC Management
- Service Management
- Updates

#### Work pane

The *Work pane*, in the right portion of the window, displays information based on the current selection from the Navigation pane. For example, when you select **Welcome** in the navigation pane, the Welcome window content displays in the work pane, as shown in Figure 2-5 on page 21.

### Status bar

The *Status bar*, in the bottom left portion of the window, provides visual indicators of current overall system status. It also includes a status overview icon that can be selected to display more detailed status information in the Work pane.

# 2.2 Systems Management - Servers

In the HMC workplace window, Systems Management includes a tree view of managed resources. Resources can include servers, partitions, frames, and custom groups. You control the activity about a managed system in this category: Power on/off, Activate/Shut down/Restart partitions, View properties of the managed system, and so on. Each managed server is a tree that includes the partitions that are defined.

This section describes the tasks to manage a server.

# 2.2.1 Servers

The *Servers* node represents the servers that are managed by this HMC. To add servers:

- 1. Click Add Managed Systems, as shown in Figure 2-6.
- 2. Then, select Add a managed system, and click Next.

Add Managed Syste	ems
<u> Add Managed</u>	Add Managed Systems
- Systems	
Add Servers	
Confirm Add	Use this wizard to add systems in the network to the systems managed by this HMC. If you know the name or IP address of the system you want to add, enter its specific name or IP address and click Next. If you want to find the IP addresses of systems in the network, you can specify a range of IP addresses and click Next to view the list of IP addresses with their system names that were discovered in the network. You can then select one or more sytems from the list to add to the managed systems of this HMC. The discovery process will take a long time.
	Add a managed system     Add
	IP Address/Host name: *
	Password:
	○ Find managed systems Find
	Enter a range of IP addresses to search for managed systems. Beginning IP Address:
	Ending IP Address: *
< Back Next >	Finish Cancel Help

Figure 2-6 Add Managed Systems window

- 3. Click **Servers** to see a listing of individually defined servers in table form in the work pane, as shown in Figure 2-7.
- 4. Select the server that you want to add to the HMC.

Hardware Management Consol	e
	hscroot   Help   Logoff
Welcome Given Systems Management	Contents of: Servers
U Servers     J 9117-MMA-SN10DD4AC-L10     J 9117-MMA-SN10FFE0B-L9	Sele ^ Name ^ Status ^ Available Processii ^ Available CB / Code ^ Code
TP Custom Groups	D 9117-MMA-SN10DD4AC-L10 Power ( 0 0
System Plans	Dependir 0.7 0.375
HMC Management	Total: 2 Filtered: 2 Selected: 0
🔀 Service Management	
🔂 Updates	
	Tasks: Servers [Expand All   Collapse All ]
Status: Attentions and Events	Connections Add Managed System
📰 🛞 🔔 😭	

Figure 2-7 System Management servers window

By default, the contents of servers displays the following attributes:

Name

Specifies the user defined name of the managed system.

Status

Displays the current status of the managed system (for example, *Operating*, *Power off*, *Initializing*, and so forth). In addition, displays icons that represent an unacceptable state and active Attention LED.

Available Processing Units

Displays the number of processing units that are available for assignment to logical partitions on the managed system. This number is the total number of processing units that are activated on the managed system minus the number of processing units that are assigned to the logical partitions, including the logical partitions that are shut down, on the managed system. This number does not include any processing units that have not yet been activated with Capacity on Demand (CoD).

Available Memory

Displays the amount of memory that is available for assignment to logical partitions on the managed system. This amount is the total amount of memory that is activated on the managed system minus the amount of memory needed by managed system firmware minus the amount of memory that is assigned to the logical partitions, including the logical partitions that are shut down, on the managed system. This number does not include any memory that has not yet been activated with CoD. The available memory amount can be shown in MB or GB. Click **MB** or **GB** in the Available Memory column title.

► Reference Code

Displays the progress System Reference Code (SRC). By clicking the displayed SRC, you can receive more information.

The table can also display the following optional attributes:

- Name
- Status
- Available Processing Units
- ► Reference Code
- Configurable Processing Units
- ► Configurable Memory
- Serial Number
- ► Type-Model
- ► CoD Processor Capable
- ► CoD Memory Capable
- Permanent Processors
- ► On/Off CoD Processor State
- ► Trial CoD Processor State
- Reserve CoD Processor State
- Utility CoD Processor State
- ► Permanent Memory
- On/Off CoD Memory State
- ► Trial CoD Memory State

These attributes display when you select the *Column configuration* icon on the table toolbar as shown in Figure 2-8. This function allows you to select additional attributes that you want displayed as columns in the table.

Hardware Management Consol	e
<ul> <li>Welcome</li> <li>Systems Management</li> <li>Servers         <ul> <li>9117-MMA-SN10DD4AC-L10</li> <li>9117-MMA-SN10FFE0B-L9</li> <li>Custom Groups</li> </ul> </li> <li>System Plans</li> <li>HMC Management</li> <li>Service Management</li> <li>Service Management</li> <li>Updates</li> </ul>	Contents of: Servers  Contents of: Servers  Select ^ Name
Status: Attentions and Events	Image: Servers         9117-MMA-SN10DD4AC-L10         A Standby         0         0.9375           Image: Servers         Image: Total: 2         Standby         0.7         6.5
📃 😣 🔔 💟	Connections

Figure 2-8 Column configuration

You can also use Views from the table toolbar to display the default server attributes in the table or to display the CoD server attributes in the table. After you make one of those selections, you need to select another item on the left pane, such as Systems Management, and then reselect **Servers** to see the change in the columns.

# 2.2.2 Properties

The Properties task displays the selected managed system's properties as shown in Figure 2-9.

9117-M	MA-SN10FF	EOB-L9				
General	Processors	Memory	I/O	Power-On Parameters	Capabilities	Advanced
Name: * 9117-MMA-SN10FFE0						
Serial nur	nber:			10FFE0B		
Type/Mod	lel:			9117-MMA		
State:				Operating		
Attention	LED:			On		
Service pr	rocessor vers	sion:		00050000		
Manufacti	uring default	configurat	ion:	False		
Maximum	number of p	artitions:		40		
Service pa	artition:			Unassigned	•	
Power	off the syste	m after all	the lo	ogical partitions are pov	wered off.	
OK Ca	ncel Help	]				

Figure 2-9 Properties task

These properties include:

- Identifying information
- Available and installed processors
- Available and installed memory
- Available and installed I/O
- Current system configuration settings
- Server capabilities

Use the Help button to get additional information for each property.

# 2.2.3 Operations

Operations includes the tasks for server operations. The following tasks are represented in the Operations tasks:

- Power On
- Power Off
- ► LED status
- Schedule Operations
- Advanced System Management Interface(ASMI)
- Utilization Data
- Rebuild
- Change Password

This section describes these tasks.

### **Power On**

Use the Power On task to start a managed system. You can choose from three different options to start your managed system:

Partition standby

When the Partition standby is completed, the system is in standby mode. Partition standby mode allows you to create and activate logical partitions.

System profile

Turns on the system according to a predefined set of system profiles. Select the system profile that you want to use from the list.

Partition auto start

Turns on the managed system to partition standby mode and then activates all partitions that are marked as auto start or those partitions that were running when the system shut down. For example, if you create a partition with four processors, dynamically remove one processor from the logical partition, and then shut down the system, the partition auto start option activates this partition with three processors because the three-processor configuration was the last configuration used. The HMC ignores whatever is specified in the profile for the partition. You can create and activate logical partitions in partition auto start mode.

### **Power Off**

This task shuts down the managed system. Turning off the managed system makes all partitions unavailable until the system is turned on again.

Before you turn off the managed system, ensure that all logical partitions have been shut down and that their states have changed from *Running* to *Ready*.

If you do not shut down all logical partitions on the managed system before you turn off the managed system, the managed system shuts down each logical partition before the managed system itself turns off. This can cause a substantial delay in turning off the managed system, particularly if the logical partitions are not responsive. Further, the logical partitions might shut down abnormally, which could result in data loss and further delays when you activate the logical partitions again.

You can choose from the following options (see Figure 2-10):

#### Normal power off

The system ends all active jobs in a controlled manner. During that time, programs running in those jobs are allowed to perform cleanup (end-of-job processing).

#### Fast power off

The system ends all active jobs immediately. The programs running in those jobs are not allowed to perform any cleanup. Some applications, such as Web servers that are providing information, might not have a problem with fast power off. Other applications, such as databases that have cached information, might loose data if the application cannot perform cleanup before the application ends.

Power Off Managed System - 9117-MMA-SN10FFE0B-L9
Powering off the managed system will make all of the partitions unavailable until the machine is powered on again. Select a power off option below and click OK to power off the managed system or click Cancel.
Power Off Options
🗵 Normal power off
○ Fast power off
OK Cancel Help

Figure 2-10 Power Off task

## **LED Status**

LED Status includes the tasks for viewing system attention LED information, lighting specific LEDs to identify a system component, and testing all LEDs on a managed system.

You can choose from the following options:

View System Attention LED

Displays the current system attention LED and corresponding partition LED states for the selected system. From this task, you can activate or deactivate system attention LEDs.

#### Identify LED

Displays the current Identify LED states for all the location codes contained in the selected enclosure. From this task, you can select a single location code or multiple location codes to operate against and activate or deactivate the LEDs by selecting the corresponding button.

Test LED

Initiates an LED Lamp Test against the selected system. All LEDs activate for several minutes.

### **Schedule Operations**

This task creates a schedule for certain tasks, such as activating a system or partition using a specific profile, backing up Profile Data, or turning on or off a managed system without operator assistance. This task can also be performed on a defined schedule.

Figure 2-11 shows what can be added for a scheduled operation.

elect	Operation
۲	Activate on a System Profile
0	Backup Profile Data
0	Power Off Managed System
0	Power On Managed System

Figure 2-11 Scheduled Operations task

From this task you can:

- Create or delete scheduled operations
- ► View scheduled operations sorted by date, object, or operation

### **Advanced System Management**

If configured to do so, the HMC connects directly to the Advanced System Management (ASM) interface for a selected system from this task. We explain this task in Chapter 14, "Advanced System Management Interface" on page 423.

## **Utilization Data**

Utilization events are records that include information about the memory and processor utilization on a managed system at a particular time. You can set the HMC to collect utilization data in this task.

### Rebuild

You can use this task to extract the configuration information from the managed system and to rebuild the information about the HMC. Rebuilding the managed system means that you update, or refresh, the information about the HMC about the managed system. Rebuilding the managed system can be helpful when the

state of the managed system is *Incomplete*. The Incomplete state means that the HMC has lost communication with the managed server and no longer has complete information.

Rebuilding the managed system is different from simply refreshing the HMC window. When the managed system is rebuilt, the HMC extracts the information from the managed system. You cannot start other tasks while the HMC rebuilds the managed system. This process can take several minutes.

### **Change Password**

You can change the HMC access password. After the password is changed, it must be changed on all other systems assessing this HMC. We explain how to change the access password in 5.2.1, "Changing the user password" on page 185.

# 2.2.4 Configuration

Configuration includes the tasks for configuring your managed systems. The Configuration tasks include:

- Create Logical Partition
- System Plans
- Manage Custom Groups
- View Workload Management Groups
- Partition Availability Priority
- Manage System Profiles
- Manage Partition Data

## **Create Logical Partition**

This task creates a new AIX, Linux, VIO Server, or i5/OS logical partition on a managed system. The Create LPAR Wizard helps you to create a new logical partition and a default profile for the partition. We explain these tasks in 7.2, "Creating logical partitions" on page 228.

### **System Plans**

System Plans records or deploys specifications for logical partitions, partition profiles, or hardware specifications on a chosen system. We explain this task in 4.1, "System plans" on page 134.

### Manage Custom Groups

Custom Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you

prefer. You can also nest groups (a group contained within a group) to provide hierachical or topology views.

There can be one or more user-defined groups already defined on your HMC. There are default groups listed under the Custom Groups node under Server Management. The default groups are *All Partitions* and *All Objects*. You can create others, delete the ones that were created, add to created groups, or delete from created groups by using the Manage Custom Groups task, as shown in Figure 2-12.

Manage Groups	^
Selected Item(s): 9117-MMA-SN10FFE0B-L9	
Select the type of group action to perform. Group Action	
<ul> <li>Create a new group</li> <li>Add to an existing group</li> <li>Remove from an existing group</li> <li>Remove group</li> <li>Create a new pattern match group</li> <li>Edit existing pattern match group</li> </ul>	III
New group name:	
New group description:	
Group name:	
OK Cancel Help	~

Figure 2-12 Manage Custom Groups

# **View Workload Management Groups**

This task displays a detailed view of the workload management groups that you have specified for a managed system as shown in Figure 2-13. Each group displays the total number of processors, processing units for partitions using shared mode processing, and the total amount of memory allocated to the partitions in the group.

ion workload grou nber of processor al amount of men sors Memory(M	ups you have spe rs, processing unit mory allocated to t IB) State
sors Memory(M	IB) State
sors Memory(M	IB) State
terreturn t	
5248	
1024	Running
128	Not Activated
4096	Running
0	Not Activated
	128 4096 0

Figure 2-13 Partition Workload Groups

# **Partition Availability Priority**

This task specifies the partition availability priority of each logical partition on a managed system. The managed system uses partition availability priorities in the case of processor failure.

If a processor fails on a logical partition, and there are no unassigned processors available on the managed system, the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. This allows the logical partition with the higher partition-availability priority to continue running after a processor failure. We explain this task in 7.1.3, "Partition availability priority" on page 225.

## **Manage System Profiles**

A system profile is an ordered list of partition profiles that is used by the HMC to start the logical partitions on a managed system in a specific configuration.

When you activate the system profile, the managed system attempts to activate each partition profile in the system profile in the order specified. A system profile

helps you activate or change the managed system from one complete set of logical partition configurations to another. They can also be used to validate the resource configuration of multiple partitions to ensure that resource conflicts do not exist between partitions.

### **Manage Partition Data**

This task provides four operations, backup, restore, initialize, and remove, to manage profile data. We explain this task in 7.3, "Managing partition data" on page 247.

# 2.2.5 Connection

The Connection tasks allow you to view the HMC connection status to service processors or frames, reset those connections, connect another HMC to the selected managed system, or connect another managed system to the HMC.

This section explains these tasks.

### **Service Processor Status**

This task displays the HMC connection status to the service processor of a selected managed system, as shown in Figure 2-14. If you have selected a frame, Service Processor Status displays the state of the connection from the HMC to side A and side B of the bulk power assembly.

Service Processor Stat	us: 9117-MMA-SN1	0DD4AC-L10					
Service processor faile	ver enabled						
Service processor failover	readiness:						
State:       Not Ready         Reason:       Not Ready (secondary service processor is not installed)							
Service Processor Status	5.						
IP Address Location Code Service Connection Connection error code							
172.16.255.254 Unavailable PRIMARY Connected							
OK Cancel Help							

Figure 2-14 Service Processor Status

### **Reset or Remove Connections**

This task removes or resets a managed system from the Contents area of the HMC.

When you remove the connection with a managed system, the connection is broken between the HMC and the managed system. Remove the connection with the managed system if you no longer want to manage the managed system using this HMC. Remove the connection before you physically disconnect the HMC from the managed system (or from the network).

When you reset the connection with a managed system, the connection is broken and then reconnected. Reset the connection with the managed system if the managed system is in a No Connection state and you have verified that the network settings are correct on both the HMC and the managed system.

# **Disconnect Another HMC**

You can disconnect another HMC from the selected managed system as shown in Figure 2-15. Also, you can find which HMC has locked the selected managed system. This task releases any lock that the other HMC might have on the selected managed system. After the disconnection is complete, the other HMC automatically attempts to reconnect to the managed system.

When you use an HMC to change a managed system, the HMC locks the managed system so that no other HMC can make conflicting changes at the same time. Normally, the HMC unlocks the managed system after the change is complete. If there is an error and the managed system remains locked, you must disconnect the HMC from the managed system to reset the lock before other HMCs can change the managed system.

Disconnect Another HMC					
The following Hardware Management Consoles are connected to the same managed server. This task will drop the connection between the selected HMC and the managed server. Once the task is performed, the disconnected HMC will try to reconnect. If the disconnected HMC has a lock on the managed server, this task forces the selected HMC to release its lock. To continue this operation, select the HMC from the list below and click OK.					
Select	ModelType*Serial	Hostname	IP Address	Locked	
۲	7310C03*10362EA	Not Available	Not Available	Yes	
				OK	Cancel Help

Figure 2-15 Disconnect another HMC

### Add Managed System

This task guides you through adding systems in the network to systems managed by this HMC.

# 2.2.6 Hardware (Information)

Hardware (Information) includes the tasks for configuring your Host Ethernet Adapter (HEA) and Host Channel Adapter, for viewing RIO Topology.

This section explains these tasks.

### **Host Ethernet Adapter**

This task display the port configuration and status of the physical HEAs on the managed system as shown in Figure 2-16.

Host Ethernet Adapters : 9117-MMA-SN10FFE0B-L9									
Choose a Physical Location Code to view / modify that Host Ethernet Adapter's information. U789D.001.DQDVWZK-P1									
Curren	t Status	Deat TD	Daut Truce	Deat Carrie TD	Dart Crown MCC Value	Compation	Chata Canad	Dualau	Town and the fills
Select	Physical Port Location Codes	Port ID	Port Type	Port Group ID	Port Group MCS value	Connection	State Speed	Duplex	Transmit Fig
۲	C10-T2	0	1 G	2	4	up	1 Gbps	full	enabled
0	C10-T1	1	1 G	2	4	down	Auto	full	disabled
Configure Logical Partition Usage Logical Partition Logical Port ID Logical Port DRC Name Logical Port burned-in MAC / user-defined MAC Capability Allowed VLAN IDs I									
VIOS1	_L9 1 Por	t 1		00145E5F1EA	0/00000000000	100000000000000000000000000000000000000	Base Minimum		)
ОК	Cancel Help								

Figure 2-16 Displaying Host Ethernet Adapters configuration information

You can change the configuration of any of the ports on an HEA by selecting the HEA, selecting the port under Current Status, and clicking **Configure**. Then, the port configuration displays as shown in Figure 2-17. We explain these tasks in detail in 7.1.1, "Host Ethernet Adapter" on page 221.

HEA Physical Port Configuration : 9117-MMA-SN10FFE0B-L9					
Use the fields below to specify the configuration for the selected physical port.					
Speed:	Duplex:				
Maximum receiving packet size: 1500 non-jumbo frame	Pending Port Group Multi-Core Scaling value:				
✓ Flow control enabled	Promiscuous LPAR: VIOS1_L9				
OK Cancel Help					

Figure 2-17 HEA Physical Port Configuration

### **Host Channel Adapter**

A Host Channel Adapters (HCA) provides a managed system with port connections to other InfiniBand® devices. That port can be connected to another HCA, a target device, or an InfiniBand switch that redirects the data coming in on one of its ports out to a device attached to another of its ports.

This task shows a list of the HCA for the managed system. You can find more information at:

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic= /iphae/iphaeinfinibandproducts.htm

### Virtual I/O Adapters

You use the Virtual I/O Adapters commands to view the topology of currently configured virtual SCSI and virtual Ethernet adapters on a selected partition.

You use the SCSI task to view the topology of virtual SCSI adapters on a partition. Displayed are:

- Adapter name
- Backing device
- Remote partition
- Remote Adapter
- ► Remote Backing Device

Use the Ethernet task to view the current virtual Ethernet configuration for the partition:

- Adapter name
- Virtual LANs
- ► I/O Server
- ► Server Virtual Adapter
- Shared Adapter

Partitions assigned to a VLAN that is bridged have access to a external network using a physical shared Ethernet adapter owned by a Virtual I/O Server.

# **View RIO Topology**

Use this task to display the current RIO topology of the selected managed system. Current Topology displays the current topology. Any discrepancies between the current topology and the last valid topology are identified as errors. The following information is shown:

- The starting location of the physical RIO cable and the RIO connection (cable to port)
- The ending location of the physical RIO cable and the RIO connection (cable to port)
- Starting Node Type Displays the values of the node. Possible values are Local Bridge, Local NIC, Remote Bridge, and Remote NIC
- Link Status Displays the leading port status
- Cable Length Displays the length of the RIO cables. Errors occur when the actual cable lengths are different from the expected cable lengths
- ► The serial number of the power-controlling managed system
- ► The serial number of the function-controlling managed system

# 2.2.7 Updates

The Updates tasks perform a guided update of the managed system, power, and I/O Licensed Internal Code. You can see the current LIC level in the View system information task. We explain these tasks in detail in Chapter 11, "Firmware maintenance" on page 303.

# 2.2.8 Serviceability

Problem Analysis on the HMC detects error conditions automatically and reports any problem that requires service to repair it. These problems are reported as serviceable events. We explain these tasks in detail in Chapter 12, "Service Management" on page 331.

# 2.2.9 Capacity on Demand

Capacity on Demand (CoD) allows you to activate one or more resources dynamically on the server as your business peaks dictate. You can activate inactive processors or memory units that are already installed on your server on a temporary and permanent basis. We explain these tasks in detail in Chapter 13, "Capacity on Demand" on page 373.

# 2.3 System Managements - Partitions

Systems Management includes a tree view of managed resources. Resources can include servers, partitions, frames and custom groups. Each managed server is a tree that includes the partitions that are defined.

This section describes the tasks displayed when a partition is selected.

# 2.3.1 Operations

Operations include the tasks for server operations. The Operations tasks include:

- Activate
- Shut Down
- Restart
- Manage Attention LED
- Schedule Operations
- Delete

### Activate

Use the Activate task to activate a partition on the managed system in the *Not Activated* state.

A list of profiles displays that are valid to start the selected partition. Select from the list of profiles and click **OK** to activate the partition. Select **Open a terminal window or console**.

### Shut Down

Use this task to shut down the selected logical partition or partitions.

For i5/OS logical partitions, use this window only if you cannot shut down the i5/OS logical partition from the command line of the operating system. Using this window to shut down an i5/OS logical partition results in an abnormal IPL.

Choose from the following options:

Delayed

The HMC shuts down the logical partition using the delayed power off sequence, allowing the logical partition time to end jobs and write data to disks. If the logical partition is unable to shut down within the predetermined amount of time, it ends abnormally, and the next restart might be longer than normal.

#### Immediate

The HMC shuts down the logical partition immediately. The HMC ends all active jobs immediately. The programs running in those jobs are not allowed to perform any job cleanup. This option might cause undesirable results if data is updated partially. Use this option only after a controlled shutdown has been unsuccessfully attempted.

#### Operating System

The HMC shuts down the logical partition normally by issuing a shutdown command to the logical partition. During this operation, the logical partition performs any necessary shutdown activities. This option is only available for AIX logical partitions.

#### Operating System Immediate

The HMC shuts down the logical partition immediately by issuing a **shutdown** -**F** command to the logical partition. During this operation, the logical partition bypasses messages to other users and other shutdown activities. This option is only available for AIX logical partitions.

### Restart

Restart Use this task to restart the selected logical partition or partitions.

For i5/OS logical partitions, use this window only if you cannot restart the i5/OS logical partition from the command line of the operating system. Using this window to restart an i5/OS logical partition will result in an abnormal IPL.

Choose one of the following options. The Operating System option and the Operating System Immediate option are only enabled if Resource Monitoring and Control (RMC) is up and configured:

#### ▶ Dump

The HMC shuts down the logical partition and initiates a main storage or system memory dump. For AIX and Linux logical partitions, the HMC also notifies the logical partition that it will be shut down. For i5/OS logical partitions, the processors are stopped immediately. After the shutdown is complete, the logical partition is immediately restarted. (i5/OS logical partitions are restarted multiple times so that the logical partition can store the dump information.) Use this option if a portion of the operation system appears to be hung and if you want a dump of the logical partition for analysis.

#### Operating System

The HMC shuts down the logical partition normally by issuing a **shutdown** -**r** command to the logical partition. During this operation, the logical partition performs any necessary shutdown activities. After the shutdown is complete, the logical partition is immediately restarted. This option is only available for AIX logical partitions. Immediate: The HMC shuts down the logical partition immediately. The HMC ends all active jobs immediately. The programs running in those jobs are not allowed to perform any job cleanup. This option might cause undesirable results if data has been partially updated. Use this option only after a controlled end has been unsuccessfully attempted.

#### Operating System Immediate

The HMC shuts down the logical partition immediately by issuing a **shutdown** -**Fr** command to the logical partition. During this operation, the logical partition bypasses messages to other users and other shutdown activities. After the shutdown is complete, the logical partition is immediately restarted. This option is only available for AIX logical partitions.

#### Dump Retry

The HMC retries a main storage or system memory dump on the logical partition. After this is complete, the logical partition is shut down and restarted. Use this option only if you have previously tried the Dump option without success. This option is only available for i5/OS logical partitions.

## **Manage Attention LED**

Use the Manage Attention LED to activate or deactivate an attention LED on your partition. All attention LEDs for the partitions on the managed system are listed. Select an LED and choose to activate or deactivate.

### **Schedule Operations**

Use this task to create a schedule for certain operations to be performed on the logical partition without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times. For example, you could schedule an operation to remove resources from a logical partition or move resources from one logical partition to another.

### Delete

The Delete task deletes the selected partition and all of the partition profiles associated with the partition from the managed system. When you delete a partition, all hardware resources currently assigned to that partition become available to other partitions.

# 2.3.2 Configuration

Configuration includes the tasks for configuring partitions. The Configuration tasks include:

- Manage Profiles
- Manage Custom Groups
- Save Current Configuration

## **Manage Profiles**

Use the Manage Profiles task to create, edit, copy, delete, or activate a profile for the selected partition.

A partition profile includes the resource configuration for the partition. You can modify the processor, memory, and adapter assignments for a profile by editing the profile.

The default partition profile for a logical partition is the partition profile that is used to activate the logical partition if no other partition profile is selected. You cannot delete the default partition profile unless you first designate another partition profile as the default partition profile. The default profile is defined in the status column.

Choose **Copy** to create an exact copy of the selected partition profile. This allows you to create multiple partition profiles that are nearly identical to one another by copying a partition profile and changing the copies as needed.

# Manage Custom Groups

Custom Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you prefer. You can also nest groups (a group contained within a group) to provide hierachical or topology views.

There can be one or more user-defined groups already defined on your HMC. There are default groups listed under the Custom Groups node under Server Management. The default groups are *All Partitions* and *All Objects*. You can create others, delete the ones that were created, add to created groups, or delete from created groups by using the Manage Groups task as shown in Figure 2-18.

Manage Groups				
Selected Item(s): 9117-MMA-SN10FFE0B-L9				
Select the type of group action to perform. Group Action				
<ul> <li>Create a new group</li> <li>Add to an existing group</li> <li>Remove from an existing group</li> <li>Remove group</li> <li>Create a new pattern match group</li> <li>Edit existing pattern match group</li> </ul>				
New group name:				
New group description:				
Group name:				

Figure 2-18 Manage Custom Groups

## **Save Current Configuration**

Use this task to save the current configuration of a logical partition to a new partition profile by entering a new profile name. This procedure is useful if you change the configuration of a logical partition using dynamic logical partitioning and you do not want to lose the changes when you restart the logical partition.

You can perform this procedure at any time after you initially activate a logical partition.

# 2.3.3 Dynamic Logical Partitioning

Dynamic Logical Partitioning (DLPAR) tasks add or remove processors, memory, and adapters to and from logical partitions dynamically.

This section discusses these tasks.

#### Processor

Use DLPAR Processor tasks to add or remove processor resources from a logical partition or to move processor resources from one logical partition to another. These tasks include:

Add or Remove

Use the Add or Remove task to add processor resources to or remove processor resources from the selected logical partition without restarting the logical partition.

► Move

Use the Move task to move processor resources from the selected logical partition to another logical partition without restarting either logical partition.

### Memory

Use DLPAR Memory tasks to add or remove memory resources from a logical partition or to move memory resources from one logical partition to another. These tasks include:

Add or Remove

Use the Add or Remove task to add memory to or remove memory from the selected logical partition without restarting the logical partition.

Move

Use the Move task to move memory from the selected logical partition to another logical partition without restarting either logical partition.

## **Physical Adapters**

Use the DLPAR Physical Adapters tasks to add I/O slots to a logical partition without restarting the partition or to move or remove I/O slots from a logical partition without restarting the partition.

These tasks include:

► Add

Use the Add task to add I/O slots to a logical partition without restarting the partition. When you add an I/O slot to a logical partition, the I/O adapter in that I/O slot and the devices that are controlled by the I/O adapter can be used by the logical partition. This function is typically used to share infrequently used devices among logical partitions by moving these devices from one logical partition to another.

#### Move or Remove

Use the Move or Remove task to remove I/O slots from a logical partition or move I/O slots between logical partitions without restarting the logical partitions. When you remove an I/O slot from a logical partition, the I/O adapter in that I/O slot and the devices that are controlled by the I/O adapter are also removed from the logical partition. If you choose to move the I/O slot to another logical partition, the I/O adapter and the devices that are controlled by the I/O slot to another logical partition, the I/O adapter and the devices that are controlled by the I/O adapter are also moved to the other logical partition. This function is typically used to share infrequently used devices among logical partitions by moving these devices from one logical partition to another.

It is recommended that you vary off the I/O slot and all I/O adapters and devices connected to the I/O slot before you remove the I/O slot from the logical partition.

# 2.4 Systems Management - Frames

Systems Management includes a tree view of managed resources. Resources can include servers, partitions, frames and custom groups.

This section describes the tasks displayed when a frame is selected.

# 2.4.1 Properties

The Properties task displays the selected frame properties. These properties include:

General

The General tab displays the frame name and number, state, type, model, and serial number.

Managed Systems

The Managed Systems tab displays all of the managed systems included in the frame and their cage numbers. A cage is a division of the enclosure that holds the managed systems, the I/O units, and the bulk power assemblies (BPAs).

I/O Units

The I/O Units tab displays all of the I/O units contained in the frame, their cage numbers, and their assigned managed systems. A cage is a division of the enclosure that holds the managed systems, the I/O units, and the bulk power assemblies (BPAs). *Not owned* in the System column indicates that the corresponding I/O unit has not been assigned to a managed system.

# 2.4.2 Operations

Operations includes the tasks for frame operations. The Operations tasks include:

- Initialize
- Rebuild
- Change Password
- Power On or Power Off I/O Unit

### Initialize

Use the Initialize task to initialize a frame.

When you initialize a managed frame, all of the frames managed by the HMC are powered on. As each individual frame is powered on, the I/O units that are contained within the frame are powered on as well. When all the I/O units for the frame have been powered on, then the managed systems that are contained within the frame are powered on. The complete initialization process can take several minutes to complete.

### Rebuild

Use the Rebuild task to rebuild frame information about the HMC.

Updating, or rebuilding, the frame acts much like a refresh of the frame information. Rebuilding the frame is useful when the system's state indicator in the Work pane of the HMC is shown as Incomplete. The Incomplete indicator signifies that the HMC cannot gather complete resource information from the managed system within the frame.

No other tasks can be performed on the HMC during this process, which can take several minutes.

### **Change Password**

Use the Change Password task to change the HMC access password on the selected managed frame. After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed frame.

Enter the current password. Then enter a new password and verify it by entering it again.

### Power On or Power Off I/O Unit

Use the Power On or Power Off I/O Unit task to power off an I/O unit.

Only units or slots that reside in a power domain can be turned off. The corresponding power on or off buttons are disabled for location codes that are not controllable by the HMC.

# 2.4.3 Configuration

Configuration includes the Manage Custom Groups task for configuring frames.

### Manage Custom Groups

Custom Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you prefer. You can also nest groups (a group included within a group) to provide hierachical or topology views.

There can be one or more user-defined groups already defined on your HMC. There are default groups listed under the Custom Groups node under Server Management. The default groups are *All Partitions* and *All Objects*. You can create others, delete the ones that were created, add to created groups, or

delete from created groups by using the Manage Custom Groups task as shown in Figure 2-19.

Manage Groups				
Selected Item(s): 9117-MMA-SN10FFE0B-L9				
Select the type of group action to perform. Group Action				
<ul> <li>Create a new group</li> <li>Add to an existing group</li> <li>Remove from an existing group</li> <li>Remove group</li> <li>Create a new pattern match group</li> <li>Edit existing pattern match group</li> </ul>				
New group name:				
New group description:				
Group name:				
OK Cancel Help				

Figure 2-19 Manage Custom Groups

# 2.4.4 Connections

The Connections tasks allow you to view the HMC connection status to frames or reset those connections. This section describes these tasks.

### **Bulk Power Assembly Status**

Use the Bulk Power Assembly Status task to view the state of the connection from the HMC to side A and side B of the bulk power assembly. The HMC operates normally with a connection to either side A or side B. However, for code update operations and some concurrent maintenance operations, the HMC needs connections to both sides.

### Reset

Use the Reset task to reset the connection between the HMC and the selected managed frame.

When you reset the connection with a managed frame, the connection is broken and then reconnected. Reset the connection with the managed frame if the managed frame is in a *No Connection* state and you have verified that the network settings are correct on both the HMC and the managed frame.

# 2.4.5 Hardware (Information)

Hardware (Information) includes the task for configuring or viewing RIO Topology.

### **View RIO Topology**

Use this task to display the current RIO topology of the selected managed frame. Current Topology displays the current topology. Any discrepancies between the current topology and the last valid topology are identified as errors.

The following information is shown:

- The starting location of the physical RIO cable and the RIO connection (cable to port)
- The ending location of the physical RIO cable and the RIO connection (cable to port)
- Starting Node Type Displays the values of the node. Possible values are Local Bridge, Local NIC, Remote Bridge, and Remote NIC
- Link Status Displays the leading port status
- Cable Length Displays the length of the RIO cables. Errors occur when the actual cable lengths are different from the expected cable lengths
- ► The serial number of the power-controlling managed system
- ► The serial number of the function-controlling managed system

## 2.4.6 Serviceability

Problem Analysis on the HMC detects error conditions automatically and reports any problem that requires service to repair it. These problems are reported as serviceable events. We explain these tasks in detail in Chapter 12, "Service Management" on page 331.

# 2.5 HMC Management

This task includes a categorized or alphabetical view of HMC management tasks and their descriptions. These tasks are used for setting up the HMC, maintaining its internal code, and securing the HMC.

To display the tasks in the work pane:

- 1. Select the HMC Management node in the Navigation Pane.
- 2. From the Work pane, select the task that you want to perform.
- 3. By default, a categorized listing of the tasks displays. The categories include:
  - Operations
  - Administration

If you want to see that level of the HMC with which you are currently working, point your mouse over **HMC Version** at the top of the work pane as shown in Figure 2-20.

Hardware Management Console	9		21			
		hscroot	Help   Logoff			
Welcome     Gill Systems Management	HMC Management (HMC Version	on Version: 7 Release: 3.1.0 Service Pack: 0	[ Alphabetical List ]			
<ul> <li>Iservers</li> <li>9117-MMA-SN10DD4AC-L10</li> <li>9117-MMA-SN10FFE0B-L9</li> <li>Custom Groups</li> </ul>	View HMC Events · Shut Down or Restart · Schedule Operations ·	Build Level: 20070501.1           Base Version: V7R3.1.0           Model Type: 7310003           Serial Number: 1052DAA           BIOS: 2AKT38RUS				
<ul> <li>Line System Plans</li> <li>Line HMC Management</li> <li>Service Management</li> <li>Updates</li> </ul>	Format Media Back up HMC Data Back up HMC Data Back up HMC Data Back up HMC Data Back up grade Data Change Network Settings Test Network Connectivity View Network Topology Tip of the Day View Licenses Change User Interface Settings Change Date and Time Launch Guided Setup Wizard	<ul> <li>Format a DVD, diskette, or high speed memory key</li> <li>Back up HMC information to DVD, to a remote system, or to a remote site</li> <li>Restore critical HMC data from a remote source</li> <li>Save upgrade data to the HMC hard drive or DVD</li> <li>tings</li> <li>View current network information and change settings</li> <li>tive wetwork diagnostic information about the network protocols for the HMC</li> <li>View network diagnostic information about the network protocols for the HMC</li> <li>View and ping nodes within the HMC network topology</li> <li>Display tips for using the console</li> <li>Read the licenses for the product</li> <li>customize the appearance of the HMC user interface</li> <li>Change the date and time for the HMC</li> </ul>				
Status: Attentions and Events	Administration Change User Password Manage User Profiles and Access Manage Users and Resource Roles Manage Users and Tasks Manage Certificates Remote Command Execution Remote Operation Change Language and Locale Create Welcome Text Manage Data Replication	Change an existing HMC user's password Add, copy, remove, and modify HMC system users and user profiles Add, copy, remove, and modify HMC system users and user profiles View the logged on users and the tasks they are running Create, modify, delete, and import certificates used on the HMC, and view Enable or disable the command line interface on an HMC Enable or disable virtual terminal connections for remotely connected HMC Control whether this HMC can be operated using a web browser from a re Change the HMC user interface language and locale Customize the greeting displayed before logging on Share customizable data between HMCs including custom group data, custom	certificate signing inform sessions mote workstation tomer information, and m			

Figure 2-20 HMC Management

# 2.5.1 View HMC Events

This task shows the console event logs on the HMC. The HMC keeps a log of significant operations and activities automatically, referred to as *console events*, that occur while the application is running. Thus, system events are individual activities that indicate when processes occur, begin and end, and succeed or fail.

When an event occurs, the data and time it occurs and a brief description of the event are recorded in the event log, shown as Figure 2-21.

View HMC Events						
View  Help						
*** * 2 2 🕐 👘 Select Action M						
Date ^	Time	^	Console Event			
05/18/2007	11:23:4	9.690	Remote support call generated on localhost failed at server first(9.3.5.229). Reason: Phone di			
05/18/2007	11:12:0	7.160	Remote support call generated on localhost is being handled by phone server first(9.3.5.229).			
05/18/2007	11:03:3	7.610	User hscroot of session 4 is using user interface "Tree Style".			
05/18/2007	11:03:3	7.010	User hscroot has logged on from location 9.3.4.128 to session id 4. The user's maximum role i			
05/18/2007	11:03:1	1.610	User hscoot attempted to log on with a user identification or password that was not valid.			
05/18/2007	11:03:0	0.760	User hscoot attempted to log on with a user identification or password that was not valid.			
05/18/2007 11:02:08.740 User hscroot attempted to log on with a user identification or password that was not vali						
05/18/2007 11:00:15.260 Remote support call generated on localhost is being handled by phone server js21a1(9.3						
05/18/2007	10:59:3	1.350	Remote support call generated on localhost is being handled by phone server riogrande(9.3.5			
05/18/2007	10:47:3	4.660	HSCE2124 User name root: setkeyoncec 9117-MMA*10FFE0B eafb23b33446ef4c 8 command (			
05/18/2007	10:46:4	2.090	User hscroot of session 3 is using user interface "Tree Style".			
05/18/2007	10:46:4	1.510	User hscroot has logged on from location kr050155.austin.ibm.com [9.41.222.193] to session			
05/18/2007	10:46:2	4.650	HSCE2001 User name object com.ibm.hsc.objmgr.cec.OmCecMgr: New managed system delet			
05/18/2007	10:46:2	1.820	HSCE2001 User name object com.ibm.hsc.objmgr.cec.OmCecMgr: New managed system addir			
05/18/2007	10:40:2	9.600	HSCE2001 User name object com.ibm.hsc.objmgr.cec.OmCecMgr: New managed system addir			
05/18/2007	10:40:2	9.320	HSCE2001 User name object com.ibm.hsc.objmgr.cec.OmCecMgr: New managed system delet			
05/18/2007	10:40:1	7.740	HSCE2001 User name object com.ibm.hsc.objmgr.cec.OmCecMgr: New managed system addir			
05/18/2007	10:40:1	7.720	HSCE2001 User name hscroot: New managed system 192.168.255.253 created.			
05/18/2007	10:39:0	9.980	Starting remote support call 2007-05-18 10:39:03 AM for console localhost(9.3.5.231). Type: (			
05/18/2007	10:39:0	9.900	Remote support call generated on localhost is being handled by phone server localhost(9.3.5.			
			Total: 324 Filtered: 324			

Figure 2-21 View HMC Events

# 2.5.2 Shut Down or Restart

This task enables you to shut down (turn off the console) or to restart the console. To shut down the console, make sure **Restart the HMC** is not selected, then click **OK** to proceed with the shutdown. To restart the console, make sure **Restart the HMC** is selected, then click **OK** to proceed with the shutdown.

# 2.5.3 Schedule Operations

This task creates a defined schedule for certain tasks, such as activating a system or partition using a specific profile, backing up Profile Data, or turning on or off a managed system without operator assistance.

# 2.5.4 Format Media

**Note:** You cannot perform this task remotely unless you have a already placed the media in the system.

This task formats a DVD-RAM, diskette, or high-speed memory key. We explain this task in detail in 12.2.3, "Managing HMC service data" on page 344.

# 2.5.5 Back up HMC Data

Note: This task backs up only the critical data associated with HMC.

This task backs up HMC information to DVD, to a remote system, or to a remote site and is critical to support Hardware Management Console operations. You should back up the HMC data after changes have been made to the HMC or information associated with logical partitions. We explain this task in detail in 11.1, "Critical Console Data backup" on page 304.

Using the HMC, you can back up all important data, such as:

- User-preference files
- ► User information
- ► HMC platform-configuration files
- ► HMC log files
- ► HMC updates through Install Corrective Service

# 2.5.6 Restore HMC Data

You can use this task to select a remote repository for restoring critical backup data for this HMC. You can choose to restore data from an Network File System (NFS) server or an File Transfer Protocol (FTP) server from the Remote Restore of Critical Data window as shown in Figure 2-22. We explain this task in detail in 11.1, "Critical Console Data backup" on page 304.



Figure 2-22 Remote restore of critical data

# 2.5.7 Save Upgrade Data

This task uses a wizard to save all of the customizable data for the HMC to the hard drive or to a DVD before performing an HMC software upgrade. We explain this task in detail in 11.3.6, "Upgrading the HMC machine code" on page 320.

## 2.5.8 Change Network Settings

This task allows you to view the current network information for the HMC and to change network settings. We explain this task in detail in 6.2.2, "LAN Adapters" on page 198.
# 2.5.9 Test Network Connectivity

This task displays network diagnostic information for the console's TCP/IP connection as shown in Figure 2-23.

Test	Test Network Connectivity							
Ping	Interfaces	Address	Routes	ARP	Sockets	TCP	UDP	IP
TCP/IF	Address or	Name to	Ping					
*								
Ping								
Cancel Help								

Figure 2-23 Test Network Connectivity

You can see information concerning the networking configuration on the HMC. There are tabs on this window (Ping, Interfaces, Address, Routes, Address Resolution Protocol (ARP), Sockets, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Protocol (IP)) to scroll through for information. This task also allows you to send a ping to a remote host. You can get additional information when you click **Help**.

# 2.5.10 View Network Topology

You can use this task to see a tree view of the network nodes known to this HMC. Examples of such nodes are managed systems, logical partitions, storage, and other HMCs. When you run this task, you can see the progress window as shown in Figure 2-24.

Network Topolog	/ Progress	
Elapsed time:	00:00:21	
Discovery starting Discovery complete Discovery complete Discovery complete Discovery complete	or local HMC or ethernet ports or managed systems or LPARs	
OK Details	Cancel Help	

Figure 2-24 Network Topology Progress

After finishing this progress, you can view attributes of a node by selecting the node in the tree view that is shown in the left pane under Current Topology as shown in Figure 2-25.

Attributes vary according to the type of node. Some examples are IP address, host name, location code, and status. You can click **Refresh** to rediscover the topology and to query the nodes again for status and other attributes.

This task also allows you to save a snapshot of the current topology and to view that saved reference topology. You can view attributes of a node in this saved topology by selecting the node in the tree view that is shown in the left pane under Saved Topology. To test network connectivity to a node, you can select the node in either the current or the saved topology and click **Ping Current Node** or **Ping Saved Node**, available only for nodes that include an IP address or a host name.

View Network Topology	
Local HMC localhost: Some nodes failed     Local HMC localhost: Some nodes failed     Hanaged System 9117-MMA-SN10DD4AC-L10: Power C     FSP Primary 192.168.255.254: Online     FSP Secondary 192.168.254.255: Online     LPAR doc: Not Available     LPAR doc: Not Available     LPAR DEV: Not Available     LPAR DEV: Not Available     I Par TEST: Not Available     I Ping Current Node Saved Topology	PING 192.168.255.254 (192.168.255.254) 56(84) bytes of data. 64 bytes from 192.168.255.254: icmp_seq=1 ttl=64 time=0.389 ms 64 bytes from 192.168.255.254: icmp_seq=2 ttl=64 time=0.319 ms 64 bytes from 192.168.255.254: icmp_seq=3 ttl=64 time=0.301 ms 64 bytes from 192.168.255.254: icmp_seq=4 ttl=64 time=0.282 ms ✓
Saved: May 18, 2007 2:09:41 PM    Local HMC localhost: Some nodes failed  Interface eth0: Full duplex link  FSP Primary 192.168.255.254: Online FSP Secondary 192.168.254.255: Online LPAR doc: Not Available LPAR BUILD: Not Available LPAR DEV: Not Available I DAR TEST: Not Available	Status: Full duplex link Interface: eth0 Link details: Settings for eth0: Supported ports: [TP] Supported link modes: 10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full Supports auto-negotiation: Yes Advertised link modes: 10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full

Figure 2-25 Network Topology Tree

Table 2-1 is a list of possible statuses for each node.

**Note:** *Unknown* is a possible status for any node where the node has been discovered, but for some reason, the status cannot be determined.

Node	Possible status
Local HMC	All nodes OK, Some nodes failed, All nodes failed (cumulative status of all child nodes)
Remote HMC	Online, Offline
Interface	No link, Half duplex link, Full duplex link
Storage Facility	Status not reported.
Managed System	Managed system status reported by <b>1ssyscfg</b> command (for example, Operating, Running)
FSP	Online, Offline
LPAR	LPAR status reported by <b>1ssyscfg</b> command. LPARs can also carry a Connection status to report their current network status as one of the following Active, On, Off, Offline
BPA	BPA status reported by <b>1ssyscfg</b> command.
BPC	Online, Offline

Table 2-1 Node status

# 2.5.11 Tip of the Day

This task allows you to view information about using the HMC. A different fact or tip display each time you log on. The Tip of the Day window opens as long as the "Show tips each time you log on" option is selected. You can also look at additional information by clicking **Previous Tip** or **Next Tip**. When you are done viewing this window, click **Close**.

If you prefer not to have this window display each time you log on, you can clear the "Show tips each time you log on" option, and then click **Close**.

# 2.5.12 View License

The Licensed Internal Code (LIC) is subject to the IBM Agreement for Licensed Internal Code. LIC does not include programs and code provided under separate license agreements, including but not limited to open source license agreements.

# 2.5.13 Change User Interface Settings

The HMC user interface is made up of several major components: the Banner, the Navigation pane, the Work pane, the Task bar, the Status bar, and the Tasks pad.

This task enables you to customize settings that control how the HMC interface displays, including specific areas such as the user interface components and nodes that display in the Navigation pane as shown in Figure 2-26.

Change User Interface Settings			
Select one or more of the items to display in the user interface:          Banner         Tasks pad         Navigation Icons         Work Pane Icons			
Select one or more of the nodes to display in the navigation pane: <ul> <li>All Partitions node</li> <li>All Objects node</li> </ul>			
Select to save display properties, table configurations, and window geometries: Save settings as my defaults at logoff			
OK Apply Factory Defaults Cancel Help			

Figure 2-26 Change User Interface Settings

# 2.5.14 Change Date and Time

This task enables you to change the time and date of the battery operated HMC clock and to add or remove time servers for the Network Time Protocol (NTP) service as shown in Figure 2-27. The battery operated clock keeps the time and date for the HMC.

Change Dat	te and Time				
Customize Consol	le Date and Time	NTP Configuration			
Battery Operated I	Hardware Manage	ment Console Cloc	.k		
Use this panel to verify or change the date and time on the Hardware Management Console clock. Changing this setting does not change the date/time settings on the managed system or logical partitions managed by this console.					
Select the part of the date or time field that you want to change, or use the custom controls to adjust the date or time. The time setting will automatically be adjusted for daylight savings time in the timezone that you select if the clock is set to UTC.					
Clock:	Local	•			
Time:	2:12:58 PM			Refresh	
Date:	5/18/07				
Time zone:	America/Chicago		•		
OK Cancel H	Help				

Figure 2-27 Change Date and Time

# 2.5.15 Launch Guided Setup Wizard

Note: You cannot perform this task remotely.

This wizard helps you set up your new system and the HMC. To set up your system and HMC successfully, complete all the tasks in the order that the wizard presents them. After you complete this wizard, you can use the properties for an object to make changes. We explain these tasks in detail in 3.2.2, "Using the HMC Guided Setup wizard" on page 80.

#### 2.5.16 Locking the HMC screen

To lock the HMC screen, open the Lock HMC Screen task from the HMC Management work pane. The HMC screen is locked immediately.

To unlock the screen and return to the HMC workplace, press Enter and specify the password for the user ID for which you are logged in.

# 2.5.17 Opening a 5250 console

Use this task to open a 5250 emulator session so you can communicate with an i5/OS logical partition.

To open a 5250 console, open the Open 5250 Console task from the HMC Management work pane. The 5250 Setup window displays. From the 5250 Setup window, you can configure and start your 5250 emulator.

# 2.5.18 Open Restricted Shell Terminal

Use this task to acquire a command line session.

To open a restricted shell terminal, open the Open Restricted Shell Terminal task from the HMC Management work pane. The Restricted Shell window displays. From the Restricted Shell window, you can issue commands remotely through secure shell access to the managed system. This provides consistent results and automates administration of managed systems.

# 2.5.19 Launch Remote HMC

You can use this task to start a session to another HMC.

To open another HMC:

- 1. Open the Launch Remote Hardware Management Console task from the HMC Management work pane.
- 2. From the Remote Hardware Management Console Addressing Information window, specify the TCP/IP address or host name of the remote HMC to be contacted.
- 3. Click **OK** to proceed.

# 2.5.20 Change User Password

You can change the HMC access password. After the password is changed, it must be changed on all other systems assessing this HMC. We explain this task in detail in 5.2.1, "Changing the user password" on page 185.

#### 2.5.21 Manage User Profiles and Access

This task manages system users who log on to the HMC. We explain this task in detail in 5.2.2, "Managing user profiles and access" on page 185.

# 2.5.22 Manage Task and Resource roles

This task is used to define and customize managed resource roles and task roles. We explain this task in detail in 5.2.3, "Customizing user task roles and managed resource roles" on page 190.

# 2.5.23 Manage Users and Tasks

This task display the list of users currently logged on and the list of all tasks running in this system. We explain this task in detail in 5.2.3, "Customizing user task roles and managed resource roles" on page 190.

# 2.5.24 Manage Certificates

This task manages the certificates that are used on the HMC. It provides the capability of getting information about the certificates that are used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates or signing certificates. We explain this task in detail in 5.1, "Certificate management" on page 178.

# 2.5.25 Remote Command Execution

You can use this task to enable remote command execution using the ssh facility.

# 2.5.26 Remote Virtual Terminal

A *Remote Virtual Terminal* connection is a terminal connection to a Logical Partition from another remote HMC. You can use this task to enable Remote Virtual Terminal access for remote clients.

#### 2.5.27 Remote Operation

This task controls whether the HMC can be operated using a Web browser from a remote workstation. By default, remote browser access to the HMC is disabled. This task allows you to enable or disable remote browser access easily.

# 2.5.28 Change Language and Locale

This task sets the language and location for the HMC. After you select a language, you can select a locale that is associated with that language. The language and locale settings determine the language, the character set, and other settings specific to the country or region (such as formats for date, time, numbers, and monetary units).

# 2.5.29 Create Welcome Text

You use this task to customize the welcome message or to display a warning message that opens before users log on to the HMC as shown in Figure 2-28. The text that you enter in the message input area for this task displays in the Welcome window after you initially access the console. You can, therefore, use this text to notify users of certain corporate policies or security restrictions that apply to the system.

Create Welcome Text			
To display a custom welcome message or warning to a user before logon, enter the text below. Since you are accessing the console remotely, you can also copy and paste the text from another program, to save typing. You are limited to 8,192 characters of input.			
Automatically reflow text (use a blank line for a new paragraph).			
Clear			
Remaining characters available for welcome text: 8192			
Classification: (optional)			
OK Reset Cancel Help			

Figure 2-28 Create Welcome Text

# 2.5.30 Manage Data Replication

This task enables or disables customized data replication. *Customized data replication* allows another HMC to obtain customized console data from or to send data to this HMC.

#### Note:

- Customizable console data is accepted from other HMCs only after specific HMCs and their associated allowable customizable data types have been configured.
- Before enabling this replication service, you might want to save your original data settings in case you need to restore these settings in the future.

The Customizable Data Replication service provides the ability to configure a set of HMCs to replicate any changes automatically to certain types of data so that the configured set of HMCs keep this data synchronized without manual intervention.

You can configure the following types of data:

- Customer information data
  - Administrator information (customer name, address, telephone number, and so forth)
  - System information (administrator name, address, or telephone of your system)
  - Account information (customer number, enterprise number, sales branch office, and so forth)
- Group data
  - All user-defined group definitions
- Modem configuration data
  - Configure modem for remote support.
- Outbound connectivity data
  - Configure local modem to RSF
  - Enable an internet connection
  - Configure to an external time source.

Manage Data Replication				
Customizable Data Replication				
🖲 Enable 🛛 Disable				
Data Source(s) Co	ustomiz	able Data Types		
HMC ^	Select	Data Types		
		Customer Information Data		
New		Group Data		
Delete		Modem Configuration Data		
~		Outbound Connectivity Data		
Local Customizable Data Change Warnings Select the customizable data types that should generate warnings when that type of data is manually changed on this Hardware Management Console and are also configured to be replicated from one or more data sources.				
Select Data Warning Types				
Customer Information	n Data			
Group Data				
Modem Configuration	Modem Configuration Data			
Outbound Connectivit	y Data			
Save Push to Slaves Sync from Master Status Cancel Help				

Figure 2-29 shows the types of customizable console data that can be replicated.

Figure 2-29 Manage Data Replication - Customizable Data Replication

You can enable the Customizable Data Replication service for the following types of operations:

#### Peer-to-peer replication

Provides automatic replication of the selected customized data types between peer HMCs. Changes made on any of these consoles are replicated to the other consoles.

#### Master-to-subordinate replication

Provides automatic replication of the selected customized data types from one or more designated master HMCs to one or more designated subordinate HMCs. Changes made on a masters console are replicated automatically to the subordinate consoles.

#### Configuring peer-to-peer replication

Figure 2-30 illustrates the process to configure peer-to-peer replication.



Figure 2-30 Peer-to-peer replication

To configure peer-to-peer replication, follow these steps:

- 1. Open the Manage Data Replication task. The Configure Customizable Data Replication window opens.
- 2. Select Enable in the Configure Data Replication panel.
- 3. The Configure Customizable Data Replication window opens.
- 4. Click **New** under Data Source(s). The Configure New Replication Source window opens.
- 5. Select an HMC to be used as a data source from the Discovered Console Information list, and click **Add**.

Alternatively, you can enter the TCP/IP address of the HMC that you want to use as a data source in the TCP/IP Address Information field, and then click **Find**.

- 6. The Customizable Data Replication window opens again as shown in Figure 2-29 on page 65.
- Select the types of data that you want to replicate from the Customizable Data Types list, from a peer HMC that is selected currently under Data Source(s).
- 8. Click Save to close the Customizable Data Replication window.
- 9. Repeat steps 1 through 8 on each of the HMCs that you want to act as peers with one another.

When communication is established between the HMCs, the requested types of customizable data are replicated automatically from one HMC to the other immediately following the change in the data itself.

# Configuring master-to-subordinate replication

Figure 2-31 illustrates the process to configure master-to-subordinate replication.



Figure 2-31 Master-to-subordinate replication

To configure master-to-subordinate replication involves two steps:

- 1. Setting up a master console.
- 2. Setting up the subordinate console.

#### Setting up a master console

To set up a master console:

- 1. Open the Manage Data Replication task. The Customizable Data Replication window opens.
- 2. Select Enable in the Configure Data Replication panel.
- 3. Click **Save** to close the Customizable Data Replication window.

**Note:** If you want to configure additional master consoles, see "Configuring peer-to-peer replication" on page 66.

#### Setting up the subordinate console

To set up the subordinate console:

- 1. Open the Manage Data Replication task. The Customizable Data Replication window opens.
- 2. Select Enable in the Configure Data Replication panel.
- 3. The Customizable Data Replication window open.
- 4. Click **New** under Data Source(s). The Configure New Replication Source window opens.
- 5. Select a HMC to be used as a data source from the Discovered Console Information list, and click **Add**.

Alternatively, you can enter the TCP/IP address of the HMC that you want to use as a data source in the TCP/IP Address Information field, and then click **Find**.

- 6. The Customizable Data Replication window opens again as shown in Figure 2-29 on page 65.
- 7. Select the types of data that you want to replicate from the Customizable Data Types list, from a peer HMC selected currently under Data Source(s).
- 8. Click Save to close the Customizable Data Replication window.
- 9. Repeat steps 1 through 8 on each of the HMCs that you want to act as peers with one another.

When open communication is established between the HMCs, the requested types of customizable data are replicated automatically from one HMC to the other immediately following the change in the data itself.

# 3

# **Installing the HMC**

To set up the Hardware Management Console (HMC), you must complete the following groups of tasks:

- Cabling the HMC to the managed server
- Gathering configuration settings for your installation and configuring the HMC
- Connecting managed systems to the HMC

The HMC can be a stand-alone HMC or an HMC that you plan to install in a rack.

This chapter provides an overview of these tasks.

# 3.1 Cabling the HMC

Attention: Do not plug the power cords into electrical outlet until you are instructed to do so.

This section discusses how to connect the HMC cables, connect the Ethernet cable, and connect the HMC to a power source. You can use these instructions to help you cable your rack-mounted or stand-alone HMC.

To cable the HMC:

1. Use the specifications for the HMC to help ensure that you position the HMC in the correct location. HMC specifications provide detailed information for your HMC, including dimensions, electrical power, temperature, environment, and service clearances.

Choose from the following options:

- a. If you are installing a rack-mounted HMC, continue with step 2.
- b. If you are installing a stand-alone HMC, skip to step 3 on page 72.
- 2. To install a rack-mounted HMC:
  - a. First, identify the location of the connectors:
    - A rack-mounted HMC 7310-CR4 (Figure 3-1)
    - A rack-mounted HMC 7310-CR3 (Figure 3-2)
    - A rack-mounted HMC 7310-CR2 (Figure 3-3)



Figure 3-1 Back view of a rack-mounted HMC 7310-CR4



Figure 3-2 Back view of a rack-mounted HMC 7310-CR3



Figure 3-3 Back view of a rack-mounted HMC 7310-CR2

- b. Next, install the HMC into a rack.
- c. After the HMC is installed into a rack, connect the monitor, keyboard, and mouse.

For connection to a HMC 7310-CR2, connect the keyboard and display to the C2T-to-KVM (keyboard, video, and mouse) adapter that you have attached previously to the HMC. The mouse is integrated with the keyboard. If your keyboard and mouse use USB connections, you can also connect them to the USB ports on the front panel of the HMC.

For connection to a HMC 7310-CR3, connect the keyboard, display, and mouse using the USB conversion option cable.

After you complete these steps, then skip to step 4 on page 77.

- 3. If you are installing a stand-alone HMC:
  - a. First, identify the location of the connectors:
    - A stand-alone HMC 7310-C06 (Figure 3-4 on page 73)
    - A stand-alone HMC 7310-C05 (Figure 3-5 on page 74)
    - A stand-alone HMC 7310-C04 (Figure 3-6 on page 75 and Table 3-1 on page 75)
    - A stand-alone HMC 7310-C03 (Figure 3-7 on page 76 and Table 3-2 on page 77)



Figure 3-4 Back view of a stand-alone HMC 7310-C06



Figure 3-5 Back view of a stand-alone HMC 7310-C05



Figure 3-6 Back view of a stand-alone HMC 7310-C04

Table 3-1 describes the physical ports of this HMC hardware platform.

Table 3-1 Description of stand-alone HMC 7310-C04

No.	Description
1	PCI Connectors (slot 1 to left)
2	PCI Express (x1) connector
3	PCI Express (x16) graphic connector
4	Ethernet connector
5	USB connector
6	Mouse connector
7	Parallel connector

No.	Description
8	System connector
9	Diagnostic LEDs
10	Power connector
11	Audio line-out connector
12	Audio line-in connector
13	VGA monitor connector
14	System connector
15	Keyboard connector
16	USB connectors



Figure 3-7 Back view of a stand-alone HMC 7310-C03

Table 3-2 describes the physical ports of this HMC hardware platform.

No.	Description
1	Power connector
2	Mouse connector
3	Parallel connector
4	USB connectors
5	Ethernet connector
6	Audio line in connector
7	PCI slots (slot 1 to right)
8	AGP slot
9	Audio line-out connector
10	Microphone connector
11	USB connector
12	VGA monitor connector
13	System connector
14	Keyboard connector

 Table 3-2
 Description of stand-alone HMC 7310-C03

- b. Attach the monitor cable to the monitor connector and tighten the screws. Attach the power cord to the monitor. Ensure that the voltage selection switch on the HMC is set to the voltage that is used in your area. The voltage selection switch is red and is located near the power connector. Move the switch so that the voltage that is used in your area is displayed.
- c. Plug the power cord into the HMC, and then connect the keyboard and mouse. For USB connections, connect the keyboard and mouse to USB ports on the HMC. You can connect the keyboard and mouse to the USB ports on the front or back panels. For PS/2 connections, connect the keyboard and mouse to their connector on the back panel of the HMC.
- 4. Connect the modem. During the installation and configuration of the HMC, the modem might dial out automatically as the HMC follows routine call-out procedures.
- 5. Connect the Ethernet (crossover) cable from the HMC to the managed server. Your HMC should be connected to the managed server in a private service DHCP network. Your Ethernet connection to the managed server

must be made using the Ethernet port that is defined as eth0 on your HMC. If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, use the primary integrated Ethernet port. If you have installed additional Ethernet adapter in the PCI slots, see Table 3-3 to determine which Ethernet port you must use.

HMC type	Rules for Ethernet placement
Rack-mounted	The HMC supports only one additional Ethernet adapter. If an additional Ethernet adapter is installed, that port is defined as eth0. In this case, the primary integrated Ethernet port is then defined as eth1, and the secondary integrated Ethernet port ID defined as eth2. If no adapters are installed, the primary integrated Ethernet port is defined as eth0.
Stand-alone model 7310-C04	<ul> <li>The definitions depend on the type of Ethernet adapter you have installed:</li> <li>If only one Ethernet adapter is installed, whether it is a 1 Gigabit Ethernet adapter or 10/100 Mbps Ethernet adapter, that adapter is defined as eth0.</li> <li>If both a 10/100 Mbps adapter and a 1 Gigabit Ethernet adapter are installed, the 1 Gigabit Ethernet adapter is always defined as eth0.</li> <li>If two 10/100 Ethernet adapters are installed, the adapter in slot 1 is defined as eth0.</li> <li>If two 1 Gigabit Ethernet adapters are installed, the adapter in slot 1 is defined as eth0.</li> </ul>
Stand-alone model 7310-C03	<ul> <li>The definitions depend on the type of Ethernet adapter you have installed:</li> <li>The 1 Gigabit Ethernet adapter is generally defined as eth0. One exception is when it is placed in slot 1, however this placement is not recommended.</li> <li>If multiple 1 Gigabit Ethernet adapters are installed, the configuration is defined in the following order: slot 2 is eth0, slot 3 is eth1, and the integrated Ethernet port is eth2.</li> <li>If adapters other than the 1 Gigabit Ethernet adapters are installed, the integrated Ethernet port is always defined as eth0.</li> </ul>

Table 3-3 HMC types and associated rules for Ethernet placement

- 6. If you use an external modem, plug the modem power supply cord into the HMC modem.
- 7. Plug the power cords from the monitor, HMC, and HMC external modem into electrical outlets.

This completes the section for cabling of the HMC.

Attention: Do *not* connect the managed system to a power source at this time.

# 3.2 Configuring the HMC using the HMC Guided Setup wizard

The HMC Guided Setup wizard helps you to set up your system and the HMC. The wizard launches automatically the first time that you start the HMC. This wizard is the easiest way to configure the HMC.

**Important:** When installing a new Server p system, do not turn on the system before connecting it to an HMC. The service processor on a Server p system is a DHCP client and will search for a DHCP server (the HMC) to obtain its IP address. If no DHCP server can be found, the service processor will assign a default IP address and simple communication with the HMC will be prevented. If this occurs, you will have to change the IP setting of the service processor manually.

To configure the HMC successfully, you must understand related concepts, make decisions, and prepare information. The Guided Setup helps you to configure the following functions:

- Change HMC date and time
- Change HMC passwords
- Create additional HMC users
- Specify contact information
- Configure connectivity information
- ► Authorize users to use Electronic Service Agent<sup>™</sup> and configure notification of problem events

After you complete this wizard, you can use the properties for an object to make changes.

# 3.2.1 The HMC Guided Setup wizard checklist

Use this checklist to make sure that you have collected the information that you need to complete the HMC Guided Setup wizard.

- Language and Locale
- Date and time zone
- □ HMC IDs and passwords
- □ HMC users and roles
- Contact information
- □ HMC network settings
- □ Media speed
- □ Private or open network
- □ HMC service and support
- □ Service Agent registration
- □ SMTP

# 3.2.2 Using the HMC Guided Setup wizard

This section provides a step-by-step guide to setting up the HMC using the HMC Guided Setup wizard. Make sure that you have completed the HMC Guided Setup wizard checklist before continuing with this section.

#### Set up language and locale

Before starting the HMC Guided Setup wizard, set up your language in one of the 42 supported languages or the default of US English. After you select a language, you can select a locale associated with that language. The language and locale settings determine the language, the character set, and other specific to the country or region such as the formats for date, time, numbers, and monetary units.

Figure 3-8 shows how to set up the language and locale. After you accept the new setting, you must log off the HMC and log on again. You can change the language at anytime, but you must log off the HMC then log on again.

Change Lan	guage and Locale	
Select the lar	nguage and locale to use on the HMC.	
Language:	English	
Locale:	en_US American English(ISO-8859-1)	-
en_PK Pakistani English(ISO-8859-1)		
	en_US American English(ISO-8859-1) en_ZA South African English(ISO-8859-1)	

Figure 3-8 Change Language and Locale

Note: In some languages, not all words are translated.

# Launching the HMC Guided Setup wizard

The HMC Guided Setup wizard launches automatically when you first start the HMC. You can also launch the wizard from the HMC desktop using the following steps:

1. Log on to the HMC with the default system administrator user ID *hscroot* with its default password *abc123*.

2. In the Work Pane, click **Guided Setup Wizard** (Figure 3-9).

Hardware Manage	ement Console	hscroot   Help   Logoff		
🖿 Welcom e	Welcome (HMCVersion)			
☑ ④ System s Management System Plans	Use the Hardware Management Console (HMC) to manage this HMC as well as servers, logical partitions, managed systems, and other resources. Click on a link in the navigation pane at the left.			
HMC Management	🗐 Systems Management	Manage servers, logical partitions, managed systems, and frames; set up, configure, view current status, troubleshoot, and apply solutions.		
Service Management	System Plans	Import, deploy, and manage system plans on the HMC.		
🖏 Updates	📕 HMC Management	Perform management tasks to set up, configure, and customize operations associated with this HMC.		
	Service Management	Perform service tasks to create, customize and manage services associated with this HMC.		
	🔯 Updates	Perform and manage updates on your system.		
	Status Bar	View details of status and messages.		
	Additional Resources			
	💼 Guided Setup Wizard	Provides a step-by-step process to configure your HMC.		
	HMC Operations Guide (View as HTML)	Provides an online version of Operations Guide for the Hardware Management Console and Managed Systems for system administrators and system operators using the HMC.		
	<sup>6d°</sup> HMC Readme	Provides hints and errata information about the HMC.		
	Online Information	Additional related online information.		
Status: Open Serviceable Evi				

Figure 3-9 HMC Welcome screen

3. The Launch Guided Setup Wizard - Welcome page opens (Figure 3-10). Click **Next** to continue with the Guided Setup wizard.



Figure 3-10 Launch Guided Setup Wizard - Welcome page

4. In the Launch Guided Setup Wizard - Change HMC Date and Time page, enter the correct date and time and time zone for your location (Figure 3-11). This information is typically the time zone for the server, assuming that the HMC is the local machine. For a remote machine, you should choose the correct time zone according your location. Click **Next** to continue with the Guided Setup wizard.

Launch Guided Setup Wizard - Change HMC Date and Time.				
	You can change th affect the systems a be adjusted for dayl Note: Changes to t	ou can change the date, time and time zone of the HMC. Changing these settings does not fect the systems and logical partitions the HMC manages. The time setting will automatically e adjusted for daylight savings time in the time zone you select. lote: Changes to the time zone do not take effect until the wizard has been completed.		
	Date: Time: Time zone:	5/1/07 11:33:16 AM America/Chicago		•
Help				Back Next Finish Cancel

Figure 3-11 Launch Guided Setup Wizard - Change HMC Date and TIme

5. The Launch Guided Setup Wizard - Change *hscroot* Password window displays as shown in Figure 3-12. Enter the new *hscroot* password that you would like (normally the default password ID *abc123*). Use of the *hscroot* user ID to access the user interface and to manage the HMC.

Use these following password rules:

- The password must contain at least seven characters.
- The characters should be standard 7-bit ASCII characters.
- These characters include the characters A-Z, a-z, 0-9, and many special characters such as tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign (\$), percent sign (%), caret (^), ampersand (&), asterisk (\*), left and right parentheses (), underscore (\_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), backslash (\), colon (:), quotation mark ("), semicolon (;), and apostrophe (').
- Passwords can include special characters, but passwords must begin with an alphanumeric character.

Launch Guid	Launch Guided Setup Wizard - Change hscroot Password			
You need to change the predefined password for the default user ID of hscroot. The original password is published in the documentation. For sign-on security, it needs to be changed immediately.				
	Enterth	e new password.		
New pass	croot word:	•••••		
Re-type n password:	ew	••••••		
Role:		hmcsuperadmin		
Help			Back Next Finish Cancel	

Figure 3-12 Launch Guided Setup Wizard - Change hscroot Password

You should change the *hscroot* default password as soon as possible as security issue.

6. The Launch Guided Setup Wizard - Change root password panel displays as shown in Figure 3-13. Enter the new *root* password that you would like (normally the default password ID *passw0rd* where 0 is the number zero). You should use *root* password rules same as *hscroot* password rules before. A service provider uses the *root* user ID to perform maintenance on the server.

Launch Guided Setup Wizard - Change root Password			
	You need to change the predefined password for the default use password is published in the documentation. For security reason immediately. The root user ID cannot be used to log in to the con- situations where advanced support services are required for your Enter the new password.	ID of root. The original s, it needs to be changed sole, but it may be needed in HMC.	
User ID: root         New password:         •••••••         Re-type new password:			
Help	E	ack Next Finish Cancel	

Figure 3-13 Launch Guided Setup Wizard - Change root Password

7. The Launch Guided Setup Wizard - Create Additional HMC Users panel displays as shown in Figure 3-14. You can optionally create new HMC users. In this example, we create a new hscoperator user ID with role as hmcoperator. Refer to 5.2, "HMC user management" on page 184 for further information about users and roles. You can also skip this step and create users manually later.

Launch Guided Setup	Wizard - Create Additional HMC Users
Optionall password creating a	y, you can create additional HMC users. Enter the user login name and the twice. Select a role for this user. A user can have only one role. To continue without new user, click Next.
User ID: User name: New password: Re-type new passwo	hscoperator •••••• rd:
Roles: hmcservicerep hmcviewer hmcoperator hmcpe hmcsuperadmin	
Help	Back Next Finish Cancel

Figure 3-14 Launch Guided Setup Wizard - Create Additional HMC Users

8. The Launch Guided Setup Wizard - Create Additional HMC Users panel displays (see Figure 3-15). If you want to create more users, then select **Yes**, otherwise select **No** and click **Next** to continue with the Guided Setup Wizard.

Launch Guided Setup Wizard - Create Additional HMC Users			
Luunon cui			
	Would you like to create another new HMC user?		
	<ul> <li>○ Yes, I'd like to create another user.</li> <li>● No.</li> </ul>		
Help	Back Next Finish Cancel		

Figure 3-15 Launch Guided Setup Wizard - Create Additional HMC Users

9. This completes the first part of the Guide Setup Wizard. The Launch Guided Setup Wizard - The Next Steps panel displays as shown in Figure 3-16.

Launch Guided Setup Wizard - The Next Steps			
	You have completed the following: • Set HMC date and time • Change the passwords of the predefined HMC user IDs • Create new HMC user IDs		
	Next, you will do the following (available locally only): • Configure HMC network settings		
	To complete the configuration of network settings, you may need to obtain certain information from your network administrator, if you haven't already. Click Help for a list of the information you need to gather. This task is available from the local HMC only.		
	Click Next to continue.		
Help	Back Next Finish Cancel		

Figure 3-16 Launch Guided Setup Wizard - The Next Steps

The next step configures the HMC network settings. You might need to discuss this step with your network administrator for HMC environment.

10. The Launch Guided Setup Wizard - Configure HMC Network Settings panel displays as shown in Figure 3-17. In our example, we see two LAN adapters available (*eth0* and *eth1*), although you might only see one adapter in your HMC system.

We show you how to configure the HMC for both a private network and an open network. We use the first Ethernet network card (eth0) for a private network, then return to this panel again to configure eth1 for an open network. We use the private network to connect the HMC with our managed systems and other HMCs. We use the second Ethernet card (eth1) for an open network.

Launch Guided Setup Wizard - Configure HMC Network Settings			
Select one LAN adapter to configure on your HMC.			
If you have more than one LAN adapter listed, you can configure remaining adapters when you are finished configuring the one you selected.			
Note: After you complete the wizard, you can configure remaining adapters or change already configured adapters. Do this by customizing network settings from HMC Configuration.			
Select         LAN Adapter         Type           •         eth0 (192.168.128.1) 00:11:25:06:40:46         Ethernet           •         eth1 (9.3.5.230) 00:0D:60:0B:38:56         Ethernet			
Help Back Next Finish Cancel			

Figure 3-17 Launch Guided Setup Wizard - Configure HMC Network Settings

Select LAN adapter eth0 to be configured first, then click **Next** to continue with the Guided Setup wizard.

11. The Launch Guided Setup Wizard - Configure eth0 Media Speed panel displays (Figure 3-18). You can choose the LAN adapter speed at Autodetection for initial setup, or you can set the adapter speed if you know the information.

Launch Gu	ided Setup Wizard - C	onfigure eth0 (192.168.128.1) 00:11:25:06:40:46
2	You can specify the r 00:11:25:06:40:46.	nedia speed of the ethernet adapter eth0 (192.168.128.1)
	Media speed:	★ Autodetection Autodetection 10Mbps Half Duplex 10Mbps Full Duplex 100Mbps Full Duplex 100Mbps Full Duplex 1000Mbps Full Duplex 1000Mbps Full Duplex 1000Mbps Full Duplex
Help		Back Next Finish Cancel

Figure 3-18 Launch Guided Setup Wizard - Configure eth0 Media Speed

For this example, we set Autodetection. Click **Next** to continue with the Guided Setup wizard.
12. The Launch Guided Setup Wizard - Configure eth0 Private Network panel displays as shown in Figure 3-19. As mentioned previously, we set the LAN adapter eth0 as a private network to connect to our managed systems.

Launch Gui	ded Setup Wizard - Configure eth0 (192.168.128.1) 00:11:25:06:40:46
	Do you want to set up a private or open network?
2	<ul> <li>Private network A network restricted to HMCs and the systems they manage.</li> </ul>
	Open network An open network contains other network endpoints besides the HMCs and the managed systems, and may span across multiple subnets and network devices.
Halp	Back Next Einish Cancel
Help	Back INext Filisii Calcel

Figure 3-19 Launch Guided Setup Wizard - Configure eth0 Private Network

In this example, we select the Private Network. Then, click Next to continue.

13. The Launch Guided Setup Wizard - Configure eth0 DHCP panel displays (see Figure 3-20). We have to define the HMC as a DHCP server so our managed system is assigned an IP address by the DHCP server.



Figure 3-20 Launch Guided Setup Wizard - Configure eth0 DHCP

The HMC becomes DHCP server to all clients in a private network. These clients will be our managed systems and other HMCs. You can configure the HMC to select one of several different IP address ranges to use for this DHCP server, so that the addresses provided to the managed systems do not conflict with addresses used on other networks to which the HMC is connected.

We have some standard nonroutable IP address ranges that are assigned to its clients. The ranges that can be selected are:

- 192.168.128.2 192.168.255.254
- 172.16.0.3 172.16.255.254
- 172.17.0.3 172.17.255.254
- 10.0.0.2 10.0.0.254
- 10.0.128.2 10.0.143.254
- 10.0.255.2 10.0.255.254
- 10.1.0.2 10.1.15.254
- 10.1.255.2 10.1.255.254
- 10.127.0.2 10.127.15.254
- 10.127.255.2 10.127.255.254
- 10.128.0.2 10.128.15.254
- 10.128.128.2 10.128.128.254
- 10.128.240.2 10.128.255.254
- 10.254.0.2 10.254.0.254
- 10.254.240.2 10.254.255.254
- 10.255.0.2 10.255.0.254
- 10.255.128.2 10.255.143.254
- 10.255.255.2 10.255.255.254

The HMC LAN adapter eth0 will be assigned one before the first IP address out of the range selected. In our example, we select the 192.168.0.2 to 192.168.255.254 range, so our HMC is given an IP address 192.168.0.1. Any other client (HMC or managed system) is given an address from this range.

The DHCP server in the HMC uses automatic allocation, which means that each managed system will be reassigned exactly the same IP address each time it is started. The DHCP server uses each client's built in Media Access Control (MAC) address to ensure that it will reassign each client with same IP address as before. When a managed system starts, it will try to contact the DHCP server to obtain its IP address. If the managed system is unable to contact the HMC DHCP server then the managed system will use its last given IP address.

We set the IP address range 192.168.0.2 to 192.168.255.254 and click **Next** to continue.

14. The Launch Guided Setup Wizard - Configure HMC Network Settings panel displays (Figure 3-21). This completes the network configuration for LAN adapter eth0 as a private network. We can proceed with network configuration for LAN adapter eth1 as an open network.

Launch Guided Setup Wizard - Configure HM	C Netwo	rk Settings	
Do you want to configure another • Yes, I want to configure another LAN adapt • No.	r LAN ada er or chai	apter? nge an already configure	d adapter.
Note: After you complete the wizard, you can c configured adapters. Do this by customizing ne	configure twork set	remaining adapters or ch tings from HMC Configur	ange already ation.
Select LAN Adapter	Туре	Configured this session	
eth0 (192.168.128.1) 00:11:25:06:40:46	Ethernet	¥	
	Luieniet		
Help		Back	Finish Cancel

Figure 3-21 Launch Guided Setup Wizard - Configure HMC Network Settings

Select **Yes** option and LAN adapter eth1 should be selected. Click **Next** to continue with the Guided Setup wizard.

15. The Launch Guided Setup Wizard - Configure eth1 Media Speed panel is then displayed (Figure 3-22). As the eth0 configuration before, you can leave the LAN adapter speed at Autodetection for initial setup, or you can set the LAN adapter speed if you know the information.

Launch Gui	ded Setup Wizard - Config	gure eth1 (9.3.5.230) 00:0D:60:0B:38:56
2	You can specify the mec 00:0D:60:0B:38:56.	dia speed of the ethernet adapter eth1 (9.3.5.230)
	Media speed:	★ Autodetection Autodetection 10Mbps Half Duplex 10Mbps Full Duplex 100Mbps Half Duplex 100Mbps Full Duplex 1000Mbps Full Duplex 1000Mbps Full Duplex 1000Mbps Full Duplex
Help		Back Next Finish Cancel

Figure 3-22 Launch Guided Setup Wizard - Configure eth1 Media Speed

16. The Launch Guided Setup Wizard - Configure eth1 Open Network display is now shown (Figure 3-23). As mentioned previously, we select Open network for eth1.

Launch Guid	ded Setup Wizard - Configure eth1 (9.3.5.230) 00:0D:60:0B:38:56
	Do you want to set up a private or open network?
2	O Private network A network restricted to HMCs and the systems they manage.
	<ul> <li>Open network An open network contains other network endpoints besides the HMCs and the managed systems, and may span across multiple subnets and network devices.</li> </ul>
Help	Back Next Finish Cancel

Figure 3-23 Launch Guided Setup Wizard - Configure eth1 Open Network

17. The Launch Guided Setup Wizard - Configure eth1 IP Assignment panel is shown in Figure 3-24. We can configure interface eth1 to obtain an IP automatically from your DHCP server or to use a fixed IP address.

Launch Gui	uided Setup Wizard - Configure eth1 (9.3.5.230) 00:0D:60:0	)B:38:56		
T.	You can have IP addresses assigned to the HMC automatically or you can specify the IP addresses to use.			
_2==	Do you want to obtain an IP address automatically?			
	<ul> <li>Yes, obtain an IP address automatically.</li> <li>No. Use the specified address.</li> </ul>			
	TCP/IP interface address: 9.3.5.230			
	TCP/IP interface network mask: 255.255.254.0			
Help	Back	Next Finish Cancel		

Figure 3-24 Launch Guided Setup Wizard - Configure eth1 IP Assignment

In our example, we configure the interface eth1 using fixed IP address, 9.3.5.20 with network mask 255.255.254.0. Click **Next** to continue with the Guided Setup wizard.

18. The Launch Guided Setup Wizard - Configure eth1 Firewall panel is now displayed as shown in Figure 3-25. Commonly, there is a firewall that controls access from outside to your network. Since the HMC is connected to an open network, we can also restrict outside access to the HMC by using built in firewall in HMC. There are some applications that running on the HMC, that can be secured from unauthorized outside access.

Launch Gui	ded Setup Wizard - Configure HMC Firewall for eth1 (9.3.5.230) 00:0D:60:0B:38:56
2	HMC firewall settings create a security barrier that allows or denies access to specific network applications on the HMC. These control settings can be specified individually for each physical network interface, allowing you control over which HMC network applications can be accessed on each network.
Recommend	Would you like to configure HMC firewall settings for this adapter?
	<ul> <li>Yes, I'd like to configure HMC firewall settings for this adapter.</li> <li>No.</li> </ul>
Help	Back Next Finish Cancel

Figure 3-25 Launch Guided Setup Wizard - Configure eth1 Firewall

We select **Yes** to configure HMC firewall settings and click **Next** to continue with the Guided Setup wizard.

19. The Launch Guided Setup Wizard - Configure HMC Firewall for eth1 panel displays then (see Figure 3-26). In the top panel are listed all the available applications that are on the HMC, and in the bottom panels are listed all applications that available to open network through the HMC firewall.

You can allow an application to pass through the firewall by selecting them from the top panel then clicking **Allow Incoming** or **Allow Incoming by IP address**. *Allow incoming* allows all remote clients access to the selected application, and *Allow Incoming by IP address* only allows specific remote clients' IP addresses to the selected application. You can select to remove an application completely from the firewall by selecting the application from the bottom panel then click **Remove**.



Figure 3-26 Launch Guided Setup Wizard - Configure HMC Firewall for eth1

20. The Launch Guided Setup Wizard - Configure HMC Network Settings panel is shown (see Figure 3-27). If you have more network adapters available, you can configure them now by selecting the adapters and the **Yes** radio button.

Launch Guided Setup Wizard - Configure HMC Network Settings				
Do you want to configure another LAN adapter?      O Yes, I want to configure another LAN adapter or change an already configured adapter.     O No.				
Note: . configu	After you complete the wizard, you can ured adapters. Do this by customizing n	configure etwork set	remaining adapters or change tings from HMC Configuration	e already 1.
Select	LAN Adapter	Туре	Configured this session	
0	eth0 (192.168.128.1) 00:11:25:06:40:46	Ethernet	✓	
0	eth1 (9.3.5.230) 00:0D:60:0B:38:56	Ethernet	✓	
	7			
Help			Back Next	Finish Cancel

Figure 3-27 Launch Guided Setup Wizard - Configure HMC Network Settings

Because our both network adapters have been configured, we select **No**, then click **Next** to continue with the Guided Setup wizard.

21. The Launch Guided Setup Wizard - Configure HMC Host Name and Domain panel displays as shown in Figure 3-28. Enter your host name for the HMC, domain name and description for the HMC. In our example, we enter host name *localhost* and domain name *localdomain*.

Launch Guided Setup Wizar	d - Configure HMC Network Settings
You need to ide	ntify your HMC to the network.
What is the HM	C host name, domain name, and description of your HMC?
HMC host name:	* localhost
Domain name:	localdomain
Description of HMC:	
Help	Back Next Finish Cancel

Figure 3-28 Launch Guided Setup Wizard - Configure HMC Host Name and Domain

22. The Launch Guided Setup Wizard - Configure HMC Gateway panel is shown (see Figure 3-29). If, required, we can specify one of our LAN adapters as a gateway device to an open network.

Launch Gu	ided Setup Wizard - Configure HMC	Network Settings
	To define a default gateway, fill in the TCP/IP address to be used for routing IP packets. Also, specify whether any open adapter can be used as the gateway device to communicate with the default gateway or select a specific adapter to be used.	
	Gateway address:	9.3.4.1 (for example: nnn.nnn.nnn)
	Gateway device:	eth 1
Help		Back Next Finish Cancel

Figure 3-29 Launch Guided Setup Wizard - Configure HMC Gateway

In our example, eth1 is the gateway device to an open network. Click **Next** to continue with the Guided Setup wizard.

23. The Launch Guided Setup Wizard - Configure DNS panel displays now (Figure 3-30).

A DNS server is a distributed database for managing host names and their IP addresses. By adding a DNS server, the HMC will allow us to find other hosts in our open network by their host name rather than by their IP addresses.

Enter the IP address of your DNS server or servers in the DNS server address field and click **Add** to register the IP address. You can enter multiple DNS server addresses here, and the order that the addresses are entered will be the order in which they are searched when trying to resolve a host name.

If you make a mistake when entering an address, you can remove it by selecting the entry and then clicking **Remove**.

Launch Guided Setup Wizard - Configure DNS	
The Domain Name System (DNS) is used to provide a locating IP-based computers. By defining DNS servers, identify servers and HMCs rather than IP addresses.	a standard naming convention for s, you can use host names to
Determine if you want to enable DNS. If DNS is enable addresses. Addresses are searched in the order they a	led, specify the DNS server are listed.
Do you want to use DNS?	
Addresses, Addresses are searched in the order they are listed.  Do you want to use DNS?      Yes, I want to use DNS by defining DNS servers.      DNS server search order:      DNS server address:      Add      934.2      Remove      No, I do not want to use DNS.	
Help	Back Next Finish Cancel

Figure 3-30 Launch Guided Setup Wizard - Configure DNS

24. The Launch Guided Setup Wizard - Configure Domain Suffix panel is shown in Figure 3-31.

Enter a domain suffix in the Domain suffix field and click **Add** to register your entry. You can enter multiple domain suffixes for your organization if you have them. The order that the addresses are entered will be the order in which they are searched when trying to map the host name to a fully qualified host name.

If you make a mistake when entering an address, you can remove it by selecting the entry and then clicking **Remove**.

	Add the domain suff unqualified names for	xes you are using. These r DNS searches. Suffixes	e are the suffixes for the s are searched in the orde	HMC to append to er they are listed.
Domain su	iffix:	Add Remove		
Help			Back Next	Finish Cancel

Figure 3-31 Launch Guided Setup Wizard - Configure Domain Suffix

25. The Launch Guided Setup Wizard - The Next Steps panel displays (see Figure 3-32). This completes the network configuration section of the Guided Setup wizard. We now continue with the next part of the wizard.

Launch Gui	ided Setup Wizard - The Next Steps
	You have completed the following (available locally only):
2	Configure HMC network settings
	Next, you will do the following:
	<ul> <li>Specify customer contact information for service-related activities</li> <li>Configure connectivity for service-related activities</li> <li>Authorize users to use Service Agent</li> </ul>
	Click Next to continue.
Help	Back Next Finish Cancel

Figure 3-32 Launch Guided Setup Wizard - The Next Steps

26. The Launch Guided Setup Wizard - Specify Contact Information panel is shown (see Figure 3-33). This is the first of three panels which contains the contact details for your organization. The information entered here is used by IBM when dealing with problems electronically reported (calling home), as well as software updates. You should enter valid contact information for your own location. The fields marked with an asterisk (\*) are mandatory and must be completed.

· Contact information: — Company name:	* IBM	
Administrator name:	* IBM Administrator	
Email address:	admin@ibm.com	
Phone number:	* 88888888	
Alternate phone numbe	17: 333333333	
Fax number:	111222333	
Alternate fax number:	666777888	

Figure 3-33 Launch Guided Setup Wizard - Specify Contact Information

27. The Launch Guided Setup Wizard - Specify Contact Address panel is displayed in Figure 3-34. It is the second Contact Information panel. You should enter your contact address information about this panel. Again, you must complete the mandatory fields (\*). Use the drop-down menus to select your Country/Region and State/Province settings.

Contir	tup Wizard - Specify Contact Information	of the HMC.	
<i>Contact Address:</i> Street address 2: City or locality: Country or region: State or province: Postal code:	* IBM Road  * Austin  * United States (of America)  * Texas * 88888		
Help		Back	Next Finish Cancel

Figure 3-34 Launch Guided Setup Wizard - Specify Contact Address

28. The Launch Guided Setup Wizard - Location of the HMC panel is displayed (see Figure 3-35). It is the last panel for the Contact Information. You should enter the location details of this HMC here. If the location address is the same as the contact address used in the previous step, then click **Use the administrator mailing address**. Otherwise enter the correct HMC location address details.

Continue completing the information about the log	n ocation of the HMC.
Location of the HMC:	
Use the administrator mailing address	
Otreet address. IBM Road	
Street address 2:	
City or locality: * IBM	
Country or region: *United States (of America)	<b>~</b>
State or province: * Texas	
Postal code: * 78758	
Hain	Back Next Finish Cancel
нер	Back Next Finish Cancel

Figure 3-35 Launch Guided Setup Wizard - Location of the HMC

In our example, we use the same address for both contact and HMC, so we selected the Use the administrator mailing address. This completes the contact information part of the HMC Guided Setup wizard service and support. Click **Next** to continue with the Guided Setup wizard.

29. The Launch Guided Setup Wizard - Configure Connectivity to Your Service Provider panel is now shown in Figure 3-36.

You can configure an outbound connection between the HMC and your service provider, such as your service provider's remote support facility. You can specify how the local HMC connects to your service provider from a local modem, an Internet Secure Sockets Layer (SSL), an Internet Virtual Private Network (VPN), or a remote pass-through system.

- A local modem enables you to use the modem on your HMC to send problem information and system data to your service provider.
- An Internet SSL enables you to use a high speed Internet connection on your HMC, the fastest option, to send problem information to your service provider.
- An Internet VPN enables you to use a high speed Internet connection on your HMC to send problem information to your service provider.
- A remote pass-through system enables you to use another HMC or a logical partition on your server to send problem information to your service provider.

Launch Gui	ded Setup Wizard - Configure Connectivity to Your Service Provider
Q	To help ensure your HMC can take advantage of support for service-related reasons, you need to set up connectivity with your service provider.
123	What type of connection or connections do you want to set up to contact your service provider?
	Connection types:
	Dial-up from the local HMC Allows you to configure the use of the local modem to connect from the local HMC to your service provider.
	Secure Sockets Layer (SSL) through the Internet Allows you to configure the use of encrypted SSL over an existing Internet connection to connect from the local HMC to your service provider.
	✓ Virtual Private Network (VPN) through the Internet Allows you to configure the use of a VPN over an existing Internet connection to connect from the local HMC to your service provider.
	Connecting through other systems or partitions Allows you to configure the HMC to pass through to other systems or partitions by specifing their TCP/IP address or host name.
Help	Back Next Finish Cancel

Figure 3-36 Launch Guided Setup Wizard - Configure Connectivity to Your Service Provider

You can select by the communications method to which you want to connect to IBM for service and support related functions. In our example, we select all four connectivity options for demonstration purposes only. Normally you would only select the options valid for your environment.

Click **Next** to continue with Guided Setup.

30. The Agreement for Service Programs panel is displayed (see Figure 3-37). You should read the agreement details carefully and click **Accept** or **Decline** 

You agree to allow International Business Machines Corporation and its subsidiaries to store and use your contact information, including names, phone numbers, and e-mail addresses, anywhere they do business. Such information will be processed and used in connection with our business relationship, and may be provided to contractors, Business Partners, and assignees of International Business Machines Corporation and its subsidiaries for uses consistent with their collective business activities, including communicating with you (for example, for processing orders, for promotions, and for	

Figure 3-37 Agreement for Service Programs

In our example, we click **Accept** to accept the terms and conditions of the IBM Agreement for Service Programs which then opens the window shown in Figure 3-38.

Launch Guided Setup Wizard - Notificatio	on of Problem Events
Launch Guided Setup Wizard - Notification         Add the email addresses that we SMTP server:         9.3.5.200         Email addresses to be notified:         Select Email Address Errors to Add         Edit         Remove	on of Problem Events will be notified when problem events occur on your system Port: 25 be Notified
Help	Back Next Finish Can

Figure 3-38 Launch Guided Setup Wizard - Notification of Problem Events

31.We enter our SMTP server information and also add the e-mail address for notifications. We then click **Next**, which opens the Launch Guided Setup Wizard - Configure Dial-up from the Local HMC panel shown in Figure 3-39.

Launch Guided Setup Wizard - Configure Dial-up from the Local HMC				
Configure the local modem if you haven't already done so by clicking Modem Configuration. Next, you need to specify which telephone numbers to use to dial your service provider. Click Add to select telephone numbers from a list or manually add telephone numbers. When connecting, the telephone numbers will be dialed in the order listed.				
Modem:       Dial prefix:   Modem Configuration				
Phone numbers (in order of use):         Select Phone Number Comment         Down         Add         Edit				
Help Back Next Finish Cancel				

Figure 3-39 Launch Guided Setup Wizard - Configure Dial-up from the Local HMC

32. In the panel, click **Modem Configuration** to set the modem parameters. The Modem Configuration display opens (Figure 3-40). You can set the Dial Type (Tone/Pulse), Wait for dial tone, Enable speaker, and the Dial prefix value.

Modem Configuration				
● Tone ● Pulse				
Other Settings Wait for dial tone Enable speaker Dial prefix:				
OK Cancel Help				

Figure 3-40 Modem Configuration

33. Click **OK** to continue with the Guided Setup wizard. Then click **Add** in the Phone numbers panel to add the IBM support service phone number. The Add Phone Number - Country or Region window display (Figure 3-41). Use the drop-down menus to select your country or region and then your state or province.

Add Pho	ne Numi	ber			
Select a p	redefined	phone number or enter	on	e manually	
Select a pi	reuenneu	phone number of enter	on	e manually.	
Available	predefine	d numbers:			
Country o	or region:	United States (of Ameri	ca	) 🗸	
State or p	rovince:	Texas	•		
Select Ph	hone Nur	Ohio	^		
0 32	25-691-64	Oklahoma			
0 28	31-249-21	Oregon			
0 46	69-656-01	Puerto Rico			
0 80	06-881-00	Rhode Island			
0 28	31-204-22	South Carolina			
<ul> <li>51</li> </ul>	2-691-44	South Dakota			
<u> </u>	2-691-60	Tennessee		▼	
- Numbert	to he adde	Texas			
Dial	0	Utan Verment	_	0-601-4495	
prefix:	3	Virginia		-091-4403	
Comment	: Austin	Washington	=		
Note: You	i can edit	West Virginia	=	sary for example to remove the area	
code.	a ourr our	Wisconsin		bury, for example, to remove the area	
		Wyoming	~		
Add Cancel Help					

Figure 3-41 Add Phone Number - Country or Region

In our example we select **United States (of America)** for our Country/region and **Texas** for our State/province. You should select the relevant values for your location.

34. The Add Phone Number panel is shown in Figure 3-42. After you have selected your Country/region and State/province, a list of available IBM support service numbers are listed. You should select the phone number nearest to your location. The phone number will then be populated in the Phone number field at the bottom of the panel. You can also manually add phone numbers if you know your IBM support service number.

Click Add to continue with the Guided Setup wizard.

Countr	y or region:	Unit	ed States (of A	merica)	•
State o	r province:	Теха	is	•	
Select	Phone Nun	nber	Comment		
۲	512-691-44	85	Austin		
0	512-691-60	05	Austin		
0	281-885-90	05	Bammel		
0	940-448-16	605	Bartonville		
0	512-581-80	)10	Bastrop		
0	979-318-33	395	Bay City		
0	832-514-34	23	Baytown		
Numb	er to be adde	d: —			
Dial prefix:	9		Phone number:	* 512-691-4485	
Comme	ent: Austin				

Figure 3-42 Add Phone Number

35. The Launch Guided Setup Wizard - List of Dial-up Number window is now displayed (Figure 3-43). You can add additional phone numbers by repeating the same procedure again and selecting a different number.

Launch Guided Setup Wizard - Configure Dial-up from the Local HMC					
Configure the local modem if you haven't already done so by clicking Modem Configuration. Next, you need to specify which telephone numbers to use to dial your service provider. Click Add to select telephone numbers from a list or manually add telephone numbers. When connecting, the telephone numbers will be dialed in the order listed.					
Dial prefix:  Modem Configuration					
Phone numbers (in order of use):       Select Phone Number Comment       • 512-691-4485 Austin       Add       Edit         Remove					
Help Back Next Finish Cancel					

Figure 3-43 Launch Guided Setup Wizard - List of Dial-up Number

36. This finishes our configuration for the Dial-up connection for the HMC. Click **Next** to continue. The Launch Guided Setup Wizard - Configure SSL using an Existing Internet Connection panel as shown in Figure 3-44.

Launch Guided Setup Wizard - Configure SSL using an Existing Internet Connection						
If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by encrypted Secure Sockets Layer (SSL) using the existing Internet connection.						
Use SSI Prox	Access					
Address:	* 9.3.5.233	Port: * 443				
Authenticate v User:	vith the SSL Proxy					
Password:	*					
Re-type password	1:* •••••••					
Help		Back	Next Finish Cancel			

*Figure 3-44 Launch Guided Setup Wizard - Configure SSL using an Existing Internet Connection* 

37. Select **Use SSL Proxy**, then enter SSL Proxy address and the port. You also can authenticate with the SSL Proxy by selecting **Authenticate with the SSL Proxy** then enter the user and password for the SSL Proxy. You should have the information from your network administrator. Click **Next** to continue with the Guided Setup wizard. The Launch Guided Setup Wizard - Use VPN using an Existing Internet Connection panel is now shown (Figure 3-45).

Launch Guid	led Setup Wizard - Use VPN using an Existing Internet Connection
	If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by virtual private network (VPN) using the existing Internet connection.
Help	Back Next Finish Cancel

Figure 3-45 Launch Guided Setup Wizard - Use VPN using an Existing Internet Connection

38. We click **Next** to accept the VPN connection for our HMC support services and continue with the Guided Setup wizard. The Launch Guided Setup Wizard - Configure Connectivity using a Pass-Through System panel is shown in Figure 3-46. The HMC can use another system in your network which already has a VPN or dial-up connection to IBM service and support.

Launch Guided Setup Wizard - Configure Connectivity using a Pas	s-Through System
You need to add the IP addresses or host names of the solution by the HMC when connecting to the service provi called pass-through systems. Click Add to select IP addresses or host names from a lis connecting, the IP addresses or host names will be used	ystems and partitions passed der. These systems or partitions are t or manually add them. When in the order listed.
Pass-through systems (in order of use):	
Down	
Add Edit Bemove	
Help	Back Next Finish Cancel

Figure 3-46 Launch Guided Setup Wizard - Configure Connectivity using a Pass-Through System

39.Click **Add** to continue with the Guided Setup wizard. The Add Pass-through System panel is shown in Figure 3-47.

Add Pass-through Sy	stem
Enter the TCP/IP addres modem or VPN.	s or host name of the system hosting a
IP address or host name:	* 9.3.5.228
Comment:	Another HMC connected to IBM
Add Cancel Help	

Figure 3-47 Add Pass-Through System

40.Enter the IP address or host name of your pass-through system. Type some comment text and click **Add** to accept the values entered. You can add multiple pass-through systems here. The order listed is the order in which the pass-through systems are used. The Launch Guided Setup Wizard - Pass-through System window displays (see Figure 3-48). It shows the list of the pass through systems.

Launch Guided Setup Wizard - Configure Connectivity using a Pass-Through System
You need to add the IP addresses or host names of the systems and partitions passed through by the HMC when connecting to the service provider. These systems or partitions are called pass-through systems. Click Add to select IP addresses or host names from a list or manually add them. When connecting, the IP addresses or host names will be used in the order listed.
Pass-through systems (in order of use):
Select IP Address or Host Name Comment
9.3.5.228 Another HMC connected to IBM     Down
Add Edit Remove
Help Back Next Finish Cancel

Figure 3-48 Launch Guided Setup Wizard - Pass-Through System

41. Click **Next** to continue with the Guided Setup wizard. The Launch Guided Setup Wizard - Authorize Users for Electronic Service Agent panel displays as shown in Figure 3-49.

You can see the information that is collected and sent to IBM by the HMC on the IBM Electronic Service Agent Web site:

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

To access this data on the Web, you must have a registered IBM ID and authorized that ID through the HMC. You can register IBM IDs through the following Web site:

## https://www.ibm.com/registration/selfreg

Enter a valid IBM ID and an optional second IBM ID if required, in the Web authorization panel. The Guided Setup only allows you to authorize two user IDs to access the data sent by the HMC to IBM.

Launch Gu	ided Setup Wizard - Authorize Users for Electronic Service Age	nt
123	IBM provides personalized Web functions that use information coll Service Agent. To use these functions, you must first register on the at: https://www.ibm.com/account/profile. To authorize users to use the Electronic Service Agent information functions, enter one or two of the IBM IDs which you registered on t website.	ected by IBM Electronic IBM Registration website to personalize the Web he IBM Registration
	BM ID	admin1@ibm.com
	Optional IBM ID	admin2@ibm.com
	Note: Use the user ID registered on the IBM Registration website.	
	To view details of the systems and to perform further user ID mainte http://www.ibm.com/support/electronic.	enance, go to
Help	В	ack Next Finish Cancel

Figure 3-49 Launch Guided Setup Wizard - Authorize Users for Electronic Service Agent

42. Click **Next** to continue with the Guided Setup wizard. The Launch Guided Setup Wizard - Notification of Problem Events panel is displayed (Figure 3-50). The HMC can alert your administrator of problems with the HMC or its managed systems through e-mail.

You can choose whether to notify your administrators of only problems reported to IBM (only call-home problem events) or of all problem events generated.

Enter the IP address and port of your SMTP server. Then click **Add** continue.

	<b>.</b>	1 11				
Launch Guided	Setup Wiza	rd - Notification o	f Problem Eve	nts		
Add	I the email a	ddresses that will	be notified whe	n problen	n events occur o	on your system.
-23=	rr server.	9.3.5.200		2	25	
Emai	l addresses	to be notified:				
Selec	ct Email Ad	dress Errors to be	Notified			
Add.	Edit	Remove				
Help					Back Next	Finish Cancel

Figure 3-50 Launch Guided Setup Wizard - Notification of Problem Events

43. The Add Email Address panel displays, as shown in Figure 3-51. Enter your administrator's e-mail address and the notification type required.

Add Email Address
Email address: admin1@ibm.com
Notification options:
<ul> <li>Only call-home problem events</li> </ul>
○ All problem events
Add Cancel Help

Figure 3-51 Add Email Address

Click **Add** to accept these values and return to the previous panel. You can enter multiple e-mail addresses by repeating this process.

44. The Launch Guided Setup Wizard - Notification of Problem Events window is displayed (Figure 3-52). It displays the e-mail address of administrator for notification of problem events.

	Add the em	ail addresse	s that will be no	tified when pro	blem ever	nts occur on	your system.
23	server:	9.3.5.200		FO	25		
	Email addre	sses to be no	tified:				
	Select Emai	Address	Errors to be N	otified			
	o admi	n1@ibm.com	Call-home				
	Add Edit	Remove					

Figure 3-52 Launch Guided Setup Wizard - Notification of Problem Events
45. Click **Next** to continue with the Guided Setup wizard. The Launch Guided Setup Wizard - Summary window displays (Figure 3-53). You can see all the changes that the Guided Setup wizard configures later. At this stage, nothing has actually been changed on the HMC. You can cancel the changes by clicking **Cancel**.

Launch Guided Setup Wizard - Summary	
Congratulations! You have completed the Guided S the following:	Setup Wizard. Click Finish to configure
The HMC date/time Setting has been successfully changed.	
Change password for HMC user hscroot Change password for	
Create user ID hscoperator with role hmcoperator	
The following network settings will be updated For LAN adapter eth0 (192,168,128.1) 00:11:25:06:40:46:	
Committing contact information	
Committing connectivity	
The IBM ID admin1@ibm.com and optional second IBM ID	
Help	Back Next Finish Cancel

Figure 3-53 Launch Guided Setup Wizard - Summary

Click **Finish** to apply the changed configurations.

**Note:** At this step, nothing has changed on the HMC. If you click **Cancel**, all changes by Launch Guided Setup Wizard will be lost.

46. The Launch Guided Setup Wizard - Status panel displays (see Figure 3-54). If every task completes, its status is updated automatically.

Γ	Launch Guided Setup Wizard - Status			
	The following shows the Guided Setup tasks you specified and the status of each. The Status column indicates if the task completed successfully, is still pending, or failed. Click the View Log button for additional details.			
	Coloct	You can close this window at any time. The tasks will continue to run.	Otatua	
	Select	I dsk Description	Status	all a
	0	Change HMC bale and Time.	Successiul	
l	0	Change HMC passwords	Successiul	
	0	Create additional HMC users	Successiul	
	0	Conligure HMC Hetwork setungs	Successiul	
	0	Specily contact information	Successiul	
	0	Configure connectivity information Authorize years to year Electropic Service Agent and configure patification of problem system	Successiul	
		Additionize users to use Electronic Service Agent and configure notification of problem events	Succession	<b>V</b>
	He	elp Back Next Finish C	ancel	

Figure 3-54 Launch Guided Setup Wizard - Status

47. You can review the log by clicking **View Log**. This log is useful if for any reason you have task that have a failed status. Figure 3-55 shows an example of the log file output.



Figure 3-55 The launch Guided Setup Wizard - Status Log

48.Click **OK** to return to previous panel, then click **Close** to continue with the Guided Setup wizard.

If you have configured the HMC network settings during the Guided Setup Wizard, then you will probably receive a message asking you to log off the HMC and log on again to apply some of changes as shown in Figure 3-56.

1 Information
Some of the changes will not go into effect until you log off the HMC and log
HSCW0016

Figure 3-56 The Launch Guided Setup Wizard - Information

49. Click **OK** to log off from the HMC then log on back to apply some changes.

This completes the HMC Launch Guided Setup Wizard.

#### Post Guided Setup Tasks

If you were not able to set up all the information through the wizard, you can go back and use the standard HMC menu to complete tasks. If you are direct connected to the HMC, some tasks could be missed at first.

### 3.3 Connecting managed systems to the HMC

Attention: When installing a new System p system, do not turn on the system before connecting it to an HMC. The server processor (SP) on a System p system is a DHCP client and will search for a DHCP server to obtain its IP address. If no DHCP server can be found, then the SP assigns a default IP address. If this occurs, you have to use ASM to change the IP setting of the SP manually.

After you have completed the HMC Guided Setup Wizard, you can connect your managed systems to the HMC by using following steps:

- 1. Connect your HMC to the HMC port of the managed system with an Ethernet cable.
- 2. Connect the managed system to a power source. The managed system will then turn on its service processor. After the service processor is turned on, proceed to the next step. This process would take three to five minutes. You can see the following sequence of events signals that power has been applied to the service processor:
  - a. Progress indicators, also referred as checkpoints, show on the control panel display while the system is being started. The display might appear blank for a few moments during this sequence.
  - b. When the service processor has completed its power on sequence, the green power light blinks slowly and the output on the control panel is similar to the following:

```
01 N V=F
T
```

3. Click **Systems Management**, then **Servers** to view the status of your managed system. It can take a few minutes for the status to display.

4. If the status shows *Pending Authentication*, you need to set passwords for the managed system. The HMC prompts you to set passwords for the managed system. If you are not prompted by the HMC to set those passwords, click **Operations** then **Change Password**. The window for setting passwords opens as shown in Figure 3-57. Set the password for each as directed.

Update Password - Authentication Passed
Authentication passed for the managed system below. Managed system name : 9117-MMA-SN10DD4AC-L10 You may change the HMC Access password at this time using the fields below. Once changed, you must update the HMC Access password for all the other Hardware Management Consoles from which you want to access this managed system.
Current HMC Access password: New HMC Access password: Verify HMC Access password: Click OK to change the password or Cancel to quit the process.
OK Cancel Help

Figure 3-57 Update Password - Authentication Passed

**Note:** If you did not configure your HMC as a Dynamic Host Configuration Protocol (DHCP) server, the HMC will not detect the managed system automatically.

5. Access the ASMI to set the time of day on the system. Refer to 14.6.3, "Time of Day" on page 446 to set the time of day on the system.

- Start the managed system by clicking Systems Management → Servers, select the managed system that you want to turn on, then click Operation, Power On as shown in Figure 3-58. There are three options for turning on the system:
  - a. Partition standby allows you to create and activate logical partitions. When the partition standby power on is completed, the system is in standby mode.
  - b. System profile turns on the system according to a predefined set of system profiles. Select the system profile that you want to use from the list.
  - c. Partition auto start turns on the managed system to partition standby and then activate all partitions that are marked as auto start or those partitions that were running when the system shut down.

Power Op - 9117-MMA-SN10DD4AC-L10
To power on the managed system, select one of the power on options below and click OK. You must specify a system profile if you choose the System Profile power on option
<ul> <li>Power On Options</li> <li>Partition standby</li> <li>System profile</li> <li>Partition auto start</li> </ul>
System Profiles Select a system profile below that contains the partitions that you want to have activated when the managed system is powered on.

Figure 3-58 Power on the managed system

This completes the instructions for installing the HMC.

# 4

# System plans and the HMC

This chapter introduces another important aspect of managing system plans. You can use the Hardware Management Console (HMC) to create import, export, view, create, remove, and deploy system plans. The HMC code level must be at Version 7 Release 3.1 or later, and it must include the latest service packs. The HMC provides a set of graphical user interfaces (GUIs) for these LPAR management functions.

**Note:** If you are connecting to the HMC from a PC workstation, there is no longer a requirement to install WebSM on the PC. You must access the HMC with Version 7.3 installed through a Web browser, not WebSM.

This chapter reviews the operations of each of these GUI interfaces for managing system plans, also referred to as *sysplans*. All of the utilities are available through the HMC graphical interface. Some functions are also available through the restricted shell, commonly referred to as the *command-level interface* (CLI). We do not document how to use the command-line functions that have not changed since they were documented in *LPAR Simplification Tools Handbook*, SG24-7231. You can find a list of these command-line functions and information about those command-line functions that have been added or changed in 4.3.3, "System plans management using restricted shell (CLI)" on page 171.

# 4.1 System plans

A system plan, also referred to as *sysplan* because of the .sysplan file extension, is a representation of the hardware and partition configuration currently on a system or the plan for deployment of hardware and configuration of partitions on a system, depending on how the sysplan file is generated:

- If the sysplan file is generated from an existing POWER5 or POWER6 system using the HMC, the file reflects the actual LPAR configuration of the server at that point in time if all the partitions are active. There is less detail if one or more partitions are not active.
- If the sysplan is generated by the System Planning Tool (SPT), the file reflects the intended LPAR configuration for a target server. The sysplan includes details on partition allocations of memory, processors, and the hardware required for each partition.

Hardware allocations can be defined as owned by the partition, and therefore required for the partition to activate. The only other choice is for the hardware to be defined as shared, in which case the hardware is optional for the partition, which can be activated without the hardware. Shared hardware can be switched between dynamically two or more partitions.

The sysplan also includes general information about the system, such as system type and model, total number of processors present and the number that are activated, and the total installed and activated memory. It has detailed information about the card slots in the processor enclosure and any I/O expansion towers or I/O drawers that will attach to the processor enclosure. The card slots are shown as empty, or occupied by IOP or IOA feature codes, and this level of detail is used for the hardware validation during the LPAR deployment process.

Note that at this time the sysplan file created by SPT includes device-level detail (for example, what type and number of disk units are attached to a storage controller IOA). In contrast, a sysplan created by the HMC does not, by default, include any detail of what is attached to and controlled by an IOA. For more information about this, refer to "Enabling hardware inventory collection from active partitions" on page 142.

A sysplan file is a composite object, which means that it could possibly include many files. The file's description is imbedded in the file, as is the file level and last modifying application information. When a sysplan file is created on the HMC or imported using the HMC GUI, the file is stored on the HMC in a predefined directory. The directory path is /opt/hsc/data/sysplan.

# 4.2 Using the HMC graphical user interface

In the HMC workplace window, *System Plans* is where you can access the graphical interfaces that you use to manage system plans on the servers directly from the HMC or remotely using the Web browser based client connecting to the HMC (see Figure 4-1).

Hardware Management Cor	nsole	
		hscroot Help Logoff
🗇 Welcom e	Welcome (HMC Version)	
System Plans HMC Management	Use the Hardware Management Console ( logical partitions, managed systems, and of at the left.	HMC) to manage this HMC as well as servers, ther resources. Click on a link in the navigation pane
욊 Service Management 없고 Updates	🕄 System s Managem ent	Manage servers, bgical partitions, managed systems, and frames; set up, configure, view current status, troubleshoot, and apply solutions.
	System Plans	Import, deploy, and manage system plans on the HMC.
	📕 HMC Management	Perform management tasks to set up, configure, and customize operations associated with this HMC.
	Service Management	Perform service tasks to create, customize and manage services associated with this HMC.
	🔂 Updates	Perform and manage updates on your system.
	En Status Bar	View details of status and messages.
	Additional Resources	
	Guided Setup Wizard	Provides a step-by-step process to configure your HMC.
	HMC Operations Guide	Provides an online version of Operations Guide for the Hardware Management Console and Managed
	(View as HTML)	operators using the HMC.
	HMC Readme	Provides hints and errata information about the HMC.
	Online Information	Additional related online information.
Status: Attentions and Events		

Figure 4-1 The HMC Welcome page

To display the system plans management tasks window, click **System Plans** (Figure 4-2). The upper section of this window lists all the system plans currently residing on the HMC. The buttons above the list lets you select and deselect, sort, filter, manage the columns of the display table, and perform tasks on selected system plans. The task options are repeated in the lower Tasks section of the main system plans management screen. Note that with no system plan selected, the only options are to import a system plan or to create a system plan.

Hardware Management Co	nsole						
						hscroot Help	Logoff
⊟ Welcome Brû∰i System s Managem en t Man System Plans	Contents of	of: System Plans	e 🖻	Tasks •			
HMC Management	Select ^	Name ^	Description ^	Source ^	Version ^	Last Modified Date ^	
Åå Service Management		🗎 9sysvics.sysplan		IBM System Planning Too	SPT 1.2	Apr 27, 2007 11:31:57 AM	<b>^</b>
©_J Updates		🗈 april19.sysplan		HMC V7R3.1.0.0	HMC 1.2	Apr 19, 2007 2:09:32 PM	=
		🗎 april19_2.sysplan		HMC V7R3.1.0.0	HMC 1.2	Apr 19, 2007 2:15:15 PM	
		🗈 current.sysplan	HMC created	HMC V7R3.1.0.0	HMC 1.2	Apr 30, 2007 2:25:07 PM	
		📓 JC01.sysplan	JC01	HMC V7R3.1.0.0	HMC 1.2	Apr 24, 2007 8:38:04 AM	-
		Total: 7	Filtered: 7 Sele	cted: 0			
	Tanka: Su	atom Diana					
	Tasks: Sy	System Plan					
Status: Attentions and Events	Import	System Plan					

Figure 4-2 The main system plan management page

Using the HMC you can:

- Create a system plan
- ► View a system plan
- Deploy a system plan
- Export a system plan
- Import a system plan
- Remove a system plan

You can save a system plan created using the HMC interface as a record of the hardware and partition configuration of the managed system at a given time.

You can deploy an existing system plan to other systems that this HMC manages that have hardware that is identical to the hardware in the system plan.

You can export and system plan to another HMC (which imports the plan) and use it to deploy the system plan to other systems the target HMC manages that have hardware that is identical to the hardware in the system plan.

You have the option to view, create, deploy, export, import, or remove a system plan. Note that these tasks can be selected in either the Tasks drop-down menu or the Tasks links in the lower part of the right frame. The following sections provide more details for each option.

Figure 4-3 shows a common starting point for each example. In our first example we have selected a system plan named *9sysvios.sysplan*.

Hardware Management Cor	nsole			OSS /EL	
				hscroot Help	Logoff
Welcom e Given System s Managem ent System Plans HMC Managem ent Service Managem ent Updates	Contents of: System Plans	P      P	n 12 12 12 HMC 12	Last Modified Date  Apr 27, 2007 11:31:57 AM Apr 19, 2007 2:09:32 PM Apr 19, 2007 2:15:15 PM Apr 30, 2007 2:25:07 PM Apr 24, 2007 5:38:04 AM May 2, 2007 5:21:45 PM	
Status: Attentions and Events	Tasks: 9sysvios.sysplan View System Plan Greate System Plan Depicy System Plan Export System Plan Import System Plan Remove System Plan				

Figure 4-3 The system plan management page with a system plan selected

#### 4.2.1 Importing a system plan to the HMC

You can load a system plan that was created using the SPT or created on another HMC using the import operation. You can import the system plan from one of the supported media types, such as CD, DVD, diskette, a USB device such as a memory card, a remote FTP site, or a PC connected to the HMC through a browser connection.

When you import a system plan, you first need to prepare the media, if needed. Then, you import the sysplan file. From the System Plans task menu, select **Import System Plan**, which opens the Import System Plan prompt window. Identify the system plan file name and whether you are importing it from media, an FTP server, or, if you are accessing the HMC through a PC-based Web browser, the sysplan file can be on that PC. In our example (Figure 4-4), the system plan file is stored on a USB flash drive. The name of the file is newConfig.sysplan, and the file was initially created using SPT and saved to the flash drive. The directory path to access the file on the flash drive is /media/sysdata.

Import Syste	em Plan	
You can impor sources.	rt a system plan file to your HMC from the following	
Select the source of the sourc	urce of the system plan file	
from media f	System plan <sup>*</sup> newConfig.sysplan file name: Sub- directory on	
O Import from a remote FTP	nedia.	
f	System plan* ile name: Remote site * hostname: User ID: *	]
	Password: *	

Figure 4-4 Import System Plan window

A successful import results in the conformation message shown in Figure 4-5.

Import System Plan Successful
Import of file newConfig.sysplan successful.

Figure 4-5 Importing a sysplan file success

#### 4.2.2 Exporting a system plan from the HMC

You can export system plans that reside on the HMC to media, an FTP server, or, if you are using a PC to access the HMC through a browser, to a directory on the PC. The process is very much like the importing of a sysplan file. If you are exporting to media, you need to format that media for use with the HMC.

#### Preparing the media

To export to external media, that media must be in a format that is available to the HMC. The easiest method is using the Format Removable Media task:

- 1. Select HMC Management from the left navigation frame.
- 2. Select **Format Media** in the right window to open the media selection box as shown in Figure 4-6.

Format Media
Select the desired media format.
Format DVD-RAM
○Format diskette
Format high-speed memory key
OK Cancel Help

Figure 4-6 Format Media

If you have a USB memory key, insert it in a USB slot on the HMC.

If you have a diskette or CD that needs to be formatted, insert it into the disk or CD drive.

- 3. Select the correct device to format and click **OK**. The memory format process starts and completes.
- 4. Insert the media into the PC and load the system plan file using the save function in SPT or by browsing to the file and copying the sysplan file to the media.

#### Exporting the system plan

From the starting point shown in Figure 4-3 on page 137, follow these steps:

- 1. Select a system plan to export.
- 2. Click **Export System Plan** either from the Tasks drop-down menu or the content Tasks link in the lower portion of the window. A dialog box opens asking where you want to export the system plan (Figure 4-7). In our example, the name of the sysplan file is april19.sysplan and the target is media/USBstick directory.

Export Sys	tem Plan
You can expo destinations. System plan name:	ort a system plan file from your HMC to the following file * april19.sysplan
<ul> <li>Select the de</li> <li>○ Export to</li> <li>○ Export to</li> <li>media</li> </ul>	estination of the system plan file this computer from the HMC Sub-directory on media: media/USBstick
○Export to a remote FTP site	Remote site *
	hostname: User ID: *
	Remote directory:
	Export Cancel Help

Figure 4-7 Export System Plan window

3. Click **Export** to initiate the export process. A results window with a success indication or an error message indicates the result of the export.

#### 4.2.3 Creating a system plan on the HMC

You can create a system plan for a system that is controlled by the HMC. The system plan has information about the current partition definitions and hardware allocations. Processor, memory, and PCI cards are identified in the system plan, even if they are not owned by a partition.

#### Notes:

- 1. Hardware controlled through an IOA controller, such as disk units and external media devices, will not be represented in the system plan unless the owning partition is running. For more information, see "Enabling hardware inventory collection from active partitions" on page 142.
- You cannot import the sysplan file that the HMC creates into the SPT to edit it. The sysplan file can only be deployed and viewed either on the HMC on which the file was created or an HMC to which the file has been moved.

From the starting point in Figure 4-3 on page 137, follow these steps:

- 1. Select Create System Plan.
- 2. The Create System Plan window prompts you for the system name, sysplan file name, a description, and a choice to view the system plan after creation, as shown in Figure 4-8.

Create System	Plan
Specify the mana the system plan d	ged system, the system plan name to create, and escription.
Managed svstem:	* RCHAS60-SN10F26EA ▼
Śystem plan name:	* Feb30.sysplan
Plan description:	System configuration on Feb 30th
🗹 View system p	plan after creation
	Create Cancel Help

Figure 4-8 Create System Plan window

3. After you have entered the requested information, click Create.

4. Following the successful creation of a system plan, a message displays (Figure 4-9) and the system plan is now in the list of plans on the HMC. Click **OK**.

0	Create System Plan Successful
Crea syste SN10 ОК	ution of system plan Feb30.sysplan based on managed m RCHAS60- DF26EA successful.

Figure 4-9 Success creating a system plan

#### Enabling hardware inventory collection from active partitions

When you use the HMC to create a system plan for a managed system, you can capture partition configuration information and a base set of associated hardware configuration information. If you have partitions already active, you can maximize the information that the HMC can obtain about the hardware.

To maximize the information that the HMC can obtain from the managed system, turn on the managed system and activate the logical partitions on the managed system, assuming that they already exist, before you create the new system plan.

Additionally, you need to set up Resource Monitoring and Control (RMC) on the HMC before you create a system plan to capture the most detailed information. Although using the RMC can take several more minutes to finish processing, by you can capture disk drive and tape drive configuration information for a managed system in the system plan. You can view this more detailed hardware information using the View System Plan task.

To enable the HMC's internal inventory collection tool (**invscout**) to be able to perform its most detailed hardware inventory retrieval operations, follow these steps:

- 1. In the HMC workplace window, select the HMC Management task.
- 2. Select **Change Network Settings**, and in the Customize Network Settings window, select the LAN Adapters tab, as shown in Figure 4-10.



Figure 4-10 Customize Network Setting - LAN Adapters for enabling RMC

- 3. In the LAN Adapters window, select the eth0 LAN Adapter and click Details.
- 4. In the LAN Adapter Details window (Figure 4-11) on the LAN Adapter tab, select **Open** within the Local Area Network information area to enable the check box for Partition Communication. Then, select **Partition** communication.

다. LAN Adapter Details
LAN Adapter Firewall Settings
Local Area Network Information         LAN interface address: 00:0D:60:0B:AB:8B eth0         ○ Private ③ Open       Media Speed (ethernet)         ✓ Partition communication       * Autodetection
DHCP Server
<ul> <li>DHCP Client/IP Address</li> <li>Obtain an IP address automatically</li> <li>Ospecify an IP address</li> <li>TCP/IP interface address: 172.17.0.2</li> </ul>
TCP/IP interface network mask: 255.255.0.0
OK Cancel Help

Figure 4-11 Customize Network Setting - LAN Adapters - partition communication

5. Click the Firewall Settings tab, scroll down the Available Applications area to see whether RMC is already specified as available. In this example, we assume that RMC has not yet been made available. Therefore, select RMC in the Allowed Hosts pane and click Allow Incoming, as shown in Figure 4-12.

Þ	🖋 LA	N Adapter Details				
L <sub>P</sub>	d <b>-</b> ^					
L	AN Adaj	pter Firewall Settings				
	LAN int	erface address: 00:0D:60:0B:AB	:8B Ethernet			
	– Availa	ble Applications				Allow Incoming
	Select	Application Name	Ports			Allow Incoming by IP Addre
	۲	Secure Shell	22:tcp			Allow remote Secure Shell
	0	Web Access	80:tcp			
	0	Secure Web Access	443:tcp 8443:tcp 9960:tcp			a00633.
	0	Secure ASM Access	9443:tcp			
	0	Open Pegasus	5989:tcp		~	
	– Allowe	ad Hosts				Remove
	Select	Application Name	Ports	Allowed Hosts		
	0	Web Access	80:tcp	0.0.0.0/0.0.0.0		
	0	Secure Web Access	443:tcp tcp:8443 tcp:9960	0.0.0.0/0.0.0.0		
	0	Secure ASM Access	9443:tcp	0.0.0.0/0.0.0.0	=	
	۲	RMC	657:udp tcp:657	0.0.0.0/0.0.0.0	-	
	0	FCS	9920:tcp udp:9900	0.0.0.0/0.0.0.0		
	0	Eclipse	4412:tcp	0.0.0.0/0.0.0.0		
	0	VTTY	9735:tcp	0.0.0.0/0.0.0.0		
ш	0	VTTY Proxy	2302:tcp	0.0.0.0/0.0.0.0		
	0	5250	2300:tcp tcp:2301	0.0.0.0/0.0.0.0		
	0	Incoming Ping	echo-request:icmp	0.0.0.0/0.0.0.0	~	
Ľ						
0	Car	ncel Help				

Figure 4-12 Customize Network Setting - LAN Adapters - enabling the RMC application

This action moves RMC into the Available Applications pane.

- 6. Click **OK** twice to open a window that states that the Network Settings Changes will be applied at the next HMC reboot.
- 7. Click **OK**. You are now back to the HMC workplace window with just the HMC Management pane on the right.

You can verify that you have enabled RMC successfully using the **1spartition** command on the HMC CLI. For more information about using the HMC CLI, refer to 4.3.3, "System plans management using restricted shell (CLI)" on page 171.

The list partition command is:

lspartition -c

For example:

hmc:> lspartition -c 9117\_MTM-10FZZD

In our example managed system, this command results in:

```
<#0> Partition:<4, partn1.business.com, 1.2.3.444>
    Active:<0>, OS<, >
```

If this command does not return any partitions, then the system might not be set up for RMC. Depending on whether the system is a System i or System p, the steps for RMC are different.

IBM Systems Hardware Information Center includes additional information about RMC. For background information about RMC, you can also refer to *A Practical Guide for Resource Monitoring and Control (RMC)*, SG24-6615. The content of this publication is based upon AIX 5L<sup>™</sup>, 5.1.

If the Create System plan from the GUI fails and if there is a need to create a system plan, use the underlying **mksysplan** CLI at the HMC command prompt, with the **noprobe** option. The **noprobe** option bypasses the default inventory collection of active partitions. So, the resulting sysplan might not have IOA/IOP controlled disk units or media enclosures.

For example:

hmc:> mksysplan -m machineName -f filename.sysplan -v -o noprobe

Note, when creating a sysplan, if there is a failure due to a Virtual I/O Server error, you can try the **noprobe** option from the CLI.

#### 4.2.4 Viewing a system plan on the HMC

The HMC has a system plan viewer similar to the viewer in the System Planning Tool. The viewer offers a non-editable presentation of the system's partitions and hardware. Using Figure 4-3 on page 137 as a starting point, select the desired plan in the main system plan management window. Click **View System Plan**.

When you are accessing the HMC remotely, you are presented with a View System Plan sign on window the first time that you launch the System Plan Viewer. This additional log in protects unauthorized users from viewing the system's configuration. It also prevents launching the Viewer from bookmarks without providing an appropriate user name and password.

You get the login window shown in Figure 4-13. If you get a sign on window, use a valid user name and password and click **Login**.

Hardware Management Console	
System Plan: Feb30.sysplan	
Login to proceed to the System Plan Viewer. Username: Password: Login	

Figure 4-13 View System Plan sign on page

Figure 4-14 shows the system plan. The left navigation frame shows a single partition or the entire system. You can also choose just specific enclosures under the Hardware section. The file history is also viewable. The viewer also has a Print option and Show Comments / Hide Comments toggle, located at the bottom of the viewer window.

If you are accessing the HMC from a PC browser, the print function is through the PC's attached and network printers. If you are using the HMC terminal itself, the print function is through printers that are connected to the HMC or network printers to which the HMC has access.

Hardware Management Console				111100	K JE	
System Plan: Feb30.sysplan						
🖃 🖹 Feb30.sysplan	Feb30.sysplan					^
History	Description:	System co	onfiguration on F	eb 30.		=
🗆 🛄 Systems	History					
E RCHAS60-SN10F26EA	Application	Version	n		Date	
	НМС	V7R3.1.0.0	Fri M	av 04 09:32:23 CDT 2	2007	
AIX2	Systems					
🖯 📼 Hardware	System: RCHASOU-SN10	F26EA				
U5095.001.01F2	Description: 940	6-520*10F26EA		Quantity:	1	
U787A.001.DQF	Memory: 327	68 MB		Memory Region Siz	ze: 64	
	Active Processors: 2.0			Total Processors:	2	
	Auto Start: no					
	Partitions					
	Partition: RCHAS60_i5	/os				
	ID: 1 Availability Priority, 1	27		Type: os400		
	Availability Pronty: 1	27				
	Partition Profile: KCH	1560_15/05				
	Memory	A 1	Processors		Virtual Process	sors
	Minimum: 24576 ME	i i	Minimum: 1	1.0	Minimum:	1
	Desired: 29696 MB		Desired: 1		Desired:	1
	Maximum: 29696 ME	<u>'      </u>	Maximum: 2	2.0	Maximum:	2
Liida Composite Drint Heli						

Figure 4-14 Viewing a system plan

The system plan section shown in Figure 4-15 shows the system's disk units. Note that the controller for the disk unit displays in the table. This detail is obtained only if the i5/OS operating system that is controlling the disk units is running. Linux and AIX operating systems do not display disk controller information or location information.

Hardware Management	t Console								
System Plan: RCHA	S61.sysplar	۱							
RCHAS61.sy History Systems RCHA History Systems RCHA History RCHA	Drives		P1-T5 - P1-T6 - (rotate counte	P1-T8 P1-T9 Back rclockwise for standalon	е)				<
E.	Backplane	Slot	Bus Device Feature	Device Description	Device Serial #	Disk Controller	Order Status	Used by Partition / Profile	
	P2	D1	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P2	D2	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P2	D3	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P2	D4	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P3	D1	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P3	D2	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P3	D3	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P3	D4	4326	35.16GB 15k RPM Disk Unit		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P4	D1	5754, 63A0	50GB 1/4 inch Cartridge Tape		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P4	D2	1994, 2640	IDE DVDROM		P1/T10	IBM	ITSO_i5/OS / ITSO_i5/OS	
	P4	D3							
<u>.</u>	Expand / P2 - D4- P2 - D3- P2 - D2- P2 - D1- P2 - D1-			P3 - D1 P3 - D2 P3 - D3 P3 - D4 P3 - D4	— P4 - D2 — P4 - D3				
Show Comments	Print I	Help							

Figure 4-15 Viewing a system plan

#### 4.2.5 Removing system plan on the HMC

When you no longer need a system plan, you can remove the sysplan file easily from the HMC. Using Figure 4-3 on page 137 as a starting point, follow these steps:

- 1. Select the desired plan in the main system plan management window.
- Click Remove System Plan either from the Tasks drop-down menu or the content Tasks link in the lower portion of the window. A conformation message displays asking if you are sure you want to delete the file (Figure 4-16).

Remove System Plan	
Confirm permanent removal of the specified system plan from this HMC. Feb30.sysplan Remove System Plan Cancel Help	

Figure 4-16 Confirm removal of system plan window

3. Click **Remove System Plan** to remove the selected sysplan file from the HMC.

## 4.3 System plans deployment

Since the publication of *LPAR Simplification Tools Handbook*, SG24-7231, from a general point of view, the deployment process has not changed a lot. Of course, due to the updates of System Planning Tool Version 2 and HMC software, the details are not the same. The major improvements of the process are related to Virtual I/O Server implementation.

In this section, we provide a summary of the deployment validation process. We cover the new deployment wizard using examples and provide details of the updates to the restricted shell CLI.

You can find specific deployment information about Virtual I/O Server in 9.1.2, "Virtual I/O Server" on page 261.

#### 4.3.1 Deployment validation process

Before deploying any system plan, it must be validated. There are two steps in this validation process. First, the hardware is validated and then, if that validation is successful, the partition is validated.

This process is detailed in *LPAR Simplification Tools Handbook*, SG24-7231. You can refer to that book at any time. However, because it is fundamental to fully understand how the validation process works, we summarize the main concepts in this section.

#### Hardware validation

When running hardware validation, the HMC checks that any planned hardware exists on the managed server and that all the I/O processors and adapters are located physically in the planned slots. Hardware validation does not necessary mean that an exact match must occur between the planned and the existing hardware. For example, you can plan on using less processors or memory than physically installed, or you can plan on not using all the physically installed I/O units.

**Important:** The HMC is not aware of the devices that are connected to the IOA. Therefore, there is no validation at a lower level than the IOA. When using the System Plan Tool, you *must* specify devices such as disk drives, CD/DVD drives, and tape drives. The validation process *cannot* perform any validation about these devices.

The validation includes all the following items:

- ► Server type, model and processor feature: an exact match is required
- > Number of processors: at least the planned number must exist
- Memory: at least the planned amount must exist
- Expansion units: all the expansion units in the plan must exist
- Slots: all the I/O processors and adapters in the plan must exist in a correct expansion or in the Central Electronic Complex (CEC) and must be at the same location
- Any serial number; an exact match is required

At this point, it is important to take actions to *avoid any ambiguity* about the expansion units or the processor enclosures CECs. You could have multiple CECs, for example on a 16-way model 570. In that case, you would have four CECs.

This ambiguity takes place when two or more installed expansion units or CECs have the same type and contain exactly the same I/O processors and adapters in the same slot. You might plan a partition to use specific expansion units due, for example, to their physical location in the racks or on the floor or to specific disks drives that the HMC cannot see. The validation process allows such a system plan, but there is no guarantee for the deployment to allocate the right expansion to the partition.

The best way to eliminate expansion units or CECs ambiguity is to specify, in the system plan, their serial number.

You must eliminate any hardware validation error, for the partition validation to start.

#### **Partition validation**

When running partition validation, the HMC checks that any *existing* partition on the server exactly matches with one of the planned partitions.

The validation includes all the following items:

- Partition name
- Partition ID
- Name of the default profile
- Processing resources in the system plan
- Memory resources in the system plan
- Physical hardware in the system plan
- ► Virtual adapters, including slot ids and maximum adapters, in the system plan

If any of these items fail, the partition validation is unsuccessful, and the deployment will fail. Some of the corrections to allow the deployment must be applied on the server. This is the case for the name of the default profile, which cannot be changed in the System Planning Tool and is the same as the partition name. This is also the case for some hardware features like the USB controller or the IDE CD controller that the HMC allows you to assign to an i5/OS partition (while it cannot use them) but the SPT does not.

#### 4.3.2 Deploy a system plan using the graphical wizard

In this section, to show the new deployment wizard related to V7R3 HMC software, we run three deployment examples:

- The first example fails due to hardware errors.
- The second example fails due to partitions errors.
- ► The third example is successful.

You can initiate deployment when you are using any right pane of the HMC by clicking **System plans** on the left pane as shown in Figure 4-17.



Figure 4-17 Launch deployment

To deploy a system, follow these steps:

1. On the list of the system plans, select the one that you want to deploy by clicking the check box to the left of the system plan, as shown in Figure 4-18. In our example, we select the **marc.sysplan** file.

Hardware Management (	Console			0947	ŧ/
				hscroot	Help Logoff
🔲 Welcom e	Contents of: System Plans				^
⊞ Îĝi System s Managem ent Îŝi System Plans	0 • # #	/ / 🛉	Tasks ▼		
HMC Management	Select ^ Name	↑ Description ↑	Source ^	Version ^	Last Modified Date
성ů Service Management	april19.sysplan		HMC V7R3.1.0.0	HMC 1.2	Apr 19, 2007 2:09:
ଷ୍ଟ୍ର Updates	april19_2.sysplan		HMC V7R3.1.0.0	HMC 1.2	Apr 19, 2007 2:15:
	🗆 🗈 current.sysplan	HMC created	. HMC V7R3.1.0.0	HMC 1.2	Apr 30, 2007 2:25:
	🔲 🖹 JC01.sysplan	JC01	HMC V7R3.1.0.0	HMC 1.2	Apr 24, 2007 8:38:
	💽 🗈 marc.sysplan 🖻		IBM System Planning Too	. SPT 1.2	May 2, 2007 5:21:
	newConfig.syspla	n			
	Total	7 Filtered: 7 Selec	ted: 1		~
	<	Ш			
	Tasks: marc.sysplan				
	View System Plan Create System Plan Deploy System Plan Export System Plan Import System Plan Remove System Plan				
Status: Attentions and Events					

Figure 4-18 Select the system plan to deploy

There are three different ways to start the deployment of the selected system plan, as shown in Figure 4-19.

- Click the contextual menu immediately to the right of the system plan name and select **Deploy System Plan**.
- Click **Deploy System Plan** in the bottom Tasks panel.
- Click **Tasks** at the top of the System Plans list panel and select **Deploy System Plan**.

Hardware Management (	Console	
	hscroot Help Logoff	
<ul> <li>□ Welcome</li> <li>☑ ☑ System s Management</li> <li>☑ ☑ System Plans</li> <li>☑ HMC Management</li> <li>※ Service Management</li> <li>※ Updates</li> </ul>	Contents of: System Plans         Select       Name       Description       Source       Version       Last Modified Date <ul></ul>	
Status: Attentions and Events	Tasks: marc.sysplan View System Plan Create System Plan Deptoy System Plan Export System Plan Import System Plan Remove System Plan	

Figure 4-19 Launch the deployment

2. After the wizard is started, its Welcome page, shown in Figure 4-20, requests that you confirm the system plan to deploy and choose the managed server to be the target of the procedure. When your choices are done (in our example, we want to deploy the *marc.sysplan* file to the *RCHAS60-SN10F26EA* server), click **Next** to continue.

Welcome - De	ploy System Plan Wizard
Welcome to the deploying an ex Select the syst system.	e Deploy System Plan wizard. This wizard will help in xisting system plan file on a managed system. em plan file to deploy and the target managed
System plan:	🔹 marc.sysplan 🔍
Managed system:	+ RCHAS60-SN10F26EA ▼
< Back Next >	Deploy Cancel Help

Figure 4-20 Confirm the deployment startup

3. Figure 4-21 shows you the validation progress. When this has completed, you can examine all the related messages, those messages that are successful as well as those messages that are unsuccessful. We provide information about the validation types in 4.3.1, "Deployment validation process" on page 151.

	·		
Validation - Deploy	System Plan Wizard		
The wizard is now va	lidating whether system plan 'marc.sysplan', can be		
leployed on managed	l system 'RCHAS60-SN10F26EA'		
- Validation Progress -			
Validation - Deploy System Plan Wizard         The wizard is now validating whether system plan 'marc.sysplan', can be eployed on managed system 'RCHAS60-SN10F26EA'         · Validation Progress         Validation Type         Status         Hardware validation         - Validation         - Validation Type         Status         Hardware validation         - Validation Messages         Gathering information            < Back       Next > Deploy         Cancel         Help			
Hardware validation	In Progress	Т	
Partition validation	in regioco		
r and on vandadon			
Validation Messages			
Gathering informatio	n	ן ר	
0			
Bask Next D	union Connect Hale		
< Back Next > De	epioy Cancel Heip		

Figure 4-21 Deployment validation in progress

Here are three examples of validation result:

 The first example is related to a system plan that fails to deploy due to hardware errors. Figure 4-22 shows unsuccessful hardware validation.

	_ 🗠			
Validation - Deploy System Plan Wizard				
Validation failed. System plan 'marc.sysplan' can not be deployed on managed				
system 'RCHAS60-SN10F26EA'. Please review validation messages.				
Validation Progress				
Validation Type Status				
Hardware validation Failed				
Partition validation	_			
- Validation Mossagos	_			
Gathering information				
Hardware validation messages:				
System plan system unit 9406_520-0, type 520, serial number DQF26EA				
matched and validated with system unit serial number DQF26EA that had				
that same serial number found on the managed system.				
Validation error: the system plan specified:				
expansion unit 5095-1, Backplane name CB1, Slot number C07, Device				
class code 0004				
expansion unit 5095-1. Backplane name CB1. Slot number C07. Device				
< Back Next > Deploy Cancel Help				
	~			

Figure 4-22 Deployment validation summary (hardware failed)

The Validation Messages panel shows the result of each particular validation step. You might need to scroll down or up to find the root cause of the failure and, in most cases, you can correct the system plan to get a successful validation.

Figure 4-23 shows the first hardware validation error message, which tells you that, in the expansion unit 5095, the slot C7 is occupied by a device which is not the same that the one specified in the system plan. The best way to correct this specific error is to update the system plan with SPT to match the hardware. Another option could be to install the right device physically according to the system plan and to adjust all the hardware to the system plan. This option might lead you to order such a device and move I/O cards from a slot to another.

After reading all the necessary messages, click Cancel to exit the window.

Validation - Deploy	System Plan Wizar	d	
Validation failed, Syst	tem plan 'marc.svspl	an' can not be deployed on managed	
system 'RCHAS60-SN	10F26EA'. Please r	eview validation messages.	
Validation Duanuas			
Validation Progress -	o		
Validation Type	Status		
Hardware validation	Failed		
Partition validation			
Validation Messages			
matched and validate	ed with system unit s	erial number DQF26EA that had 🛛 🖄 📗	
that same serial num	ber found on the ma	naged system.	
Validation error: the s	system plan specifie	d:	
expansion unit 5095	-1, Backplane name	CB1, Slot number C07, Device	
class code 0C04			
the same object foun	d on the managed s	ystem specified:	
expansion unit 5095	-1, Backplane name	CB1, Slot number C07, Device	
class code 0200			
for the same item.			
System plan expans	ion unit, type 5095 se	erial number 01F26EA not valid as 💌	
	play Canaal Hair		
< Dack Next > De	eproy Cancel Help		
			~

Figure 4-23 Example of hardware validation error

**Note:** The partition validation does not begin while there are errors on the hardware validation type.

 The second example is related to a system plan that fails to deploy due to partition errors. Figure 4-24 shows successful validation for the hardware part, and failed validation for the partition validation type.

				. 🛆
	Validation - Deploy	System Plan Wizard		
١	alidation failed. Syst	tem plan 'marc.sysplan' can r	not be deployed on managed	
S	vstem 'RCHAS60-SN	110F26EA'. Please review va	alidation messages.	
Г	Validation Progress -			1
	Validation Type	Status		
1	Hardware validation	Successful		
IN	Partition validation	Failed		
	Validation Mossages			
	Gathering information	2		
	Hardware validation	messages:		
	System plan system	unit 9406_520-0, type 520, s	erial number DQF26EA 👘	
	matched and validate	ed with system unit serial nur	nber DQF26EA that had	
	that same serial number found on the managed system.			
	System plan expansion unit 5095-1, type 5095, serial number 01F26EA			
	matched and validated with expansion unit serial number 01F26EA that had			
	that same serial number found on the managed system.			
	no deproyment valid	anon enors round when com	ame PCHAS60-	
	specified by the syste	em plan marc.syspian, plan n		
	< Back Next > De	eploy Cancel Help		

Figure 4-24 Deployment validation summary (partition failed)

The Validation Messages panel shows the result of each particular validation step. You might need to scroll down or up the list to find the root cause of the failure, and, in most cases, you can correct the system plan to get a successful validation.

Figure 4-25 shows the first partition validation error message, which tells you the partition 3 name of the system plan does not match with the existing partition 3 name. To fix this problem, you can either rename the partition in the system plan with SPT or rename the partition with the HMC.

After reading all the necessary messages, click **Cancel** to exit the window.

	· · · · · · · · · · · · · · · · · · ·			
Validation - Deploy System Plan Wizard				
Validation failed Syst	em plan 'marc sysplan' can not be deployed on manage	he		
system 'BCHAS60-SN	10F26FA' Please review validation messages	, u		
Validation Progress –				
Validation Type	Status			
Hardware validation	Successful			
Partition validation	Failed			
Validation Messages		_		
reported hardware.		^		
Partition validation m	lessages:			
validation error: the s	system plan specified:			
partition, Partition ID	d on the managed system encodied.			
ne same objection	a Dartition name ANO			
for the same item	3, Parilium name AMZ			
Validation error parti	tion Partition ID 0. Drofile name AIX0 was found on the			
managed eveters but	did not match any planned chiegts found for item			
narraged system but	2 type found in the system plan. This item must be			
	s type found in the system plan. This item must be	•		
Book Novt Do	nlav Canaal Hain			
< Back Next > De	proy Cancel Help			

Figure 4-25 Example of partition validation error

 The third example is related to a system plan which gets successful validation. Figure 4-26 shows a successful validation for both hardware and partition steps. You can review all the messages in the Validation Messages panel, then click **Next** to continue.

	Validation Donlow System Dlan Wizard				
	Validation - Deploy System Plan Wizard				
i	Hardware and Partition Validation are complete for system plan 'RCHAS61.sysplan' and managed system 'RCHAS61-SN10F257A'				
1	Validation Progress				
	Validation Type Status				
1	Hardware validation Successful				
Ι	Partition validation Successful				
,	Validation Messages				
	Hardware validation messages: System plan system unit 9406_520-0, type 520, serial number * matched and validated with system unit serial number DQF257A found on the managed system.				
	No deployment validation errors found when				
	comparing the hardware as specified by the system				
	plan RCHAS61.sysplan, plan name RCHAS61-				
	SN10F257A, against the managed system RCHAS61-				
	< Back Next Deploy Cancel Help				

Figure 4-26 Example of successful validation

- 4. After the validation, the next panel is the starting point of the deployment. There are two portions in this panel:
  - a. The first contains the list of all the actions that are planned (see Figure 4-27). In our example, the system plan is built with one i5/OS partition that hosts three Linux partitions.

Notice the Partially deployed status of the i5/OS partition. This status means that some items of the partition exists on the server and does not need to be deployed. Specifically, here, the partition and the profile are created (and the LPAR is running at the time of the screen capture). These items will not be deployed again.

Notice also the Deploy column. Each action of the plan can be deselected if you prefer run it at a later deployment. Notice that, even if there are deselected items, the dependency is checked before running the deployment. So, you cannot, for example, deploy an hosted partition while the hosting one does not exist.

If you need to review the details of a specific action, you can select this one in the radio boxes of the Select column and click **Details**.

Partitio	Partition Deployment - Deploy System Plan Wizard					
Use this checked more det	page to specify w plan actions will l ails about the par	vhich partition be deployed. S rtition plan act	plan actions to deple elect a row in the Pa ion.	oy on the m artition Plar	nanaged system. On Actions table to	nly the view
Partition F	lan Actions			$\frown$		
Selec	t Dependency	/ Hierarchy	Plan Action	Deploy	Status	
0	1.1	(	Partition ITSO_i5/0		Partially deployed	)
0	1.1.2		Partition vcx	Image: A start of the start		
$\sim$	1.1.3		Partition LinuxVIO			
0	1.1.4		Partition IPT2			
			Details			
Partition [	eployment Step (	Order	·			
This tab	le displays the pa	rtition deployr	nent steps that will b	be peforme	d based on the ite	ms
checked	in the Partition	Plan Actions ta	ble.			
Deplo	yment Step					
Partitio	n vcx					
Partitio	n LinuxVIO					
Partitio						=
Partitio	n Profile ITSO_i5/	OS Virtual SCSI	Adapters			
Partitio	n Profile ITSO_15/	OS Virtual Ethe	ernet Adapters			
Partitio	Partition Profile ITSO_i5/OS Virtual Serial Adapters					
Partitio	Partition Profile vcx					
Partition Profile LinuxVIO						
Partition Profile IPT2						
Partituo	In Profile VCX VIrtu	lat SCSI Adapte	15			•
< Back Next > Degloy Cancel Help						

Figure 4-27 Request the details of a specific action
b. Click **Details**. The HMC links to the System Plan Viewer, restricted to the view associated with selected action. The System Plan Viewer *report* for the action is displayed in a separate window, as shown in Figure 4-28. In this example, we show the planned profile for the vcx partition. After the review is finished, just close this window.

**Note:** You might need to authenticate again to the HMC when accessing this option.

Partition: vcx ID: 2 Description: vcx partition Availability Priority: 127												
Partition Profile: vcx												
Memory       Processors       Virtual Processors         Minimum: 1152 MB       Minimum: 0.3       Minimum: 1         Desired: 1152 MB       Desired: 0.3       Desired: 1         Maximum: 2176 MB       Maximum: 1.0       Maximum: 2         Sharing Mode: uncap       Dedicated: no       Naximum: 2         Additional Properties       Operating Environment: Linux       Invironment: Linux												
Slot R	Required		IEEE 802.1	Compatible		ype <u>Slot</u>	Rec	<u>uired</u>	Remote Parti	tion / Profile	Remote Slot	
2 y	es	:	1 no		CI	ient 3	yes	5	ITSO_i5/OS /	ITSO_i5/O	5 6	
Virtual 9	Serial											
Type	Slot	Requir	ed Remote P	artition / I	<u>Profile</u>	Remote	<u>Slot</u>					
Server	0	yes										
Server	1	yes										
Hardwa	re											
	Unit		Backplane	Slot	Bus	Require	ed 🛛	De	vice Feature		Device Des	scription
9406_5	520-0	F	1	Т7		yes		EUSB		Embedded	USB Controlle	r
9406_520-0 P1 T12			yes		EIDE		Embedded	IDE controller	AIX/Linux			

Figure 4-28 Details of an action, shown by a restricted view System Plan Viewer

c. The second portion contains the detailed list of all the steps that the HMC performs to deploy the plan as shown in Figure 4-29. You can scroll down and up to review all the steps.

Partition Deployment - Deploy System Plan Wizard Use this page to specify which partition plan actions to deploy on the managed system. Only				
ecked pl re detai	lan actions will be deployed. S Is about the partition plan act	ielect a row in the Pa ion.	rtition Pla	n Actions table to
tition Pla	an Actions			
Select	Dependency Hierarchy	Plan Action	Deploy	Status
0	1.1	Partition ITSO_i5/OS		Partially deployed
0	1.1.2	Partition vcx		
0	1.1.3	Partition LinuxVIO	- -	
0	1.1.4	Partition IPT2		
eploy artition	n the Partition Plan Actions ta ment Step vcx	able.		
artition	LinuxVIO			
artition	IPT2			
artition	Profile ITSO_i5/OS Virtual SCS	Adapters		
artition	Profile ITSO_15/OS Virtual Ethe	ernet Adapters		
artition	Profile vcx	at Adapters		
artition	i i onto i on			
artition artition	Profile LinuxVIO			
artition artition artition	Profile LinuxVIO Profile IPT2			
artition artition artition artition	Profile LinuxVIO Profile IPT2 Profile vcx Virtual SCSI Adapte	ers		

Figure 4-29 List of the deployment steps

d. When you are ready to deploy, after reviewing details of the actions, eventually deleting some of the actions, and reviewing the deployment steps, as shown in the Figure 4-30, click **Deploy** to start the deployment.

Partition	n Deployment - Deploy Syste	m Plan Wizard			
Use this page to specify which partition plan actions to deploy on the managed system. Only checked plan actions will be deployed. Select a row in the Partition Plan Actions table to vie more details about the partition plan action.					nly the riew
artition Pla	an Actions				
Select Dependency Hierarchy Plan Action Deploy Status					
0	○ 1.1 Partition ITSO_i5/OS   Partially deployed				
0	1.1.2	Partition vcx			
0	1.1.3	Partition LinuxVIO			
0	1.1.4	Partition IPT2	<ul><li>✓</li></ul>		
Partition Deployment Step Order This table displays the partition deployment steps that will be peformed based on the items checked in the Partition Plan Actions table.					
Deploy	ment Step				
Partition	VCX				^
Partition	LinuxVIO				
Partition	IPT2				
Partition	Profile ITSO_i5/OS Virtual SCS	Adapters			
Partition	Profile ITSO_i5/OS Virtual Ethe	ernet Adapters			
Partition Profile ITSO_i5/OS Virtual Serial Adapters					
Partition Profile vcx					
Partition Profile LinuxVIO					
Partition Profile IP12					
Alabert Folder Field Partition Profile vcx Virtual SCSI Adapters     Alabert Science Help					ľ

Figure 4-30 Partition Deployment - Deploy System Plan Wizard

5. Figure 4-31 shows the last panel before running the deployment. There is a summary of all the steps that the HMC performs. Click **Deploy** to start the operations.

Notice the warning just above the buttons at the bottom of the window.

The deploy process time, depending on the complexity and the number of partitions, generally ranges from 5 to 20 minutes, and might be longer for specific deployments, when using Virtual I/O Server partitions for example.

Summary - Deploy System Plan Wizard				
You are now ready to deploy the system plan. Click Deploy to deploy the system plan in the order shown below.				
Managed system: RCHAS61-SN10F257A				
Deployment Step Order				
Deployment Step				
Backup existing partition configuration data				
Partition vcx				
Partition LinuxVIO				
Partition IPT2				
Partition Profile ITSO_i5/OS Virtual SCSI Adapters				
Partition Profile ITSO_i5/OS Virtual Ethernet Adapters				
Partition Profile ITSO_i5/OS Virtual Serial Adapters				
Partition Profile vcx				
Partition Profile LinuxVIO				
Partition Profile IPT2				
Note Please DO NOT perform any other actions on this managed system while deployment is running.				

Figure 4-31 Ready to deploy

While the deployment is running, as shown on the Figure 4-32 on page 168 and Figure 4-33 on page 169, you can follow its progress. Each step is In progress then Successful, from the top to the bottom of the Deploy progress portion of the panel. Notice that you have to move the cursor of this list by yourself to see those steps that do not fit in the initial window.

**Note:** The first step that you cannot disable is always to perform a backup of the actual partitions configuration.

In the Messages portion of the panel, we see the detailed results of each step. In our example, when running the step "Partition Profile ITSO\_i5/OS Virtual Serial Adapters", you can see that there is no result yet. However, when running the previous step, we can see that one of the results was the following message:

Virtual Ethernet Adapter deployed for slot 5 on profile ITSO\_i5/OS of partition 1 on managed system RCHAS61-SN10F257A.

Notice that the display sort, for this list, is the opposite of the steps sort. You see the latest event first and the first one last, and therefore, there is no need to scroll down or up this list during the deployment.

Deployme	nt Progress - Deploy System Plan Wizard
Store Dep	oloyment status: In Progress
Note	
Please DO	NOT perform any other actions on this managed system while
deployment	t is running.
System plan:	RCHAS61.sysplan
Managed sys	stem: RCHAS61-SN10F257A
Deploy Progr	ess
Status	Step
Successful	Backup existing partition configuration data
in Progress	Partition vcx
	Partition LinuxVIO
	Partition IPT2
	Partition Profile ITSO_i5/OS Virtual SCSI Adapters
	Partition Profile ITSO_i5/OS Virtual Ethernet Adapters
	Partition Profile ITSO_i5/OS Virtual Serial Adapters
	Partition Profile vcx
	Partition Profile LinuxVIO
	Partition Profile IPT2
Messages	
* The exist	ting partition configuration for managed
system RCH	IAS61-SN10F257A was backed up to file
0705081710	32RCHAS61-SN10F257ARCHAS61 prior to
deploying p	olan items on the managed system.
Stop Clase	Help
	1. sette

Figure 4-32 Deployment starting



Figure 4-33 Deployment in progress

When the deployment is complete, as shown in Figure 4-34, review all the steps and messages to make sure that everything is OK. Then, click **Close** to finish the session.

Deployment Progress - Deploy System Plan Wizard					
Deproyment status. Deproyment complete					
Please DO NOT perform any other actions on this managed system while deployment is running					
deproyment is running.					
System plan: BCHAS61 system					
Managed system: RCHAS61-SN10E257A					
Deploy Progress					
Status Step					
Successful Partition Profile IP12					
Successful Partition Profile vox Virtual Scsi Adapters					
Successful Partition Profile vox Virtual Ethernet Adapters					
Successful Partition Profile Vicx virtual Senal Adapters					
Successful Partition Profile LinuxVIO Virtual SCSI Adapters					
Successful Partition Profile LinuxVIO Virtual Eneriet Adapters					
Successful Partition Profile IPT2 Virtual SCSI Adapters					
Successful Partition Profile IPT2 Virtual Star Adapters					
Successful Partition Profile IPT2 Virtual Corial Adapters					
Successful Partition Profile IP12 Virtual Serial Adapters	<u> </u>				
Messages					
Virtual social adapter pet depleyed Virtual social					
adapter already deployed for slot 0 op profile IPT2 of					
partition 4 on managed system RCHAS61-SN10F257A.					
* Virtual Ethernet adapter deployed for slot 2 on					
profile IPT2 of partition 4 on managed system					
RCHAS61-SN10F257A.					
* Virtual SCSI adapter deployed for slot 3 on profile					
IPT2 of partition 4 on managed system RCHAS61-					
SNTOF257A.					
Verdenner					
Stop Close Help					
h2					

Figure 4-34 Deployment complete

#### 4.3.3 System plans management using restricted shell (CLI)

This section focuses on the HMC CLI commands that are designed for managing tasks relating to system plans. Four of CLI command were introduced in HMC V5R2 code level and remain unchanged. Since System Planning Tool Version 1, their function and syntax did not change. We do not document existing parameters in HMC V5R2 code level here.

One of the CLI commands was introduced in HMC V5R2 and is updated in the HMC V7R3 code level. It has new parameters. We document only these new parameters here.

To get more information about the unchanged commands and parameters, or about the way to use the restricted shell, refer to *LPAR Simplification Tools Handbook*, SG24-7231.

#### **Unchanged commands**

The unchanged commands are the basic commands, which are:

- lssysplan used to display a list of the system plans.
- deploysysplan used to deploy a system plan on a managed server.
- rmsysplan used to delete a particular system plan.
- cpsysplan used to export (copy from the HMC) or import (copy into the HMC) a system plan. Because this command is unchanged, unlike the GUI there is no way to specify exporting or importing to or from the current PC.

#### **Updated commands**

The **mksysplan** command has two new optional parameters. This command is used to create a system plan that contains the actual LPAR configuration of a specific managed server. The two new optional parameters are:

► -o is used to specify an option for inventory collection

By using this parameter with the **noprobe** value (the only allowed one), you can request not to scan the devices which are attached to IOA cards. This way, you do not retrieve in your system plan, any disk drives attached to the disks controllers, any tape drives which are unknown by the HMC, but are only known by the operating system of the partitions. Using this parameter allows the command to run much more faster, if you do not need the devices level details.

If you do not specify the **-o** parameter, the HMC requests the operating system of each active partition to return the devices information for each IOP.

**Important:** To be able to receive devices information from the operating system, the corresponding partition *must be running*.

With or without using the option, the display output is the same as you can see in the Example 4-1. The first command does not specify **-o** parameter, and therefore gather all the devices information. The second one specifies **-o** parameter, and therefore does not request the operating system of the partitions to provide devices information.

Example 4-1 The mksysplan command with or without -o parameter

```
hscroot@RCHAS6OH:~> mksysplan -f marc.sysplan -m 9406-520*10F26EA
Started inventory gather process ...
System plan marc.sysplan created successfully for the system
9406-520*10F26EA.
hscroot@RCHAS6OH:~> mksysplan -f marc.sysplan -m 9406-520*10F26EA -o
noprobe
Started inventory gather process ...
System plan marc.sysplan created successfully for the system
9406-520*10F26EA.
hscroot@RCHAS6OH:~>
```

Both commands create the same system plan whose name is marc.sysplan but their contents are different.

Without specifying **-o** noprobe, like the first one, you get the devices information from the running partitions, as you can see in Figure 4-35 on page 173. You can see the disk drives details.

Hardware Management Concole							$I \Delta$	<u></u>	0/1/3	
System Plan: marc system								<b>//</b> 02555		
	Drives									<b>A</b>
History	Backplane	<u>Slot</u>	<u>Bus</u>	<u>Device</u> Feature	D	Device escription	Device Serial <u>#</u>	<u>Disk</u> <u>Controller</u>	<u>Order</u> Status	Used by Part
E RCHAS60-SN10F26EA	DB1	D01			Dis	k Unit	68- 0CB7DDC	CB1/C02	Own	RCHAS60_15 RCHAS60_15
Partitions	DB1	D02			Dis	k Unit	68- 0CBD3C5	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
HOSTED_AIX	DB1	D03			Dis	k Unit	68- 0CF67B8	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
Hardware	DB1	D04			Dis	k Unit	68- 0CF4C46	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
U5095.001.01F26EA U787A.001.DQF26EA	DB1	D05			Dis	k Unit	68- 0CB3893	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB1	D06			Dis	k Unit	68- 0CF4B77	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D07			Dis	k Unit	68- 0D258B2	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D08			Dis	k Unit	68- OCBE30E	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D09			Dis	k Unit	68- 0CAA40E	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D10			Dis	k Unit	68- 0C9C017	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D11			Dis	k Unit	68- OCB5ECD	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	DB2	D12			Dis	k Unit	68- 0D24963	CB1/C02	Own	RCHAS60_i5 RCHAS60_i5
	D01	Collap	DB1	stem Ima	ge	CB1		008		
	D02 D03 D04 D05			B01 B02				006 005 004 003 002 001		≣
	[ D07 [ D08 [ D09 [ D10			ВОЗ			P01			
Hide Comments Print Help	D11 D12			ВО4	)		P02			~

Figure 4-35 Disk information is gathered when not using -o noprobe on mksysplan

When specifying **-o** noprobe, the same query does not retrieve those devices information, as shown in Figure 4-36.



Figure 4-36 Disk information is not gathered when using -o noprobe on mksysplan

-v is used to specify verbose display output

This parameter does not have any value. You can specify it or not. When specified, the display output contains more information about the steps that the HMC performs. As shown in the Example 4-2, depending on the -o parameter usage, the display output are not exactly the same. Both commands specify -v parameter. The first gathers the devices information while the second does not.

Example 4-2 The mksysplan with -v parameter and with or without -o parameter

```
hscroot@RCHAS60H:~> mksysplan -f marc.sysplan -m 9406-520*10F26EA -v
Started inventory gather process ...
Gathering slot level hardware and logical definitions ...
Creating new VPD files for the system ...
Adding inventory sensed from each active partition.... If you dont need
a system plan to include realtime inventory, retry using the -o noprobe
option
Gathering VIOS identified hardware and logical definitions ...
Completed inventory gathering without errors ...
Writing system plan ...
System plan marc.sysplan created successfully for the system
9406-520*10F26EA.
hscroot@RCHAS60H:~> mksysplan -f marc.sysplan -m 9406-520*10F26EA -v -o
noprobe
Started inventory gather process ...
Gathering slot level hardware and logical definitions ...
Gathering VIOS identified hardware and logical definitions ...
Completed inventory gathering without errors ...
Writing system plan ...
System plan marc.sysplan created successfully for the system
9406-520*10F26EA.
hscroot@RCHAS60H:~>
```

**Note:** The equivalent GUI action that creates system plans makes use of the default of the **mksysplan** command. Therefore, it always gathers all the device information without any verbose output.

# 5

# HMC security and user management

In this chapter, we discuss Certificate Management and User Administration within the Hardware Management Console (HMC) environment. We describe both certificate management and HMC user management.

### 5.1 Certificate management

HMC security management has changed from earlier versions of the HMC. Most options under System Manager Security are no longer needed in Version 7.3. Object Manager and Server Security are now gone. The new option for securing HMC remote connections is Manage Certificates under the Administration tab of HMC Management.

Security certificates ensure that the HMC can operate securely in the client-server mode. The managed machines are servers and the managed users are clients. Servers and clients communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity.

When a user wants remote access the HMC user interface through a Web browser, the user requests the secure page by https://hmc\_hostname. The HMC then presents its certificate to the remote client (Web browser) when establishing connection with the HMC. The browser verifies that the certificate was issued by a trusted party, check that the dates are still valid, as well as making sure that the certificate was created for that specific HMC.

Manage Certificates is located in the Administration section of HMC Management, as shown in Figure 5-1.

Hardware Management Cor	nsole		hscroot	Help   Logoff
Welcom e	HMC Management (HMC Vers	ikn )		[ Alphabetical List ]
🖽 🗐 System s Management	Operations			
System Plans	View HMC Events	* Display the event log of HMC operations and activitias		
HMC Management	Shut Down or Restart Schedule Operations	Shut down or restart the HMC     Customize a schedule for HMC operations		
Service Management	Format Media	* Formatia DVD, diskatta, or high append memory key		
	Back up HMC Data	* Back up HMC information to DVD, to a remote system, or to a remote site		
Ge opdates	Restore HMC Data	Bemotely restore backed up critical data for the HMC		
	Save Upgrade Data	* Use a wizard to save upgrade data to the hard drive or to a DVD		
	Change Network Settings	* View current network information and change settings		
	Test Network Connectivity	View network diagnostic information about the network protocols for the HMC		
	View Network Topology	* View, save, and ping current network topology		
	Tip of the Day	* Display tips for using the console		
	View Licenses	* Bead the licenses for the product		
	Change User Interface Settings	* Customize the appearance of the HMC workplace		
	Change Date and Time	* Change the date and time for the HMC		
	Launch Guided Setup Wizard	* Run the Guided Setup Wizard and step through setting up your HMC for the first time		
	Administration			
	Change User Password	* Change an existing HMC user's password		
	Change User Profiles and Access	* Add, copy, remove, and modify HMC system users and user profiles		
	Manage Task and Resource Roles	Customize and manage profiles for user access levels and managed resources		
	Manage Users and Tasks	* View the logged on users and the tasks they are running		
	Manage Certificates	* Create, modify, delete, and import certificates used on the HMC, and view certificate signing information		
	Remote Command Manage Certific	ates nable or disable the command line interface on an HMC		
	Remote Operation	Enable or disable a new HMC subpanel in the workplace		
		Control whether this HMC call be operated using a web browser from a remote workstation		
	Change Language and Locale	* Change the HMC interface language and locale		
	Create Welcome Text	Customize the greeting displayed before logging on		
	Manage Data Replication	Configure the Data Replication settings for the HMC		
Statute: Open Serviceable Events				
https://9.3.5.228/hmc/ui/bonsai/launch.do?type=18	stask=00000107			9.3.5.228 🙈

Figure 5-1 Manage Certificates

The available options in Manage Certificates allow you to create, modify, import, and remove certificates. There are a couple of notable changes from earlier HMC versions in HMC V7R3. Remote access is now available through a Web browser. Previous versions used WebSM remote client. Another notable change in certificate management is that HMC V7 does not allow a public or private key ring file to be created.

#### 5.1.1 Creating a new certificate

You can create a new self-signed certificate or a certificate signed by a trusted third party. By default, the HMC comes with a self-signed certificate. To create a new certificates signed by a Certificate Authority:

1. Select HMC Management  $\rightarrow$  Manage Certificates  $\rightarrow$  Create  $\rightarrow$  New Certificate as shown in Figure 5-2.

<b>i</b>	Manage Certificates					
Creat	e 🔻 Selected 👻 Advanc	ed 🗸				
New	Certificate					
		Certificate for this console				
Select	Property	Value				
0	Version	3				
0	Serial Number	282610813796040340283750365322500161555				
0	Issuer	EMAILADDRESS=email_test@ibm.com, CN=localho				
0	Valid From	May 14, 2007 5:17:56 PM				
0	Valid Until	May 13, 2008 5:17:56 PM				
0	Subject	EMAILADDRESS=email_test@ibm.com, CN=localho				
0	Subject Alternative Names	DNS: localhost.localdomain, DNS: localhost, IP: 9.				
Apply	Apply Cancel Help					
•						

Figure 5-2 Create New Certificate

2. You are given the option of creating a self-signed certificate or a certificate signed by a Certificate Authority as shown in Figure 5-3. Select **Signed by a Certificate Authority**.



Figure 5-3 Certificate Signing

3. The HMC displays the **New Certificate** window as shown in Figure 5-4. Complete the New Certificate form and click **OK**.

New Certificat Enter the following inf created:	e ormation for the certificate signing request	to be	
Organization (e.g. IBM) Organization unit (e.g. Hardware Development)	IBM		
Two letter country or region code (e.g. US) State or Province (e.g. CA) Locality (e.g. Los Angeles) Number of days until expiration (e.g. 365)	US - United States (of America) Texas Austin 365		•
E-mail address (e.g. xxxx@ibm.com) OK Cancel Help	email_test@ibm.com		
Done		9.3.5.231	

Figure 5-4 New Certificate

4. A window displays prompting you for the certificate to be stored as shown in Figure 5-5. You have the option of storing the certificate on Removable media on the console or on the file system on the system running the browser. Make your choice to continue.



Figure 5-5 Certificate location

5. A message box displays asking for Save verification as shown in Figure 5-6. Click **OK** to save the Certificate Signing Request as a file. You are then prompted if you want to use a temporary self-signed certificate until your certificate is signed and returned.

Clicking Yes creates a self-signed certificate.



Figure 5-6 Creating a self-signed certificate while waiting on a signed certificate from a Certificate Authority

You are returned to the **Manage Certificates** window shown in Figure 5-2 on page 180. Many of the values will be Not available.

- 6. Click **Apply** to apply the new self-signed certificate. *These values are updated after the certificate has been applied and the console has been restarted*. The next window asks for verification to replace the current certificate.
- 7. Click **Yes** to proceed. You are then presented with a message box asking if the certificate was replaced successfully or if any errors occurred.
- 8. Click **OK**. Clicking OK at this point restarts the console.
- After your certificate request is signed and returned, you need to import the certificate and apply by clicking HMC Management → Manage
   Certificates → Advanced → Import Certificate. After the certificate has been imported, apply it and restart the console.

#### 5.1.2 Modifying existing certificates

You can modify certain properties of an existing certificate. To modify a certificate, from the Manage Certificates window, select the radio button of the entry you want to modify, then click **Selected**  $\rightarrow$  **Modify**. Modifiable properties are:

- Valid Until
- Subject
- Subject Alternative Names

For example, to modify the Valid Until property, select the radio button for that property and then select **Selected**  $\rightarrow$  **Modify**. The window shown in Figure 5-7 displays.



Figure 5-7 Modify Current Certificate

#### 5.1.3 Advanced options for modifying existing certificates

There are several advanced options available for working with certificates under the Advanced tab. You can:

Delete and Archive Certificate

Allows you to remove the current certificate. After deleted, the certificate is actually archived on the HMC.

Work with Certificate

Allows you to view and restore archived certificates. Figure 5-8 shows the Archived Certificate window.

Action	15 🔻					
Inst	all					
Viev	v Archived Issuer Certificat	te	Archived Certificate			
Select	Property	۷al	ue			
0	Version	3				
0	Serial Number	259	9986092997607498156908375640	7814179		
0	Issuer	CN	=localhost.localdomain, OU=xxx, O=	×xx, ST=Al		
0	Valid From	Ma	y 15, 2007 10:22:34 AM			
0	Valid Until	De	: 30, 2037 9:22:34 AM			
0	Subject	CN	=localhost.localdomain, OU=xxx, O=	×xx, ST=Al		
0	Subject Alternative Names	DN	S: localhost.localdomain, DNS: local	nost, IP: 9.		
Close	Close Help					
•				▶		
javascript:	menuItemLaunchAction();			9.3.5.231 🙆		

Figure 5-8 Restoring Archived Certificate

To restore an archived certificate, select **Actions**  $\rightarrow$  **Install**. A window displays asking for verification for restoring the certificate. Click **Yes** to proceed. *This action restarts the console if the installation is successful*.



Figure 5-9 Restore Archived Certificate Verification

Import certificate

Allows you to import a certificate from media or a remote file system. Select the location of the certificate to import. When the certificate has been uploaded, you need to apply and restart the console.

View Issuer certificate

Displays available information about the issuer of the certificate.

### 5.2 HMC user management

In the Administration section of the HMC Management Task, there are four options for creating and managing users. Some of these tasks are handled in the Setup Wizard when the HMC is initially configured. The options in the HMC Management Administration section allow you to modify the initial user configuration.

#### 5.2.1 Changing the user password

To use this function, select HMC Management  $\rightarrow$  Change User Password.

This option allows you to change the password of the current user. The current password is needed for this option and the new password must be different than the current password. Figure 5-10 shows the Change User Password window.

Change User Password To change your password, enter your current password					
and your new password twice below and click OK. Current password:					
New password:					
Confirm new password:					
	OK Cancel Help				
Done	9.3.5.231 🔗				

Figure 5-10 Change User Password window

#### 5.2.2 Managing user profiles and access

To use this function, select HMC Management  $\rightarrow$  Manage User Profiles and Access.

This option allows you to add, copy, remove, and modify HMC system users and user profiles. The administrative functions display in a drop-down menu from the User menu.

Mana	Manage User Profiles and Access					
User	Help	•				
Select a User ID below and click "User" to manage the console users.						
Select	User ID	Description				
۲	hscroot	HMC Super User				
0	hscpe	HMC User				
0	root	root				
Done			9.3.5.231	<u>.</u>		

Figure 5-11 User Profiles window

#### Adding a new user with Super Administrator role

To add a new user with the Super Administrator role, follow these steps:

 Select User → Add to add a new user. The HMC displays the Add User window as shown in Figure 5-12.

Add User User Information User ID: Description:	
Details Password:	
Confirm password:	
Password expires in (da	ays):
🗖 Enforce strict passwo	ord rules
Select Managed Resour	rce Roles
AllSystemResour	ces
Select Task Roles	
C hmcservicerep	
O hmcviewer	
O hmcoperator	
O hmcpe	
C hmcsuperadmin	
OK Cancel Help	
Done	9.3.5.231 🚔

Figure 5-12 Add User window

2. Insert the new user ID, a description of the user ID, the password for the new user ID, and re-enter the new password. Select hmcsuperadmin from Task Roles to create a new user with the System Administrator role. You can select Enforce strict password rules to give the password expiration and type the number of the expiration day as shown in Figure 5-13. (This option sets the password to expire after the number of the days specified.)

Add User					
User Infor	User Information				
User ID:	hmcadmin				
Descripti	ion: HMC Syste	m Adminis	it		
Details					
Passwor	d:	1	****		
Confirm	password:	3	*****		
Passwor	d expires in (da	iys):	180		
🗹 Enford	ce strict passwo	ord rules			
Select M	anaged Resour	ce Roles			
🗹 🗹	ISystemResourc	es:			
Select Ta	ask Roles				
O hr	mcservicerep				
O hr	mcviewer				
O hr	mcoperator				
O hr	mcpe				
Mmcsuperadmin					
OK Cancel Help					
Done				9.3.5.231	

Figure 5-13 Add a new user with Super Administrator role using strict password rules

3. Click **OK** to create a new user. The new user ID is added in User profiles window as shown in Figure 5-14.

Mana	Manage User Profiles and Access					
User	User - Help -					
Select	a User ID be	elow and click "User" to man	age the console users.			
Select	User ID	Description				
0	hscroot	HMC Super User				
0	hscpe	HMC User				
۲	hmcadmin	HMC System Administrator				
0	root	root				
Done			9.3.5.231 🙆			

Figure 5-14 User Profiles user ID list updated

#### Adding a new user with Viewer role

To add a new user with the Viewer role, follow these steps:

- Select User → Add to add a new user. The HMC displays the Add User window as shown in Figure 5-12 on page 186.
- 2. Insert the new user ID, a description of the user ID, the password for the new user ID, and re-enter the new password. Select viewer from Task Roles in order to create a new user with the Viewer role. You can select Enforce strict password rules to give the password expiration and type the number of the expiration day as shown in Figure 5-15. (This option sets the password to expire after the number of the days specified.)

Add User					
User Information					
User I	User ID: hmcviewer				
Descri	ption: HMC View	'er			
Details					
Passv	vord:		*****		
Confir	m password:		*****		
Passv	vord expires in (d	ays):	180		
🗹 Enf	orce strict passw	ord rules			
Select	Managed Resou	rce Roles			
	AllSystemResour	rces			
Select	Task Roles				
0	hmcservicerep				
۲	hmcviewer				
0	hmcoperator				
0	hmcpe				
0	O hmcsuperadmin				
ок	Cancel Help	_			
Depe				0.25.221	
Done				9.3.3.231 🔤	

Figure 5-15 Add a new user with Viewer role using strict password rules

3. Click **OK** to create a new user. The new user ID is added in User profiles window as shown in Figure 5-16.

Manage User Profiles and Access					
User	Help 🗸				
Select a User ID below and click "User" to manage the console users.					
Select	User ID	Description			
۲	hscroot	HMC Super User			
0	hscpe	HMC User			
0	hmcadmin	HMC System Administrator			
0	hmcviewer	HMC Viewer			
0	root	root			
Done				9.3.5.231	

Figure 5-16 User Profiles user ID list updated

The HMC Viewer is given very limited access to functions in the HMC. Figure 5-17 shows the limited menu for the HMC Viewer.

Hardware Management Cor	nsole	
		hmcviewer   Help   Logoff
E Welcom e	HMC Management (HMC)	/ersion ) [Alphabetical List ]
🗉 🗐 Systemis Managemient	Operations	
System Plans HMC Management HMC Management	Test Network Connectivity View Network Topology Tip of the Day View Licenses Change User Interface Settings	<ul> <li>View network diagnostic information about the network protocols for the HMC</li> <li>View, save, and ping current network topology</li> <li>Display tips for using the console</li> <li>Read the licenses for the product</li> <li>Customize the appearance of the HMC workplace</li> </ul>
@ Updates	Adm inistration	
Status: Open Serviceable Events	Change User Password Manage Users and Tasks Change Language and Locale	<ul> <li>Change an existing HMC user's password</li> <li>View the logged on users and the tasks they are running</li> <li>Change the HMC interface language and locale</li> </ul>
Transferring data from 9.3.5.228		9.3.5.228 🚔

Figure 5-17 Very limited menu available for HMC Viewer user

#### 5.2.3 Customizing user task roles and managed resource roles

You can customize HMC Task Roles and Managed Resource Roles through the HMC console. You can add new Task Roles and Managed Resource Roles based on existing roles in the HMC. System defined roles cannot be modified, but you can create a new role based on system defined role or existing role.

To manage access task and resource roles, select **HMC Management**  $\rightarrow$  **Administration**  $\rightarrow$  **Manage Access Task and Resource Roles**. The Customize User Controls window displays as shown in Figure 5-18.

Manage Task and Resource Roles Edit▼ Help▼				
Select a Role below and click "Edit" to manage the def Managed Resource Roles C Task Roles Select Managed Resource Roles AllSystemResources	ïned role.			
Done	9.3.5.231 🙈			

Figure 5-18 Customize User Controls window

## Creating, copying, modifying, or deleting managed resource roles

A managed resource role assigns permissions for a managed object or group of objects, such as a managed system or a logical partition. In a managed resource role, you can define access to specific managed systems rather than all managed system controlled by the HMC.

You can create a new managed resource role, copy an existing managed resource role, modify existing managed resource roles, or delete an existing managed resource role from the Customize User Controls window. Select **Managed Resource Roles**, then select the desired operation from the Edit menu. By default, there is only one managed resource role: it is *AllSystemResources*.

To create a new managed resource role:

- 1. Click **Edit**  $\rightarrow$  **Add**, and the Add Role window displays.
- 2. Enter the name for the new managed resource role, and choose the resource role from which the new managed resource role objects will be based.
- 3. Select which object is available for the new managed resource role, then click **Add** to add them to the new managed resource role current objects.
- 4. Click **OK** to create a new managed resource role.

Figure 5-19 shows an example of creating a new managed resource role.



Figure 5-19 Add a new managed resource role

To copy a managed resource role, select the desired managed resource role and select **Edit**  $\rightarrow$  **Copy**. You cannot copy a user defined managed system role created from the **Add** menu, but you can copy system defined managed resource roles, which is AllSystemRoles. From the Copy Role window, you can also customize the object configurations for a new copy of managed resource role.

To delete a managed resource role, select desired managed resource role and select **Edit**  $\rightarrow$  **Remove**. A verification window displays as shown in Figure 5-20.

O Delete Item Verification				
Are you sure you want to delete this item? ACT03005 Yes No				
Done 9.3.5.231 🚔				

Figure 5-20 Delete managed resource or task role verification

To modify existing managed resource roles, select a managed resource role you want to change, and select **Edit**  $\rightarrow$  **Modify**. You can change the objects' configuration, then click **OK** to save the changes.

#### Creating, copying, modifying, or deleting task roles

A task role defines the access level for a user to perform tasks on the managed object or group of objects, such as a managed system or logical partition. There are five system defined task roles:

- hmcservicerep
- hmcviewer
- ► hmcoperator
- ► hmcpe
- ► hmcsuperadmin

You can create a new task role, copy an existing task role, modify an existing task role, or delete an existing task role from the Customize User Controls window. You cannot modify or remove system defined task roles. Select **Task Roles**, then select the desired operation from the **Edit** menu.

To create a new user task role:

- 1. Click **Edit**  $\rightarrow$  **Add**, and the Add Role window displays.
- 2. Enter the name for the new managed resource role, and choose the task role from which the new task role objects will be based.
- 3. Select which object will be available for the new task role, and then click **Add** to add them to new task role current objects.

4. Click **OK** to create a new task role. Figure 5-21 shows an example of creating a new task role.

Add Role		
Role name:	UserAdmin	
Based on:	hmcsupera	admin 🗾
Available Tasks		Current Tasks
🕒 <u>WUI Permission</u>	Add	🖻 <u>WUI Permission</u>
⊕- <u>Frame</u>	Remove	⊕ <u>Frame</u>
		<u>■ Managed System</u>
Logical Partition		Logical Partition
<sup>ter</sup> <u>HMC Console</u>		<sup>te⊢</sup> <u>HMC Console</u>
OK Cancel Help		
Done		9.3.5.231 🙆

Figure 5-21 Add user role

To copy a task role, select the desired task role and select **Edit**  $\rightarrow$  **Copy**. From the Copy Role window, you can also customize the object configurations for a copy of the task role.

To delete a task role, select the desire task role an select **Edit**  $\rightarrow$  **Remove**. a verification window will be shown as in Figure 5-20 on page 193. System defined task roles cannot be removed.

To modify existing task roles, select a task role you want to change, and select **Edit**  $\rightarrow$  **Modify**. You can change the objects' configuration, then click **OK** to save the changes. Only user defined task roles that are created by HMC users can be modified.

# 6

# Network configuration and the HMC

This chapter provides a general overview of the types of network configurations for the Hardware Management Console (HMC) and explains how to configure HMC network settings. This chapter also describes how to use the HMC workplace to obtain network diagnostic information.

### 6.1 Types of HMC network configurations

The HMC supports several network communications:

- HMC to managed system connection performs most of the hardware management functions in which HMC issues control function requests through service processor of the managed system.
- HMC to logical partition connection collects platform related information, such as hardware error events or hardware inventory, from the operating system running in the logical partitions, as well as coordinates certain platform activities, such as DLPAR or concurrent maintenance with those operating systems.
- HMC to remote users connection provides remote users with access to HMC functionally. Remote users can access the HMC using:
  - The remote operation to access all the HMC GUI functions remotely.
  - SSH to access the HMC command line functions remotely.
  - A virtual terminal server for remote access to virtual logical partition consoles.
- ► *HMC to service and support connection* transmits data such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communication path to make automatic service calls.

### 6.2 Configuring HMC network settings

This section describes network configuration for the HMC. To open the Change Network Setting window, select **Change Network Settings** from the main menu.

#### 6.2.1 HMC Identification

HMC identification provides information that is needed to identify the HMC in the network. The Identification tab of the Change Network Settings window (Figure 6-1) includes the following information:

Console name

HMC name that identifies the console to other consoles in the network. This name is short host name.

► Domain name

An alphabetic name that the Domain Name Services (DNS) can translate to the IP address.

► Console Description

Short description for the HMC.

Change N	Jetwork Settir	ngs		
Identification	LAN Adapters	Name Services	Routing	1
Use the fr Specify ho computer. Console name: Domain name:	ollowing informa st name, doma localhost localdom	ation to identify s in name, and a s ain	your console short descript	on the network. ion of this
Console descrip	otion:			
OK Cancel He	эlр			
Ē			📄 🔒 🥑 Ir	nternet

Figure 6-1 HMC Identification tab

#### 6.2.2 LAN Adapters

The LAN Adapters tab (Figure 6-2) shows a summarized list of all Local Area Network (LAN) adapters that are installed on the HMC. You can view details of each LAN adapter by clicking **Details**, which launches a window that allows you to change LAN adapter configuration and firewall settings.

Change Network Setti	ings		
Identification LAN Adapters	Name Services	Routing	
LAN Adapters Ethernet eth0 00:11:25:0 Ethernet eth1 00:0D:60:0 Details OK Cancel Help	)6:82:89 (192.16 )B:46:CA (9.3.5.2	8.128.1) 231)	
E Done		Internet	

Figure 6-2 LAN Adapters tab
### LAN Adapter configuration

The LAN Adapter Details window, shown in Figure 6-3, describes the LAN adapter configuration of Ethernet eth0 on the LAN Adapter tab.

모 LAN Adapter Details
LAN Adapter Firewall Settings
Local Area Network Information LAN interface address: 00:11:25:06:82:89 eth0
Private O Open     Media Speed (ethernet)     Autodetection
<ul> <li>Partition communication</li> </ul>
DHCP Server Enable DHCP server Address Range 192.168.128.2 - 192.168.255.254
DHCP Client/IP Address
Obtain an IP address automatically     Specify an IP address     TCP/IP interface address:     192.168.128.1
TCP/IP interface network mask: 255.255.128.0
OK Cancel Help
🖹 Done

Figure 6-3 LAN Adapter configuration

The LAN Adapter tab of this window includes the following information:

Local Area Network Information

The LAN interface address shows Media Access Control (MAC) Address on the card and the adapter name. These values uniquely identify the LAN adapter and cannot be changed. A private network is used by the HMC to communicate by its managed system and an open network connect the HMC outside the managed system. Media speed specifies the speed in duplex mode of an Ethernet adapter. The options are Autodetection, 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, or 1000 Mbps Full Duplex. The connection between the HMC and its managed systems can be implemented either as a private or open network. The term open refers to any general, public network that contains elements other than HMCs and service processors that is not isolated behind an HMC. The other network connections on the HMC are considered open, which means that they are configured in a way that you would expect when attaching any standard network device to an open network.

In a private service network, however, the only elements on the physical network are the HMC and the service processors of the managed systems. In addition, the HMC provides Dynamic Host Configuration Protocol (DHCP) services on that network, which allow it to automatically discover and assign IP configuration parameters to those service processors. You can configure the HMC to select one of several different address ranges to use for this DHCP service, so that the addresses provided to the service processors do not conflict with addresses used on the other networks to which the HMC is connected. The DHCP services allow the elements on the private service network to be automatically configured and detected by the HMC, while at the same time preventing address conflicts in the network.

On a private network, therefore, all of the elements are controlled and managed by the HMC. The HMC also acts as a functional firewall, isolating that private network from any of the open networks to which the HMC is also attached. The HMC does not allow any IP forwarding; clients on one network interface of the HMC cannot directly access elements on any other network interface.

To take advantage of the additional security and ease of setup, implement service network communications through a private network. However, in some environments, this is not feasible because of physical wiring, floor planning, or control center considerations. In this case, the service network communications can be implemented through an open network. The same functionality is available on both types of networks, although the initial setup and configuration on an open network require more manual steps.

DHCP Server

Choose **Enable DHCP Server** only if this adapter is defined as private network, then choose one range of addresses for the DHCP Server to distribute. If the adapter is defined as open, this setting is not available.

If you want to configure the first network interface as a private network, you can select from a range of IP addresses for the DHCP server to assign to its clients. The selectable address ranges include segments from the standard nonroutable IP address ranges.

In addition to these standard ranges, a special range of IP addresses is reserved for IP addresses. This special range can be used to avoid conflicts in cases where the HMC-attached open networks are using one of the

nonroutable address ranges. Based on the range selected, the HMC network interface on the private network will be automatically assigned the first IP address of that range, and the service processors will then be assigned addresses from the rest of the range.

The DHCP server in the HMC uses automatic allocation, which means that each unique service processor Ethernet interface will be reassigned exactly the same IP address each time it is started. Each Ethernet interface has a unique identifier based upon a built-in MAC address, which allows the DHCP server to reassign the same IP parameters.

► DHCP Client/IP address

There are two options:

- *Obtain an IP address automatically* allows the HMC to obtain an available IP address automatically.
- Specify an IP address specifies an IP address to be used, providing TCP/IP interface address and TCP/IP interface network mask.

### **Firewall Settings**

You use the Firewall Settings tab of the LAN Adapter Details window to view and change current firewall adapter settings for the specified LAN interface address. Select **Allow Incoming** to allow access to incoming network traffic from this address, or select **Allow Incoming by IP Address** to allow access by incoming network traffic from hosts specified by an IP address and network mask, as shown in Figure 6-4.

	apter Firewall Settings						
N int	erface address: 00:11:25:06:8:	2:89 Ethernet					
ailab	ole Applications	-				_	Allow Incoming
Select	t Application Name	Ports					Allow Incoming by IP Address
•	Secure Shell	22:tcp			-		Allow remote Secure
0	Secure Remote Web Access	443:tcp 8443:tcp 9960:tcp	0				Shell access.
0	Open Pegasus	5989:tcp					
0	RMC	657:udp 657:tcp					
					1 (iii		
lowed	Hosts	9920:tcp 9900:udp				-	Remove
lowed	Hosts	9920:tcp 9900:udp	Allow	und Ho	ctc	•	Remove
lowed Select	FCS d Hosts t Application Name Open Pegasus	9920:tcp 9900:udp  Ports 5989:tcp	Allov 0.0.0	<b>ved Ho</b> .0/0.0.(	sts	✓	Remove
lowed Select	Hosts t Application Name Open Pegasus RMC	9920:tcp 9900:udp  Ports 5989:tcp 657:udp tcp:657	Allov 0.0.0 0.0.0	<b>ved Ho</b> .0/0.0.1	sts 0.0	<ul> <li>▲</li> </ul>	Remove
lowed Select	FCS d Hosts t Application Name Open Pegasus RMC FCS	9920:tcp 9900:udp  Ports 5989:tcp 657:udp tcp:657 9920:tcp udp:9900	Allov 0.0.0 0.0.0	<b>ved Ho</b> .0/0.0.1 .0/0.0.1	sts 0.0 0.0	•	Remove
C Select	Hosts t Application Name Open Pegasus RMC FCS VTTY	9920:tcp 9900:udp  Ports  5989:tcp 657:udp tcp:657 9920:tcp udp:9900 9735:tcp	Allov 0.0.0 0.0.0 0.0.0 0.0.0	<b>ved Ho</b> .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 5.0 5.0 5.0 5.0	<ul> <li>▲</li> </ul>	Remove
lowed Select	Hosts t Application Name Open Pegasus RMC FCS VTTY VTTY VTTY Proxy	9920:tcp 9900:udp  Ports  5989:tcp  657:udp tcp:657  9920:tcp udp:9900  9735:tcp  2302:tcp	Allov 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	<b>ved Ho</b> .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 0.0 0.0 0.0 0.0 0.0 0.0	•	Remove
C Select	FCS d Hosts t Application Name Open Pegasus RMC FCS VTTY VTTY VTTY Proxy 5250	9920:tcp         9900:udp           Ports         5989:tcp           657:udp         tcp:657           9920:tcp         udp:9900           9735:tcp         2302:tcp           2302:tcp         2300:tcp	Allov 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	ved Ho .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 0.0 0.0 0.0 0.0 0.0 0.0 0.0	•	Remove
lowed Select	FCS d Hosts t Application Name Open Pegasus RMC FCS VTTY VTTY VTTY Proxy 5250 Incoming Ping	9920:tcp         9900:udp           Ports         5989:tcp           657:udp         tcp:657           9920:tcp         udp:9900           9735:tcp         2302:tcp           2300:tcp         tcp:2301           echo-request:icmp         1	Allow 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	ved Ho .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	•	Remove
lowed Select	FCS d Hosts t Application Name Open Pegasus RMC FCS VTTY VTTY Proxy 5250 Incoming Ping L2TP	9920:tcp         9900:udp           Ports         5989:tcp           657:udp         tcp:657           9920:tcp         udp:9900           9735:tcp         2302:tcp           2300:tcp         tcp:2301           echo-request:icmp         1701:udp	Allov 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	ved Ho .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	•	Remove
	FCS d Hosts t Application Name Open Pegasus RMC FCS VTTY VTTY Proxy 5250 Incoming Ping L2TP SLP	9920:tcp         9900:udp           Ports         5989:tcp           657:udp         tcp:657           9920:tcp         udp:9900           9735:tcp         2302:tcp           2302:tcp         tcp:2301           echo-request:icmp         1701:udp           427:udp         tdp	Allov 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	<b>ved Ho</b> .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1 .0/0.0.1	sts 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.		Remove

Figure 6-4 Firewall Settings tab

### 6.2.3 Name Services

You use the Name Services tab to specify Domain Name Services (DNS) for configuring the console network settings (Figure 6-5). DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. With DNS, people can use names to locate a host, rather than using the IP address.

Change Network Settings
Identification LAN Adapters Name Services Routing
DNS Configuration DNS enabled DNS Server Search Order Add 9.3.4.2 Remove
Domain Suffix Search Order Add Remove
OK Cancel Help

Figure 6-5 Name Services tab

# 6.2.4 Routing

On the Routing tab, you specify routing information for configuring the console network settings, such as add, delete, or change routing entries and specify routing options for the HMC as shown in Figure 6-6.

Change	e Network Set	tings		
Identification	LAN Adapters	Name Services	Routing	
Routing Infor	mation			
Select Type	Destination	Gateway	Subnet Mask	Interface
<ul> <li>Net</li> </ul>	192.168.128.0	192.168.128.1	255.255.128.0	eth0
Default Gates Gateway ad	vay Informatio dress 9.3.4.1	n Gateway de	vice	
🗖 Enable	'routed'			
OK Cancel	Help			
🞒 Done			🔒 🥑 Interne	et 🛛

Figure 6-6 Routing configuration

### **Routing Information**

The routing information displays the following information:

- ► *Type* displays the specific route, which can be on of three choices:
  - Net

Specifies a network-specific route. The destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for that network are using the TCP/IP address of the router, unless a host route also applies for the communication to the destination host address.

**Note**: When a conflict occurs between a host and net route, the host route is used.

- Host

Specifies a host-specific destination. The destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

Default

Specifies all destinations not defined with another routing table entry. With a default route, the destination address is all zeros. If no host or net routes apply when communicating with a destination host address, the communication is routed through the default router using the TCP/IP address given by the router address.

- Destination displays the TCP/IP address of the destination host, network, or subnet.
- Gateway displays the TCP/IP address of the next hop in the path to the destination.
- Subnet Mask displays the subnet mask used by network interface to add routes
- Interface displays the name of the network interface that is associated with the table entry.

### **Default Gateway Information**

The Default Gateway Information provides:

► Gateway address

The default gateway is the route to all networks. It informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source

► Gateway device

Network interface that is used as gateway device.

### The Enable "routed" option

You use the *Enable "routed"* option to enable or disable the network routing daemon, *routed*. If disabled, it stops the daemon from running and prevents any routing information from being exported from this HMC.

# 6.3 Testing network connectivity

You can use the HMC workplace to obtain network diagnostic information about the HMC's network protocols. You can use the Test Network Connectivity window to access any of the following functions:

- ► Ping
- Interfaces
- Address
- Routes
- ARP (Address Resolution Protocol)
- Sockets
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- IP (Internet Protocol)

This section explains each of these functions. To open the Test Network Connectivity window, select **Test Network Connectivity** on the main window.

### 6.3.1 Ping

Use the Ping function to send an echo request (ping) to a remote host to see whether the host is accessible and to receive information about that TCP/IP address or name. Specify any TCP/IP address or name in the TCP/IP Address or Name to Ping field, then click **Ping** as shown in Figure 6-7.

Test	Network Co	onnectivi	ty					
Ping	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP
TCP/I *	P Address o	r Name to	Ping					
Cance	el Help							

Figure 6-7 Network Diagnostic Information - Ping

The result for that TCP/IP address or name displays as shown in Figure 6-8.

J [	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP
11	Address	or Name to	Ping					
з.	5.228		1					
ſĢ	9.3.5.228	(9.3.5.228	100/12	8) byt	es of dat	a.		
b	ytes from	9.3.5.228:	icmp se	g=l tt	1=64 time	=0.19	9 ms	
3 b	ytes from	9.3.5.228:	icmp se	- q=2 tt	:1=64 time	=0.16	9 ms	
зb	ytes from	9.3.5.228:	icmp_se	q=3 tt	:1=64 time	=0.182	2 ms	
8 b	ytes from	9.3.5.228:	icmp_se	q=4 tt	:1=64 time	=0.17	8 ms	
зb	ytes from	9.3.5.228:	icmp_se	q=5 tt	l=64 time	=0.179	9 ms	
- 9	.3.5.228 p	ing statis	tics					
pac	kets trans	mitted, 5	received	, 0% p	acket los	s, ti	ne 4002	2ms
: m	in/avg/max	/mdev = 0.	169/0.18	1/0.19	9/0.015 m	13		
g								
	Holp							
CEI	Tieth							

Figure 6-8 Network Diagnostic Information - Ping result

### 6.3.2 Interfaces

The Interfaces tab displays the statistics for the network interfaces that are configured currently as shown in Figure 6-9. To update the information that is displayed with the most recent information, n click **Refresh**.

Test Network Co	onnectivi	ty						
Ping Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP	
Kernel Interface Iface MTU Met RX eth0 1500 0 3108 eth1 1500 0 6179 lo 16436 0 25897 s10 576 0 0 0 0 Refresh	table -OK RX-ER 4 0 0 0 1 4 0 0 0 1 0 0 0 0 2 0 1 0 0 0	R RX-DRP 6763 0 0 3110 0 0 58970 0 ( MOPRU	RX-OVR O BMRU O BMRU D O LRU	а ТХ-ОК Т. Г	X-ERR	TX-DRP	TX-OVF	ξ
Cancel Help								
Ĵ					<u></u>	🥑 Inter	rnet	

Figure 6-9 Network Diagnostic Information - Interfaces

# 6.3.3 Address

The Address tab displays TCP/IP addresses for the configured network interfaces. To update the information that is displayed with the most recent information, click **Refresh** as shown in Figure 6-10.

Ping Inte	erfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP
ethO Lini inet add UP BROAD RX packe TX packe collision RX bytes Base add ethl Lini inet add UP BROAD RX packe Collision RX packe collision RX packe collision RX packe collision RX packe Collision RX packe Collision RX packe	<pre>#Taces &amp; encap r:192.1 CAST RU ts:3172 ts:1709 ns:0 tx :569960 ress:0x &amp; encap r:9.3.5 CAST RU ts:6268 ts:1318 ns:0 tx :640232 encap:L r:127.0 ACK RUN Help </pre>	Address :Ethernet 68.128.1 B NNING MULT 0 errors:0 queuelen:1 2 (5.4 Mb) 2840 Memor :Ethernet .231 Bcast NNING MULT 7 errors:0 queuelen:1 9 (6.1 Mb) ocal Loopb .0.1 Mask: NING MTU:1	Routes HWaddr 00 cast:192 TCAST MTT dropped: 000 TX byte: y:e812000 HWaddr 00 :9.3.5.2 TCAST MTT dropped dropped 000 TX byte: ack 255.0.0.1 6436 Met:	ARP 0:11:2. 168.2. J:1500 0 ove: 0 ove: 0 ove: 0:29700 00-e81. 0:0D:6 55 Masl J:1500 0 ove: 0 ove: 0 ove: 155 Masl J:1500 0 ove: 155 Masl J:1500 0 ove: 155 Masl J:1500 0 ove: 155 Masl J:1500 0 ove: 155 Masl J:1500 0 ove: 155 Masl J:1500 155 Masl J:1500 1	Sockets 5:06:82:8 55.255 Ma Metric:1 rruns:0 f rruns:0 c 305 (2.8 7 40000 0:0B:46:C x:255.255 Metric:1 rruns:0 f rruns:0 c 4151 (12.	TCP 9 sk:255 rame:0 arrier Mb) A .254.0 rame:0 arrier 1 Mb)	UDP 255.1	1P 28.0

Figure 6-10 Network Diagnostic Information - Address

### 6.3.4 Routes

The Routes tab displays the Kernel routing table and corresponding network interfaces. You can click **Refresh** to update the information that is displayed with the most recent information as shown in Figure 6-11.

Test	Network C	onnectiv	ity					
Ping	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP
Kern Dest	el IP routi: ination Gat	ng table eway Genm	ask Flags	MSS W	indow irt	t Ifac	:e	
207. 129.	25.252.196 42.160.16 9	9.3.4.1 2 .3.4.1 25	55.255.25 5.255.255	5.255 .255 U	UGH O O O GH O O O	ethl		
9.3. 192.	4.0 0.0.0.0 168.128.0 1	255.255. 92.168.12	254.0 U 0 8.1 255.2	0 0 e	thl .0 UG 0 0	0 eth	ιO	
10.2	53.0.0 0.0. 254.0.0 0.0	0.0 255.2	55.0.0 U 255.0.0 U	000	sl0 eth0			
127.	0.0.0 0.0.0	.0 255.0. 0.0.0.0	0.0 U O O UG O O O	ethl				
Canc	el Help							
Done						<u>a</u>	Internet	:

Figure 6-11 Network Diagnostic Information - Routes

# 6.3.5 ARP

The ARP tab displays the Address Resolution Protocol (ARP) connections. ARP is used to find the host's hardware address if only the network layer address is known and is usually used to translate an IP address to a MAC address. To update the information that is displayed with the most recent information, you can click **Refresh** as shown in Figure 6-12.

ing	Inter	faces	A	ddress	Rou	tes	AR	P	<u>So</u>	ck	ets	ТСР	U	DP	ΙP
TP a	dres	ः माग	type	e Flage	HIJ S	addre	99	Ма	sk D			-			
192.	168.2	55.25	53 Ox	1 0x0	00:00	):00:	00:	00	:00	120	eth(	5] )			
192.	168.2	55.25	54 Ox	1 0x2	00:14	4:5E:	4F:	OA	:78	*	eth0	)			
192.	168.2	54.25	55 Ox	(1 0x2	00:14	4:5E:	4F:	10	:EE	*	eth0	)			
9.3.	4.1 0:	x1 O>	2 00	):0F:23	:6E:0		*	et	hl						
9.3.	4.2 0	x1 0>	2 00	):CO:49	:D5:D	)8:DF	*	et	hl						
9.3.	5.114	0x1	0x2	BA:33:	BA:C3	3:30:	04	*	ethl						
9.3.	5.171	0x1	0x2	00:0D:	60:0E	8:66:	13	*	ethl						
9.3.	5.229	0x1	0x2	00:0D:	60:0E	3:31:	6C	*	ethl						
9.3.	5.228	0x1	0x2	00:0D:	60:OE	8:38:	57	*	ethl						
9.3.	5.194	0x1	0x2	00:14:	5E:5H	7:1E:	AO	*	ethl						
9.3.	4.128	0x1	0x2	00:0D:	60:22	2:AF:	СВ	*	ethl						
9.3.	5.129	0x1	0x2	00:0D:	60:04	A:51:	ΕO	*	ethl						
9.3.	5.128	0x1	$0 \times 0$	00:00:	00:00	:00:	00	*	ethl						
Refr	esh														
Jance	ei He	elp													

Figure 6-12 Network Diagnostic Information - ARP

## 6.3.6 Sockets

Use the Sockets tab to display information about TCP/IP sockets. Socket is a communication endpoint on the IP network. To update the information that is displayed with the most recent information, click **Refresh** as shown in Figure 6-13.

Test Network Connectivity	
Ping Interfaces Address Routes ARP Sockets TCP UDP IP	
Active Internet connections (servers and established)	
Proto Recv-Q Send-Q Local Address Foreign Address State	
tcp 0 0 0.0.0.0:9920 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.0:9090 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.0:8899 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.0:5988 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.0:5989 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0:9318 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.9735 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.9960 0.0.0.* LISTEN	
tcp 0 0 0.0.0.0:6060 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.9197 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.8877 0.0.0.0:* LISTEN	
tcp 0 0 127.0.0.1:32781 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.8080 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0:6000 0.0.0:* LISTEN	
tcp 0 0 0.0.0.0:6288 0.0.0.0:* LISTEN	
tcp 0 0 0.0.0.0132849 0.0.0.0.* LISTEN	
tcp 0 0 0.0.0.0557 0.0.0.0* LISTEN	
tcp U U U.U.U.6289 U.U.U.U:* LISTEN	
Refresh	
Cancel Help	
🔄 Done	1

Figure 6-13 Network Diagnostic Information - Sockets

# 6.3.7 TCP

The TCP tab displays information about Transmission Control Protocol (TCP) connections. To update the information that is displayed with the most recent information, click **Refresh** as shown in Figure 6-14.

Test	Network C	onnectiv	ity									
Ping	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP				
ActiProttcp	Interfaces ve Internet o Recv-Q Se 0 0 localho 0 0 localho 44 0 localh 44 0 localh 44 0 localh 44 0 localh 44 0 localho 0 localho	Address connecti nd-Q Loca st.:ccfwin st.locald st.locald st.locald st.locald st.locald st.locald st.locald st.locald st.locald ost.local ost.local ost.local ost.local ost.local ost.local st.local st.local st.local st.local st.local	Routes           ons (w/o           1 Address           nterhmc           om:6288           os:32865           os:32865           os:32865           os:32856           os:32856           os:32856           os:32856           os:32856           os:32856           os:32856           os:32856           os:32856           os:35965           do:36108           do:36110           do:36110           do:36107           do:36112           c-https	server server s Fores js21al localho l	sockets rs) ign Addre .itsc.aus ost.local ost.local ost.local ost.local ost.local .itsc.aus ost.local host.locas host.locas host.locas host.locas host.locas host.locas host.locas	ss Sta sti:397 .do:361	te 17 EST 12 FIN mc EST 88 EST 10 FIN 11 FIN 03 EST 1t EST 1t EST 288 CL 288 CL 288 CL 288 CL 288 CL 288 CL 288 CL 288 CL 288 CL	ABLIS WAIT WAIT ABLIS ABLIS ABLIS WAIT ABLIS ABLIS OSE_W OSE_W OSE_W OSE_W OSE_W OSE_W OSE_W OSE_W	HED 2 2 HED ED HED 2 2 HED HED AIT AIT AIT AIT AIT AIT HED			
Canc	el Help											
Ē										📀 Int	ernet	

Figure 6-14 Network Diagnostic Information - TCP

# 6.3.8 UDP

Use the UDP tab to display information about User Datagram Protocol (UDP) statistics as shown in Figure 6-15. To update the information that is displayed with the most recent information, click **Refresh**.

Test	Network C	onnectiv	ity								
Ping	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP			
Activ Proto udp 0 udp 0 udp 0 udp 0 udp 0 udp 0 udp 0 udp 0 Cance	<pre>re Internet 0 Recv-Q Se: 0 0 *:filen 0 0 *:filen 0 0 *:rmc * 0 0 *:l2tp 0 0 *:svrlo 0 0 *:iua * 0 0 *:bootp 0 0 *:bootp ssh</pre>	connecti nd-Q Loca et-tms *: et-rpc *: :* c *:* :* s *:* s *:* s *:*	ons (onl) 1 Addres: * *	y serv 3 Fore:	ers) ign Addre	ss Sta	te				
ē									) 🥑 Int	ernet	

Figure 6-15 Network Diagnostic Information - UDP

# 6.3.9 IP

The IP tab displays the IP and corresponding network interfaces. You can click **Refresh** to update the information that is displayed with the most recent information as shown in Figure 6-16.

Test	Network C	onnectiv	ity					
Ping	Interfaces	Address	Routes	ARP	Sockets	ТСР	UDP	IP
Acti Prot tcp tcp tcp tcp tcp tcp tcp tcp tcp tc	<pre>ve Internet o Recv-Q Se 0 0 9.3.5.2 0 0 127.0.0 44 0 127.0. 44 0 127.0. 44 0 127.0. 44 0 127.0. 44 0 127.0. 44 0 127.0. 0 0 9.3.5.2 0 0 9.3.5.2 0 0 9.3.5.2 0 0 9.3.5.2 0 0 127.0.0 0 0 127.0.0 esh</pre>	connecti nd-Q Loca 31:9920 9 31:32865 31:9960 9 .1:32856 31:8443 9 31:9920 9 31:8443 9 31:35322 .1:35965 0.1:36181 0.1:36183 0.1:36184 31:8443 9 31:33021 31:9920 9 .1:32791 .1:32788	nons (w/o 1 Addres 3.5.228 9.3.5.17 .3.4.128 127.0.0. .41.222. .3.5.229 .41.222. 127.0.0 127.0.0 127.0.0 127.0.0 127.0.0 127.0.0 3.4.128 9.3.5.121 .3.5.171 127.0.0. 127.0.0	serve s Fore : 39717 1:9920 : 2381 1:6288 193:30 : 42803 193:30 1:8080 1:8080 1:8080 1:8080 1:8080 1:628 .1:6288 .1:6288 .1:6288 .1:6288 .1:6288 .1:6288 .1:6288 .1:6288 .1:62888 .1:62888 .1:62888 .1:628888 .1:6288888 .1:62888888888888888888888888888888888888	rs) ign Addre ESTABLIS ESTABLISH ESTABLISH ESTABLIS 44 ESTABLIS 54 ESTABLIS 54 ESTABLIS 8 CLOSE_W 8 STABLISH ESTABLIS ESTABLIS ESTABLIS	SS Sta HED ED HED ISHED HED ISHED HED AIT AIT AIT ED HED HED HED HED	te	
Done						🥝 Inte	rnet	

Figure 6-16 Network Diagnostic Information - IP

# 6.4 Viewing network topology

Use the Network Topology window to see a tree view of the network nodes known to this HMC (Figure 6-17). Examples of such nodes are managed systems, logical partitions, storage, and other HMCs. You can view attributes of a node by selecting the node in the tree view that is shown in the left pane under Current Topology. Attributes vary according to the type of node. Some examples are IP address, host name, location code, and status. Click **Refresh** to rediscover the topology and to query the nodes again for status and other attributes.



Figure 6-17 Network Topology

Table 6-1 shows the possible status for each node.

Node	Possible Status
Local HMC	All nodes OK, Some nodes failed, All nodes failed
Remote HMC	Online, Offline
Interface	No link, Half duplex link, Full duplex link
Storage Facility	Status not reported
Managed system	Managed system status reported by the <b>1ssyscfg</b> command (Operating, Running)
FSP	Online, Offline
LPAR	LPAR status reported by the <b>1sstscfg</b> command. LPARs can also carry a connection status to report their current network status as Active, On, Off, Offline
BPA	BPA status reported by the 1ssyscfg command
BPC	Online, Offline

 Table 6-1
 Possible status for each node

Each status has its meaning which is evaluated when determining cumulative status for the Local HMC node, as shown in Table 6-2.

Table 6-2 Meaning of node status

Status	Evaluation for cumulative status (OK/Fail)	Meaning
All nodes OK	ОК	Child node statuses are OK
Some nodes failed	Fail	One or more child node statuses failed
All nodes failed	Fail	All child nodes statuses failed
No link	Fail	No link detected on interface
Half duplex link	ОК	Half duplex link detected on interface
Full duplex link	ОК	Full duplex link detected on interface
Active	ОК	LPAR is pingable and known to RMC
On	Fail	LPAR is pingable but not known to RMC
Off	Fail	LPAR is not pingable nor known to RMC

Status	Evaluation for cumulative status (OK/Fail)	Meaning
Offline	Fail	For LPARs: LPARs is not pingable but is known to RMC For Remote HMCs: Remote HMC is not pingable but is known to this HMC For FSPs, BCPs: FSP or BPC are not pingable
Online	ОК	Remote HMC is pingable FSP is pingable BPC is pingable
Unknown	Fail	Status window be determined
Operating, Running, or any other text from 1ssyscfg	N/A	Not evaluated when determining the cumulative status

This task also allows you to save a snapshot of the current topology and to view that saved reference topology. You can view attributes of a node in this saved topology by selecting the node in the tree view that is shown in the left pane under Saved Topology.

To test network connectivity to a node, you can select the node in either the current or the saved topology and click Ping Current Node or Ping Saved Node, available only for nodes that include an IP address or a host name.

# 7

# Partitioning

This chapter discusses the various ways to create partitions on POWER5 and POWER6 systems using the Hardware Management Console (HMC).

**Note:** The System Planning Tool and system plans are closely tied to this topic. For more information on the System Planning Tool, see *IBM System i and System p*, SG24-7487.

You can use the HMC graphical user interface or the command line interface to create the LPARs. Each LPAR will have one or more profiles that includes the settings that are used when the LPAR is turned on. Multiple profiles allow you to save multiple configurations for a single LPAR, giving you the ability to configure an LPAR to handle different workloads and to save that information to make it easily repeatable and scheduled.

# 7.1 Partitioning concepts

HMC Version 7 includes three significant changes in how resources are handled with managed server partitions. The changes for POWER6 managed servers include:

Host Ethernet adapter

The configuration of the host Ethernet adapter for your POWER6 server has a separate configuration area on the HMC. See 7.1.1, "Host Ethernet Adapter" on page 221 for information.

Shared pool usage of dedicated capacity

On POWER6 servers, you can configure dedicated partitions to become processor donors for idle processors they own. See 7.1.2, "Shared pool usage of dedicated capacity" on page 223 for information.

Partition availability priority

This function allows you to configure a partition hierarchy of availability for when a processor fails. See 7.1.3, "Partition availability priority" on page 225 for information.

# 7.1.1 Host Ethernet Adapter

On POWER6 servers only, the configuration of the integrated Host Ethernet Adapter for partitions is handled in a different area. To get to the Host Ethernet Adapter area:

 In the HMC workplace window, select Systems Management → Servers then select the name of the server. Select Hardware → Adapters → Host Ethernet to open the window shown in Figure 7-1.

					×				
Host Ethernet Adapters : 9117-M	MA-SN1	0FFE0B-L	9						
Chaose a Physical Location Code to view / modify that Host Ethernat Adapter's information									
	VIEW / II	iouny that i	iost Ethernet A	apter 5 miormation.					
U789D.001.DQDVWZK-P1									
Select a physical port of the HostEth	arnat Ad	antor in the	table below to	display the port's currer	t partition usage				
Select a physical point of the HostEth	ennet Au	apter in the		uispiay the poils curren	n parunon usage.				
Current Status									
Select Physical Port Location Codes	Port ID	Port Type	Port Group ID	Port Group MCS Value	Connection State				
O C10-T2	0	1 G	2	4	up				
<ul> <li>C10-T1</li> </ul>	1	1 G	2	4	down				
Configure									
Logical Partition Usage									
Logical Partition Logical Port ID Log	ical Port	DRC Nam	e Logical Port	humed-in MAC / user-d	efined MAC Cana				
Eoglean annion Eoglean on ib Eog	icai i on	DHUMan	le Logical Port	bumed-in MAO / dser-d	enneu MAO Oapa				
OK Cancel Help									
					-				
•					Þ				

Figure 7-1 Host Ethernet Adapter configuration

2. Select the Ethernet adapter that you want to configure, and then select **Configure** to open the window shown in Figure 7-2. Here you can set the network adapter speed, duplex mode, packet size, and default partition control for the integrated controller. These numbers depends on the type of network switch to which you are connecting the server.

HEA Physical Port Configu	ration : 9117-MMA-SN10FFE0B-L9
Use the fields below to specify physical port.	the configuration for the selected
Speed: 1 Gbps	Duplex: full
Maximum receiving packet size: 1500 non-jumbo frame	Pending Port Group Multi-Core Scaling value: 4
☑ Flow control enabled	Promiscuous LPAR: VIOS1_L9
OK Cancel Help	

Figure 7-2 Configure Host Ethernet Adapter

3. When you have finished, select **OK** and your selections are saved.

# 7.1.2 Shared pool usage of dedicated capacity

Beginning with POWER6, HMC V7 R3 allows for the shared use of dedicated processing resources. The option to donate resources is turned off by default when partitions are created as *Dedicated* and can be configured through the partition property window. (To read about how to create a dedicated partition, see "Configuring a dedicated processor partition" on page 236.)

To verify that your system is capable of sharing dedicated capacity:

 In the HMC workplace window, select Systems Management → Servers then select the name of the server. Select Tasks → Properties to open the window shown in Figure 7-3.

eneral	Processors	Memory	1/0	Power-On Parameters	Ca	pabilities	Advance
- Capal	pilities ———						
Capab	oility				Value		
i5/OS	Capable				True		
525	0 Application	Capable			False		
CoD C	Capable				True		
Pro	cessor Capal	ole			True		
Mer	nory Capable	)			True		
Micro-	partitioning C	apable			True		
Virtual	I/O Server C	apable			True		
Logica	l Host Chanr	nel Adapte	r Cap	ability	True		
Logica	I Host Ethern	iet Adapte	r Cap	ability	True		
Huge	Page Capabl	e			True		
Barrie	r Synchroniza	tion Regi	ster (E	SR) Capable	True		
Servic	e Processor I	-ailover C	apabl	e	True		
Share	d Ethernet Ad	lapter Fail	over (	Capable	True		
Redun	idant Error Pa	th Report	ing Ca	apable	True		
GX PI	us Capable				False		
Partitio	on processor	compatibl	ity mo	de capable	True		
Partition Availability Priority Capable					True		
Electro	onic Error Rej	porting Ca	pable		True		
Active	Partition Pro	cessor Sh	aring	Capable	l rue		

Figure 7-3 Active partition processor sharing

- 2. Select the Capabilities tab. At the bottom of the window, the status for processor sharing on the managed server is listed.
- 3. To configure the managed server as a processor donor and open the window as shown in Figure 7-4, select **Systems Management** then select the name of the server. Select the name of the partition to view the partition properties.

Go to the Hardware tab to view the settings for processors, memory, and I/O.

4. On the Processors tab, you can select the radio buttons for when you want to allow processor sharing for this particular partition. In this window, *inactive* and *active* refer only to the partition's activation state. Before POWER6, dedicated processors were not shared with other partitions, even if the processors were idle. With POWER6 systems you can now share idle processing power from dedicated processors.

When the LPAR with dedicated processors is inactive the processors are always idle. With this version of the HMC and POWER6 systems you can also share the idle processor cycles to the shared processor pool when the partition is active. This gives you the performance benefit of configuring dedicated processors to a partition while at the same time providing the server utilization benefit of sharing idle resources with other partitions.

- Allow when partition is inactive

When this option is selected, the dedicated resources for this partition are allocated to other active partitions for their shared processor usage.

- Allow when partition is active

When this option is selected, as processors become idle on this partition, the idle processors are allocated to other active partitions for their shared processor usage.



Figure 7-4 Processor sharing

### 7.1.3 Partition availability priority

New for POWER6 servers with the HMC V7 is the concept of *Partition Availability Priority*. This configuration option allows you to set up a hierarchy of partitions to cover for the event of a processor failure and ensures that high priority partitions have a higher guarantee of processor access than other partitions when a processor fails.

**Note:** The Partition Availability Priority option under System Plans displays only for POWER6 servers. If you are managing a POWER5 server, this option is not available.

To access the window shown in Figure 7-5, select **Systems Management**  $\rightarrow$  **Servers** then select the name of the server. Select **Configuration**  $\rightarrow$  **System Plans**  $\rightarrow$  **Partition Availability Priority**.



Figure 7-5 Setting partition availability priority

The managed system uses partition-availability priorities in the case of processor failure. If a processor fails on a logical partition and if there are no unassigned processors available on the managed system, the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. This allows the logical partition with the higher partition-availability priority to continue running after a processor failure.

When a processor fails on a high-priority logical partition, the managed system follows these steps to acquire a replacement processor for the high-priority logical partition:

- 1. If there are unassigned processors on the managed system, the managed system replaces the failed processor with an unassigned processor.
- 2. If there are no unassigned processors on the managed system, the managed system checks the logical partitions with lower partition-availability priorities, starting with the lowest partition-availability priority.
- 3. If a lower-priority logical partition uses dedicated processors, the managed system shuts down the logical partition and replaces the failed processor with one of the processors from the dedicated-processor partition.
- 4. If a lower-priority logical partition uses shared processors, and removing a whole processor from the logical partition would not cause the logical partition to go below its minimum value, the managed system removes a whole processor from the shared-processor partition using Dynamic Logical

Partitioning and replaces the failed processor with the processor that the managed system removed from the shared-processor partition.

- 5. If a lower-priority logical partition uses shared processors, but removing a whole processor from the logical partition would cause the logical partition to go below its minimum value, the managed system skips that logical partition and continues to the logical partition with the next higher partition availability.
- 6. If the managed system still cannot find a replacement processor, the managed system shuts down as many of the shared-processor partitions as it needs to acquire the replacement processor. The managed system shuts down the shared-processor partitions in partition-availability priority order, starting with the lowest partition-availability priority.

A logical partition can take processors only from logical partitions with lower partition-availability priorities. If all of the logical partitions on your managed system have the same partition-availability priority, then a logical partition can replace a failed processor only if the managed system has unassigned processors.

By default, the partition availability priority of Virtual I/O Server logical partitions and i5/OS logical partitions with virtual SCSI adapters is set to 191. The partition-availability priority of all other logical partitions is set to 127, by default, as shown in Figure 7-5.

**Note:** Do not set the priority of Virtual I/O Server logical partitions to be lower than the priority of the logical partitions that use the resources on the Virtual I/O Server logical partition.

Do not set the priority of i5/OS logical partitions with virtual SCSI adapters to be lower than the priority of the logical partitions that use the resources on the i5/OS logical partition.

# 7.2 Creating logical partitions

To create a logical partition, begin in the HMC workplace window. Select **Systems Management**  $\rightarrow$  **Servers** and then select the name of the server. This action takes you to the view shown in Figure 7-6.

Tasks: p5+-9133-55A-SN10D1FAG						
Properties						
Configuration						
Create Logical Partition						
AIX or Linux VIO Server						
Manage Custom Groups View Workload Management Groups Manage System Profiles						
Manage Partition Data						
Restore Initialize Backup Delete						
Hardware (Information)						
Updates     Updates						
■ Capacity On Demand (CoD)						

Figure 7-6 System partitioning view

Expand **Configuration** and then expand **Create Logical Partition** to open the area to create an AIX, Linux, or Virtual I/O Server partition.

# 7.2.1 Creating an AIX or a Linux partition

**Note:** The options and window views for creating a Virtual I/O Server (*VIO Server*) partition are the same as those that we present in this section. Thus, we do not document the steps for the VIO Server.

To create an AIX or a Linux partition, follow these steps:

 Select Configuration → Create Logical Partition → AIX or Linux to open the window shown in Figure 7-7. Here you can set the partition ID and specify the partition's name. Then, select Next.

Create Lpar Wizard	
→ Create Partition	Create Partition
Partition Profile Processors Processing Settings Memory VO	This wizard helps you create a new logical partition and a default profile for it. You can use the partition properties or profile properties to make changes after you complete this wizard.
Virtual Adapters Optional Settings	To create a partition, complete the following information:
Profile Summary	System name : p5+-9133-55A-SN10D1FAG Partition ID : 9 Partition name : AIX_dev1
< Back Next >	Finish Cancel Help
🛃 Done	📄 📄 🙆 👘 Internet

Figure 7-7 Create an AIX partition

2. Enter a profile name for this partition and click **Next** (Figure 7-8). You can then create a partition with either *shared* or *dedicated* processors on your server.

Create Lpar Wizard	d
✓ Create Partition	Partition Profile
→ Partition Profile Processors Processing Settings Memory I/O Virtual Adapters	A profile specifies how many processors, how much memory, and which I/O devices and slots are to be allocated to the partition. Every partition needs a default profile. To create the default profile, specify the following information :
Optional Settings Profile Summary	System name: p5+-9133-55A-SN10D1FAG
	Partition name: AIX_dev1 Partition ID: 9
	Profile name: sample profile
	This profile can assign specific resources to the partition or all resources to the partition. Click Next if you want to specify the resources used in the partition. Select the option below and then click Next if you want the partition to have all the resources in the system.
	Use all the resources in the system.
< Back Next >	Finish Cancel Help
E Done	🕒 🔁 👹 Internet

Figure 7-8 Create an AIX partition

### Configuring a shared processor partition

This section describes how to create a partition with a *shared* processor. If you want to create a partition with a *dedicated* processor, refer to "Configuring a dedicated processor partition" on page 236.

To configure a shared processor partition:

1. Select Shared and then select Next, as shown in Figure 7-9.



Figure 7-9 Create a shared processor partition

- 2. Specify the processing units for the partition as well as any settings for virtual processors, as shown in Figure 7-10. The sections that immediately follow this figure discuss the settings in this figure in detail.
- 3. After you have entered data in each of the fields (or accepted the defaults) select **Next** and then proceed to "Setting partition memory" on page 238.

Create Lpar Wiza	rd	
Crosts Datition	Processing Settings	
✓ <u>Create Partition</u> ✓ <u>Partition Profile</u> ✓ Processors	Specify the desired, minimum, and maximum processing se	ettings in the fields
→ Processing Settings	Total usable processing units: 8.00	
<u>Memory</u> I/O	Minimum processing units * 0.3	
Virtual Adapters Optional Settings	Desired processing units: * 4.0	
Profile Summary	Maximum processing units: *8.0	
	Virtual processors Minimum processing units required 0.10 for each virtual processor:	
	Minimum virtual processors: * 1.0	
	Desired virtual processors: * 4.0	
	Maximum virtual processors: *16.0	
	☑ Uncapped Weight : 128.0	
< Back Next >	Finish Cancel Help	
Done		🔒 👩 Internet

Figure 7-10 Shared partition settings

### Processing Settings area

In the Processing Settings area, you must specify the minimum number of processors that you want the shared processor partition to acquire, the desired amount, and the maximum upper limit allowed for the partition.

The values in each field can range anywhere between .1 and the total number of processors in the managed server and can be any increment in between in tenths of a processor.

Each field defines the following information:

### Minimum processing units

The absolute minimum number of processing units required from the shared processing pool for this partition to become active. If the number in this field is not available from the shared processing pool, this partition cannot be activated.

This value has a direct bearing on dynamic logical partitioning (DLPAR), as the minimum processing units value represents the smallest value of processors the partition can have as the result of a DLPAR deallocation.

### Desired processing units

This number has to be greater than or equal to the amount set in *Minimum processing units*, and represents an amount of processors asked for above the minimum amount. If the minimum is set to 2.3 and the desired set to 4.1, then the partition could become active with any number of processors between 4.1 and 2.3, whatever number is greater and available from the shared resource pool.

When a partition is activated, it queries for processing units starting at the desired value and goes down in .1 of a processor until it reaches the minimum value. If the minimum is not met, the partition does not become active.

Desired processing units only governs the possible number of processing units a partition can become active with. If the partition is made *upcapped*, then the hypervisor can let the partition exceed its desired value depending on how great the peak need is and what is available from the shared processing pool.

### Maximum processing units

This setting represents the absolute maximum number of processors this partition can own at any given time, and must be equal to or greater than the *Desired processing units*.

This value has a direct bearing on dynamic logical partitioning (DLPAR), as the maximum processing units value represents the largest value of processors the partition can have as the result of a DLPAR allocation.

Furthermore, while this value affects DLPAR allocation, it does not affect the processor allocation handled by the hypervisor for idle processor allocation during processing peaks.

**Note:** Whether your partition is *capped* or *uncapped*, the minimum value for *Maximum processing units* is equal to the value specified for *Desired processing units*.

### **Uncapped option**

The Uncapped option represents whether you want the HMC to consider the partition capped or uncapped. Whether a partition is *capped* or *uncapped*, when it is activated it takes on a processor value equal to a number somewhere between the minimum and desired processing units, depending on what is available from the shared resource pool. However, if a partition is capped, it can gain processing power only through a DLPAR allocation and otherwise stays at the value given to it at time of activation.

If the partition is *uncapped*, it can exceed the value set in *Desired virtual processors* and it can take the number of processing units from the shared processor pool that it needs. This is not seen from the HMC view of the partition, but you can check the value of processors owned by the partition from the operating system level with the appropriate commands.

The *weight* field defaults to 128 and can range from 0 to 256. Setting this number below 128 decreases a partition's priority for processor allocation, and increasing it above 128, up to 256, increases a partition's priority for processor allocation.

If all partitions are set to 128 (or another equivalent number), then all partitions have equal access to the shared processor pool. If a partition's *uncapped weight* is set to 0, then that partition is considered *capped*, and it never owns a number of processors greater than that specified in *Desired processing units*.

### Virtual processors area

The values that are set in the Virtual processors are of this window govern how many processors to present to the operating system of the partition. You must show a minimum of one virtual processor per actual processor, and you can have as many as 10 virtual processors per physical processing unit.

As a general recommendation, a partition requires at least as many virtual processors as you have actual processors, and a partition should be configured with no more than twice the number of virtual processors as you have actual processors.

Each field defines the following information:

#### Minimum virtual processors

Your partition must have at least one virtual processor for every part of a physical processor assigned to the partition. For example, if you have assigned 2.5 processing units to the partition, the minimum number of virtual processors is three.

Furthermore, this value represents the lowest number of virtual processors that can be owned by this partition as the result of a DLPAR operation.
#### Desired virtual processors

The desired virtual processors value has to be greater than or equal to the value set in *Minimum virtual processors*, and as a general guideline about twice the amount set in *Desired processing units*. Performance with virtual processing can vary depending on the application, and you might need to experiment with the desired virtual processors value before you find the perfect value for this field and your implementation.

**Note:** The desired virtual processors value, along with the resources available in the shared resource pool, is the only value that can set an effective limit on the amount of resources that can be utilized by an uncapped partition.

#### Maximum virtual processors

You can only have 10 virtual processors per processing unit. Therefore, you cannot assign a value greater than 10 times the *Maximum processing units* value as set in "Processing Settings area" on page 232. It is recommended, though not required, to set this number to twice the value entered in *Maximum processing units*.

**Note:** Regardless of the number of processors in the server or the processing units owned by the partition, there is an absolute upper limit of 64 virtual processors per partition with the HMC V7 software.

Finally, this value represents the maximum number of virtual processors that this partition can have as the result of a DLPAR operation.

#### Configuring a dedicated processor partition

This section describes how to create a partition with a *dedicated* processor. If you want to create a partition with a *shared* processor, refer to "Configuring a shared processor partition" on page 231.

To configure a dedicated processor partition:

1. Select Dedicated and then select Next, as shown in Figure 7-11.



Figure 7-11 Create dedicated processor partition

2. Specify the number of minimum, desired, and maximum processors for the partition, as shown in Figure 7-12. For a description on what each field represents, refer to "Processing Settings area" on page 232.

**Note:** If you are creating a partition on a POWER6 server, you can still configure the partition to donate idle processors to the shared processing pool. For more information, refer to 7.1.2, "Shared pool usage of dedicated capacity" on page 223.

3. After you have entered the values for the fields, select Next.

Create Partition	Processing Settings
<ul> <li><u>Partition Profile</u></li> <li>Processors</li> </ul>	Specify the desired, minimum, and maximum processing settings in the fields below.
→ Processing Settings	Total number of processors : 8
<u>Memory</u> I/O	Minimum processors: * 1.1
Virtual Adapters	Desired processors: * 2.2
Profile Summary	Maximum processors: * 3.3
< Back Next >	Finish Cancel Help

Figure 7-12 Processor settings with dedicated processors

#### Setting partition memory

Now, you need to set the partition memory, as shown in Figure 7-13.

Create Lpar Wizar	d
Create Lpar Wizard  ✓ Create Partition  ✓ Partition Profile  ✓ Processors  ✓ Processing  Settings  → Memory I/O Virtual Adapters Optional Settings Profile Summary	Memory         Specify desired, minimum and maximum amounts of memory for this profile using a combination of the gigabyte and megabyte fields below.         Installed memory (MB):       32768         Current memory available for partition usage (MB):       31872         Minimum memory       Desired memory       Maximum memory         0       Image (MB)       Image (MB)
< Back Next >	0 ♥ GB 0 ♥ GB 1 ♥ GB 256 ♥ MB 512 ♥ MB 0 ♥ MB Finish Cancel Help
ē	🔒 🕘 Internet

Figure 7-13 Set partition memory

The *minimum*, *desired*, and *maximum* settings are similar to their processor counterparts:

#### Minimum memory

Represents the absolute memory required to make the partition active. If the amount of memory specified under minimum is not available on the managed server then the partition cannot become active.

#### Desired memory

Specifies the amount of memory beyond the minimum that can be allocated to the partition. If the minimum is set at 256 MB and the desired is set at 4 GB, then the partition in question can become active with anywhere between 256 MB and 4 GB.

#### Maximum memory

Represents the absolute maximum amount of memory for this partition, and it can be a value greater than or equal to the number specified in *Desired* 

*memory*. If set at the same amount as desired, then the partition is considered *capped*, and if this number is equal to the total amount of memory in the server then this partition is considered *uncapped*.

After you have made your memory selections, select Next.

#### Configuring physical I/O

On the I/O window, as shown in Figure 7-14, you can select I/O resources for the partition to own. If you want the partition to own virtual resources, refer to "Configuring virtual resources" on page 240. After you have made your selections in this window, select **Next**.

Create Lpar Wizard	I/O						
<ul> <li><u>Create Partition</u></li> <li><u>Partition Profile</u></li> <li><u>Processors</u></li> <li><u>Settings</u></li> <li>Memory</li> </ul>	Add as	d below are t	ne physical I Add as de	/O resources fo	or the managed system. Select slot to	view the properties of each d	evice.
→ <u>vo</u> Virtual Adapters Optional Settings Profile Summary		Unit U787B.001 U787B.001 U787B.001 U787B.001 U787B.001 U787B.001 U787B.001 U787B.001	A DNWB206 DNWB206 DNWB206 DNWB206 DNWB206 DNWB206 DNWB206 DNWB206 Tota	Bus         Slot         2         C3           3         C4         3         C5         3         T14         3         T16         4         C1         4         C2         4         T7         4         T9         al: 9         Filtered:         5	Added  Description Empty slot Empty slot Empty slot Storage controller Other Mass Storage Con Empty slot Empty slot Universal Serial Bus UH PCI 10/100/1000Mbps E 9		ode ^] I.DNWB206-P1-C3 I.DNWB206-P1-C4 I.DNWB206-P1-C5 I.DNWB206-P1-T14 I.DNWB206-P1-T14 I.DNWB206-P1-C1 I.DNWB206-P1-C2 I.DNWB206-P1-T7 I.DNWB206-P1-T9
< Back Next >	Finish	Cancel	lelp				

Figure 7-14 Configure physical I/O

#### **Configuring virtual resources**

If you have adapters assigned to the virtual I/O server (as explained in Chapter 9, "Virtual I/O" on page 259), you can create a virtual adapter share for your partition. Follow these steps:

1. Select Actions  $\rightarrow$  Create  $\rightarrow$  SCSI Adapter to create a virtual SCSI share.

Alternatively, select  $\textbf{Actions} \rightarrow \textbf{Create} \rightarrow \textbf{Ethernet Adapter}$  to create a shared Ethernet share.

✓ Create Partition       ✓         ✓ Partition Profile       Actions ▼         ✓ Processors       ✓         ✓ Processing Settings       Edit         ✓ Memory       ✓         ✓ VO       Delete
→ Virtual Adapters       Number of virtu       Serial Adapter       2         Optional Settings       Profile Summary       Profile Summary       2         Select ^ Type       ^ Adapter ID ^ Connecting Partition ^ Connecting Adapter ^ Required ^ Yes
Server Serial 1 Total: 2 Filtered: 2 Selected: 0           < Back         Next > Finish         Cancel         Help

See Figure 7-15.

Figure 7-15 Configure virtual resources

2. You can specify your server partition, get System VIOS info, and specify a tag for adapter identification, as shown in Figure 7-16. When you have entered all of the data, select **OK**.

Create Virtual SCSI Adapter	
Some text to explain this thing. Adapter : *2 Type of adapter : Client	
□ This adapter is required for partition activation. Server wasp5I_vio(1) ▼ System VIOS Info Server 2 adapter ID :	
OK Cancel Help	T
😇 Done 📄 📄 🔮 Internet	

Figure 7-16 Create virtual SCSI adapter

You are returned to the virtual adapters window as shown in Figure 7-17. When you are done creating all the virtual resources, select **Next**.

Create Lpar Wizard								
<ul> <li>✓ Create Partition</li> <li>✓ Partition Profile</li> <li>✓ Processors</li> <li>✓ Processing Settings</li> <li>✓ Memory</li> <li>✓ I/O</li> <li>→ Virtual Adapters Optional Settings Profile Summary</li> </ul>	Virtual Actions Virtual re- settings a Maximum Number of Select ^ O	dapters sources allow f re listed below witual adapte of vitual adapte f vitua	ior the sharing rs : ers : Adapter ID ^ 3 0 1 Total: 3 Filte	of physical hardwa *1 3 t Action • Connecting Partiti wasp5I_vio(1) ered: 3 Selected:	o o o	tween logical partition Connecting Adapter 2	s. The current virtua	I adapter
< Back Next > Finish	Cancel	Help						
👌 Done							📄 🎒 💣 Internet	:

Figure 7-17 Virtual adapters

#### **Optional Settings window**

On the Optional Settings window shown in Figure 7-18 you can:

- ► Enable connection monitoring
- ► Start the partition with the managed system automatically
- Enable redundant error path reporting

You can also specify one of the various boot modes that are available.

After you have made your selections in this window, click Next to continue.

✓ Create Partition	Optional Settings
<ul> <li>Partition Profile</li> <li>Processors</li> <li><u>Processing</u></li> <li><u>Settings</u></li> <li><u>Memory</u></li> <li><u>IO</u></li> <li><u>Virtual Adapters</u></li> <li><u>Optional</u></li> <li><u>Settings</u></li> <li>Profile Summary</li> </ul>	Select optional settings for this partition profile using the fields below.  Enable connection monitoring Automatically start with managed system Enable redundant error path reporting Boot modes  Normal System Management Services (SMS) Diagnostic with default boot list (DIAG_DEFAULT) Diagnostic with stored boot list (DIAG_STORED) Open Firmware OK prompt (OPEN_FIRMWARE)
< Back Next >	Finish Cancel Help

Figure 7-18 Optional settings

#### Enabling connection monitoring

Select this option to enable connection monitoring between the HMC and the logical partition that is associated with this partition profile. When connection monitoring is enabled, the Service Focal Point (SFP) application periodically tests the communications channel between this logical partition and the HMC. If the channel does not work, the SFP application generates a serviceable event in the SFP log. This ensures that the communications channel can carry service requests from the logical partition to the HMC when needed.

If this option is not selected, the SFP application still collects service request information when there are issues on the managed system. This option only controls whether the SFP application automatically tests the connection and generates a serviceable event if the channel does not work.

Clear this option if you do not want the SFP application to monitor the communications channel between the HMC and the logical partition associated with this partition profile.

#### Starting with managed system automatically

This option shows whether this partition profile sets the managed system to activate the logical partition that is associated with this partition profile automatically when you power on the managed system.

When you power on a managed system, the managed system is set to activate certain logical partitions automatically. After these logical partitions are activated, you must activate any remaining logical partitions manually. When you activate this partition profile, the partition profile overwrites the current setting for this logical partition with this setting.

If this option is selected, the partition profile sets the managed system to activate this logical partition automatically the next time the managed system is powered on.

If this option is not selected, the partition profile sets the managed system so that you must activate this logical partition manually the next time the managed system is powered on.

#### Enabling redundant error path reporting

Select this option to enable the reporting of server common hardware errors from this logical partition to the HMC. The service processor is the primary path for reporting server common hardware errors to the HMC. Selecting this option allows you to set up redundant error reporting paths in addition to the error reporting path provided by the service processor.

Server common hardware errors include errors in processors, memory, power subsystems, the service processor, the system unit vital product data (VPD), non-volatile random access memory (NVRAM), I/O unit bus transport (RIO and PCI), clustering hardware, and switch hardware. Server common hardware errors do not include errors in I/O processors (IOPs), I/O adapters (IOAs), or I/O device hardware.

If this option is selected, this logical partition reports server common hardware errors and partition hardware errors to the HMC. If this option is not selected, this logical partition reports only partition hardware errors to the HMC.

This option is available only if the server firmware allows you to enable redundant error path reporting (the Redundant Error Path Reporting Capable option on the Capabilities tab in Managed System Properties is True.

#### Boot modes

Select the default boot mode that is associated with this partition profile. When you activate this partition profile, the system uses this boot mode to start the operating system on the logical partition unless you specify otherwise when activating the partition profile. (The boot mode applies only to AIX, Linux, and virtual I/O server logical partitions. This area is unavailable for i5/OS logical partitions.) Valid boot modes are as follows:

Normal

The logical partition starts up as normal. (This is the mode that you use to perform most everyday tasks.)

#### System Management Services (SMS)

The logical partition boots to the System Management Services (SMS) menu.

#### Diagnostic with default boot list (DIAG\_DEFAULT)

The logical partition boots using the default boot list that is stored in the system firmware. This mode is normally used to boot customer diagnostics from the CD-ROM drive. Use this boot mode to run standalone diagnostics.

#### Diagnostic with stored boot list (DIAG\_STORED)

The logical partition performs a service mode boot using the service mode boot list saved in NVRAM. Use this boot mode to run online diagnostics.

#### Open Firmware OK prompt (OPEN\_FIRMWARE)

The logical partition boots to the open firmware prompt. This option is used by service personnel to obtain additional debug information.

#### **Profile summary**

When you arrive at the profile summary as shown in Figure 7-19, you can review your partition profile selections. If you see anything that you want to change, select **Back** to get to the appropriate window and to make changes.

If you are satisfied with the data represented in the Profile Summary, select **Finish** to create your partition.

Create Lpar Wizard		
	-	
✓ Create Partition	Profile Summary	
<ul> <li>✓ <u>Partition Profile</u></li> <li>✓ <u>Processors</u></li> <li>✓ <u>Processing</u></li> </ul>	This is a summary of t partition and profile. To the details of the physi	the partition and profile. Click Finish to create the o change any of your choices, click Back. You can see ical I/O devices you chose by clicking Details.
✓ <u>Settings</u> ✓ <u>Memory</u>	You can modify the pr profile properties after	rofile or partition by using the partition properties or you complete this wizard.
<ul> <li>✓ <u>Virtual Adapters</u></li> <li>✓ <u>Optional Settings</u></li> <li>→ <u>Profile Summary</u></li> </ul>	System name: Partition ID: Partition name: Partition environment: Profile name:	p5+-9133-55A-SN10D1FAG 9 AIX_dev1 : AIX or Linux sample profile
	Desired memory: Desired processors: Physical I/O devices:	0.0 GB 512.0 MB 1.0 2 Details
	Boot mode:	NORMAL
	Virtual I/O adapters:	0 Ethernet 0 SCSI 2 Serial
< Back Next >	Finish Cancel Help	
🕘 Done		📄 📄 🔮 Internet

Figure 7-19 Profile summary

After you select **Finish**, for a few minutes the window shown in Figure 7-20 displays. When this window goes away, go back to your main HMC view, and the partition that you created is listed under the existing partitions on your managed server.

 Create Logical Partition	•
🔒 🥑 Internet	_//

Figure 7-20 Partition creation status window

### 7.3 Managing partition data

This section discusses how to manipulate partition profile data on the HMC. It includes information about:

- ► Restore: Load profile data locally from the HMC or from removable media
- Initialize: Initialize all profile images

**Note:** Initialize removes *all* profile data saved to the HMC. Do not perform this action if you want to preserve *any* of the profile data saved on the HMC.

- **Backup**: Save profile data to the HMC
- ► Delete: Remove profile data

#### 7.3.1 Restore

The *restore* option allows you to restore profile data from a local backup stored on the HMC. To restore profile data, select **Configuration**  $\rightarrow$  **Manage Partition Data**  $\rightarrow$  **Restore**. Select the backup image that you would like to restore, and then select **OK**, as shown in Figure 7-21. The restore can take approximately a minute and a half or longer to complete.

Pro	Profile Data Restore - 9117-MMA-SN10FFE0B-L9						
Sele syste	Select a profile backup file from which to restore the managed system's profile data. Then select a restore option.						
Sele	ct File Name	Backup Time					
C	backupFile	May 9, 2007 3:44:30 PM GMT+05:00					
С	test1	May 8, 2007 7:17:58 PM GMT+05:00					
0	09MAY2007	May 9, 2007 4:33:01 PM GMT+05:00					
- <i>Rе</i> он он ок	OPMAY2007 May 9, 2007 4:33:01 PM GMT+05:00      Restore Options      Full restore from the selected backup file     C Backup priority merge current profile and backup     C Managed system priority merge current profile and backup      OK Cancel Help						

Figure 7-21 Restore profile data

You have the following options for restore:

► Full restore

A full restore ignores all current partition profile data and restores the system using only the backup file. If you want to preserve any of the existing partition profile data that resides on the managed server during the restore process, you consider using *Backup priority* or *Managed system priority* instead of a full restore.

Backup priority

This option merges the backup file with the current partitions on the system. This option is useful when you want to do a restore and have the backup file restore existing partitions to a previous state. An example of when this option would be useful is if you have a a partition where you have changed the memory, processors, or adapters, but the previous configuration of the partition performed better. By using this option, you can restore the partition to its previous state from a backup. Keep in mind this holds true for all partitions included in the backup data.

This option ultimately overwrites existing profile data with the profile data contained in the backup you are selecting.

#### Managed system priority

This option merges the backup file with the current partitions on the system, but if the backup file contains data for any of the current partitions their current state takes precedence over their backup state. This option is useful to restore deleted partitions without affecting the other partitions on the system.

This option ultimately preserves existing partition profile data while restoring data for partitions not currently on the system.

#### 7.3.2 Initialize

The *initialize* option clears all current profile data on the managed server and effectively removes all partitions from the hypervisor and system image on the HMC. (This option does not remove profile backups. To do that, see 7.3.4, "Delete" on page 251.)

To use this option, select **Configuration**  $\rightarrow$  **Manage Partition Data**  $\rightarrow$  **Initialize**. If you are certain that you want to remove all the partitions on the managed server, select **Yes** as shown in Figure 7-22.



Figure 7-22 Initialize profile data

**Note:** You cannot initialize profile data if any partition on the managed system is in the *Standby* or *Operating* state. All partitions on the managed system must be in the *Not Activated* state to initialize profile data.

Times vary on how long it takes to initialize profile data. To initialize data can take as long as two minutes or longer.

When complete, your managed server will be clear of any profile data. From this point, you can create new partitions on the server or restore partition profile data from a previous backup. Read 7.3.1, "Restore" on page 248 on how to restore profile data.

#### 7.3.3 Backup

The *backup* option allows for the backup of profile data for all partitions on a managed server to be saved locally on the HMC. To use this option, select **Configuration**  $\rightarrow$  **Manage Partition Data**  $\rightarrow$  **Backup**. Enter a name for the backup, and then select **OK** to continue, as shown in Figure 7-23.

Profile Data Backup - 9117-MMA-SN10FFE0B-L9	<b></b>
Enter a name for the new backup file below.	
Backup file name: * 09MAY2007	
OK Cancel Help	

Figure 7-23 Backup profile data

The backup can take a minute or longer, depending upon how many partitions are on the system.

When the backup is complete, a message displays (Figure 7-24).



Figure 7-24 Backup profile data results

#### 7.3.4 Delete

The *delete* option allows you to delete a single backup image of the managed server partition profile data. To use this option, select **Configuration**  $\rightarrow$  **Manage Partition Data**  $\rightarrow$  **Delete**. Select the partition profile image that you want to remove and select OK, as shown in Figure 7-25.

Profile Data Delete - 9117-MMA-SN10FFE0B-L9						
Select one or more profile data backup files, then click "OK" to delete them.						
Select	File Name	Backup Time				
0	test1	2007-05-08 19:17:58.0				
۲	09MAY2007	2007-05-09 16:33:01.0				
OK Cancel Help						

Figure 7-25 Delete profile data

A status window opens after you select **OK**. The HMC simply returns you to the main partition view when the deletion is complete.

# 8



A *dual HMC* is a redundant Hardware Management Console (HMC) management system that provides flexibility and high availability. When two HMCs manage one system, they are *peers*, and each can be used to control the managed system. One HMC can manage multiple managed systems, and each managed system can have two HMCs. If both HMCs are connected to the server using private networks, each HMC must be a DHCP server set up to provide IP addresses on two unique, nonroutable IP range.

This chapter discusses redundant HMC configurations and considerations.

# 8.1 Redundant HMC configurations

You can configure a redundant HMC in a configuration in which dual HMC servers are connected to the service processors.

Using a redundant HMC configuration with your service processor setup requires a specific port configuration, as shown in Figure 8-1. In this configuration, each service processor connects to a network hub that is connected to each HMC. The network hubs that are connected to the service processors must remain in the *power-on* state. Any 10/100BASE-T Ethernet switch or hub can be used to connect the server and HMC.



Figure 8-1 Dual HMC configuration on a private network

The HMC's first Ethernet port, eth0, should be configured to be a DHCP server over a private network. By default, the FSP uses a DHCP client to request an IP address. This occurs when power is applied to the server or FSP is reset. The FSP has two default IP addresses: 192.168.2.147 on HMC1 port and 192.168.3.147 on HMC2 port. Always turn on the HMC first, then the server, during setup, so that an IP address is available for the FSP, by which the HMC will also discover the servers on its private service network. See Figure 8-2.



Figure 8-2 Dual HMC physical connections

For information about how to configure an HMC, refer to Chapter 3, "Installing the HMC" on page 69.

# 8.2 Redundant remote HMC

A redundant remote HMC configuration is very common. When customers have multiple sites or a disaster recovery site, they can use their second HMC in the configuration remotely over a switched network, as illustrated in Figure 8-3. The second HMC can be local, or it can reside at a remote location. Each HMC must use a different IP subnet.



Figure 8-3 Example of redundant remote HMC

## 8.3 Redundant HMC configuration considerations

In a redundant HMC configuration, both HMCs are fully active and accessible at all times, enabling you to perform management tasks from either HMC at any time. There is no primary or backup designation.

You need to consider the following points:

Because authorized users can be defined independently for each HMC, determine whether the users of one HMC should be authorized on the other. If so, the user authorization must be set up separately on each HMC.

- Because both HMCs provide Service Focal Point and Service Agent functions, connect a modem and phone line to only one of the HMCs and enable its Service Agent. To prevent redundant service calls, do not enable the Service Agent on both HMCs.
- Perform software maintenance separately on each HMC, at separate times, so that there is no interruption in accessing HMC function. This allows one HMC to run at the new fix level, while the other HMC can continue to run at the previous fix level. However, the best practice is to upgrade both HMCs to the same fix level as soon as possible.

The basic design of HMC eliminates the possible operation conflicts issued from two HMCs in the redundant HMC configuration. A locking mechanism provided by the service processor allows interoperation in a parallel environment. This allows an HMC to temporarily take exclusive control of the interface, effectively locking out the other HMC. Usually, this locking is held only for the short duration of time it takes to complete an operation, after which the interface is available for further commands.

Both HMCs are automatically notified of any changes that occur in the managed systems, so the results of commands issued by one HMC are visible in the other. For example, if you choose to activate a partition from one HMC, you will observe the partition going to the Starting and Running states on both HMCs.

The locking between HMCs does not prevent users from running commands that might seem to be in conflict with each other. For example, if the user on one HMC activates a partition, and a short time later a user on the other HMC selects to power the system off, the system will turn off. Effectively, any sequence of commands that you can do from a single HMC is also permitted when it comes from redundant HMCs.

For this reason, it is important to consider carefully how to use this redundant capability to avoid such conflicts. You might choose to use them in a primary and backup role, even though the HMCs are not restricted in that way. The interface locking between two HMCs is automatic, usually of short duration, and most console operations wait for the lock to release without requiring user intervention.

However, if one HMC experiences a problem while in the middle of an operation, it might be necessary to release the lock manually. HMC 2 can be used to disconnect HMC 1. When an HMC is disconnected, all locks owned by the HMC are reset. To due this, any *hmcsuperadmin* user can run the Disconnect Another HMC GUI task on HMC 2 against HMC1. This task can only be done from the graphical interface. There is no corresponding command line version of this task.

When running two HMCs to the same server, you should also be careful with long running functions, as they might be impacted if they have not completed before an additional function is run on the second HMC.

With the previous considerations in mind, there a number of good reasons to utilize the redundant HMC configuration. This list is not exhaustive:

- ► Redundancy of critical configuration information.
- Ability to apply maintenance to an HMC while the other is available for production management functions.
- ► Reduced risk of no HMC available.
- Knowing that a long running command is running against one system, being able to use the second HMC to perform functions on another system without waiting.

# 9

# Virtual I/O

Virtual I/O provides the capability for a single physical I/O adapter and disk to be used by multiple logical partitions of the same server, allowing consolidation of I/O resources and minimizing the number of I/O adapters that are required.

In this chapter, we introduce the basic concept of a virtual I/O on an HMC V7 and discuss the main topics of Virtual SCSI, Virtual Ethernet, and Shared Ethernet Adapter.

We do not discuss how to install or configure the Virtual I/O Server in this chapter. If you information more about virtualization, refer to:

- Advanced POWER Virtualization on IBM System p5: Introduction and Configuration, SG24-7940
- ► IBM System p Advanced POWER Virtualization Best Practices, REDP-4194.
- ► Hardware Information Center

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp

# 9.1 Understanding virtual I/O

*Virtual I/O* describes the ability to share physical I/O resources between partitions in the form of *virtual adapter cards* that are located in the managed system. Each logical partition typically requires one I/O slot for disk attachment and another I/O slot for network attachment. In the past, these I/O slot requirements would have been physical requirements. To overcome these physical limitations, I/O resources are shared with virtual I/O. In the case of *Virtual Ethernet*, the physical Ethernet adapter is not required to communicate between LPARS. *Virtual SCSI* provides the means to share I/O resources for SCSI storage devices.

#### 9.1.1 POWER Hypervisor for virtual I/O

The POWER Hypervisor<sup>™</sup> provides the interconnection for the partitions. To use the functionalities of virtual I/O, a partition uses a virtual adapter as shown in Figure 9-1. The POWER Hypervisor provides the partition with a view of an adapter that has the appearance of an I/O adapter, which might or might not correspond to a physical I/O adapter.



Figure 9-1 Role of POWER Hypervisor for virtual I/O

#### 9.1.2 Virtual I/O Server

The Virtual I/O Server can link the physical resources to the virtual resources. By this linking, it provides virtual storage and Shared Ethernet Adapter capability to client logical partitions on the system. It allows physical adapters with attached disks on the Virtual I/O Server to be shared by one or more client partitions.

Virtual I/O Server mainly provides two functions:

- Serves virtual SCSI devices to clients, which is described in 9.2, "Virtual SCSI" on page 262.
- Provides a Shared Ethernet Adapter for virtual Ethernet, which is described in 9.4, "Shared Ethernet Adapter" on page 267.

Virtual I/O Server partitions are not intended to run applications or for general user logins. The Virtual I/O Server is installed in its own partition. The Virtual I/O Server partition is a special type of partition which is marked as such on the first window of the Create Logical Partitioning Wizard program.

Currently the Virtual I/O Server is implemented as a customized AIX partition, however the interface to the system is abstracted using a secure shell-based command line interface (CLI). When a partition is created as this type of partition, only the Virtual I/O Server software boot image will boot successfully when the partition is activated.

This Virtual I/O Server should be properly configured with enough resources. The most important resource is the processor resources. If a Virtual I/O Server has to host a lot of resources to other partitions, you must ensure that enough processor power is available.

# 9.2 Virtual SCSI

Virtual SCSI is based on a client/server relationship. A Virtual I/O Server partition owns the physical resources, and logical client partitions access the virtual SCSI resources provided by the Virtual I/O Server partition. The Virtual I/O Server partition has physically attached I/O devices and exports one or more of these devices to other partitions as shown in Figure 9-2.



Figure 9-2 Virtual SCSI overview

The client partition is a partition that has a virtual client adapter node defined in its device tree and relies on the Virtual I/O Server partition to provide access to one or more block interface devices. Virtual SCSI requires POWER5 or POWER6 hardware with the Advanced POWER Virtualization feature activated.

#### 9.2.1 Client/server communications

In the Figure 9-2, the virtual SCSI adapters on the server and the client are connected through the hypervisor. The virtual SCSI adapter drivers (server and client) communicate control data through the hypervisor.

When data is transferred from the backing storage to the client partition, it is transferred to and from the client's data buffer by the DMA controller on the physical adapter card using redirected SCSI Remote Direct Memory Access (RDMA) Protocol. This facility enables the Virtual I/O Server to securely target memory pages on the client to support virtual SCSI.

#### 9.2.2 Adding a virtual SCSI server adapter

You can create the virtual adapters in two periods. One is to create those during installing the Virtual I/O Server. The other is to add those in already existing Virtual I/O Server. In this chapter, we suppose that we already created the Virtual I/O Server.

Before activating a server, you can add the virtual adapter using the Manage Profiles task. For an activated server, you can only do that through dynamic LPAR operation if you want to use virtual adapters immediately. This procedure requires that the network is configured with connection to the HMC to allow for dynamic LPAR.

Now, you can add the adapter through dynamic LPAR. To add the adapter:

- Select the activated Virtual I/O Server partition in HMC. Then click Virtual Adapters in the Dynamic Logical Partitioning section in the Task pane. The Virtual Adapters window opens.
- 2. Click Actions  $\rightarrow$  Create  $\rightarrow$  SCSI Adapter, as shown in Figure 9-3.

Edit	ties llow fo	or the sharing o	f physical hardware betw	een logical partitions. The	current virtu
Create Delete	Ethe SCS	ernet Adapter I Adapter		Reserved slot numbers: 0 - 10	
444 4	\$ 1 E	Sel	ect Action 💌		
Select ^	Type ^	Adapter ID ^	Connecting Partition ^	Connecting Adapter ^	Required ^
0	Ethernet	2	N/A	N/A	Yes
0	Ethernet	3	N/A	N/A	Yes
0	Ethernet	39	N/A	N/A	Yes
0	Server SCSI	10	doc(2)	2	No
0	Server Serial	0	Any Partition	Any Partition Slot	Yes
0	Server Serial	1	Any Partition	Any Partition Slot	Yes
		Total: 6 F	iltered: 6 Selected	d: 0	
Detail le	(minutes) : 0 vel : 1 ancel Help		<b>▼</b>		

Figure 9-3 Create SCSI Adapter

3. In the next window, you create the new virtual SCSI adapter, as shown in Figure 9-4. If the clients are not known to the HMC, select **Any client can connect**. If you select this option, you have to change the client partition options to the proper name of the client after you create the clients.

If you know which client partition is connected, select **Only selected client partition can connect**. Then, choose the client adapter ID number.

Click OK.

Create Virtual SCSI Adapter: VIOS1 L9							
Virtual SCSI adapter							
Adapter : * 11							
Type of adapter : Server							
O Any client partition can connect							
Only selected client partition can connect							
Client partition : doc(2)							
Client adapter ID : 2							
OK Cancel Help							

Figure 9-4 Create Virtual SCSI Adapter

4. Now, you can see the new virtual SCSI adapter in the Virtual Adapters window as shown in Figure 9-5. In our example, we set up the adapter to connect to the *doc* partition with *Adapter ID 11*.

Virtual Adapters: VIOS1_L9										
Actions -										
Virtual resources allow for the sharing of physical hardware between logical partitions. The current virtual adapter settings are listed below.										
Maximum virtual adapters : * 40 Reserved slot numbers: 0 - 10										
Number of virtual adapters : 7										
👯 😰 😰 📑 Select Action 💌										
Select ^	Type ^	Adapter ID ^	Connecting Partition ^	Connecting Adapter ^	Required ^					
0	Ethernet	2	N/A	N/A	Yes					
0	Ethernet	3	N/A	N/A	Yes					
0	Ethernet	39	N/A	N/A	Yes					
0	Server SCSI	10	doc(2)	2	No					
	Server SCSI	11	doc(2)	2	No					
0	Server Serial	0	Any Partition	Any Partition Slot	Yes					
0	Server Serial	1	Any Partition	Any Partition Slot	Yes					

Figure 9-5 Display new virtual SCSI adapter

**Note:** We found that it is good to have a server slot number that is consistent with the client slot number. You can save time figuring out the slot mappings later.

# 9.3 Virtual Ethernet

*Virtual Ethernet* enables inter-partition communication without having physical network adapters assigned to each partition. It can be used in both shared and dedicated POWER5 and POWER6 processor partitions, provided that the partition is running AIX 5L V5.3 or Linux with the 2.6 kernel or a kernel that supports virtualization. This technology enables IP-based communication between logical partitions on the same system using a Virtual LAN capable software switch (POWER Hypervisor).

Due to the number of partitions possible on many systems being greater than the number of I/O slots, virtual Ethernet is a convenient and cost saving option to enable partitions within a single system to communicate with one another through a virtual Ethernet LAN. These connections exhibit characteristics similar

to physical high-bandwidth Ethernet connections and support multiple protocols (IPv4, IPv6, and ICMP).

Virtual Ethernet does not require the purchase of any additional features or software, such as the Advanced POWER Virtualization feature. Virtual Ethernet is different from Shared Ethernet adapter in that, there is no connection to a physical Ethernet adapter which connects to a physical Ethernet network. To use virtual Ethernet to connect to a physical Ethernet adapter which connects to a physical Ethernet network, you must implement Shared Ethernet adapter.

#### 9.3.1 Virtual LAN overview

Virtual LAN (VLAN) is a technology used for establishing virtual network segments on top of physical switch devices. Multiple VLAN logical devices can be configured on a single system as shown in Figure 9-6. Each VLAN logical devices can be used to configure the same types of Ethernet IP interfaces as are used with physical Ethernet adapters.



Figure 9-6 VLAN example: Two VLANs

#### 9.3.2 Virtual Ethernet connection

Virtual Ethernet connections supported in POWER5 and POWER6 processor based systems use VLAN technology to ensure that the partitions can access only data that is directed to them. The POWER Hypervisor provides a virtual Ethernet switch function based on the IEEE 802.1Q VLAN standard that enables partition communication within the same server as shown in Figure 9-7. The connections are based on an implementation internal to the Hypervisor that moves data between partitions.



Figure 9-7 Virtual Ethernet connection

#### 9.3.3 Adding virtual Ethernet

You can create virtual Ethernet adapters in the same manor as creating a virtual SCSI adapter as described in 9.2.2, "Adding a virtual SCSI server adapter" on page 263.

## 9.4 Shared Ethernet Adapter

A Virtual I/O Server partition is not required for implementing a VLAN. Virtual Ethernet adapters can communicate with each other through the POWER Hypervisor without the functionality of the Virtual I/O Server. Shared Ethernet adapter bridges external networks to internal VLANs. The Shared Ethernet Adapter hosted in the Virtual I/O Server partition acts as an OSI Layer 2 switch between the internal and external network.

Figure 9-8 shows the Shared Ethernet Adapter used as a bridge between the virtual Ethernet and physical Ethernet.



Figure 9-8 Shared Ethernet Adapter configuration

The bridge interconnects the logical and physical LAN segments at the network interface layer level and forwards frames between them. The bridge performs the function of a MAC relay (OSI Layer 2) and is independent of any higher layer protocol. Figure 9-9 is a close-up view of the Virtual I/O Server partition.



Figure 9-9 Shared Ethernet Adapter OSI layer

The bridge is transparent to the Internet Protocol (IP) layer. For example, when an IP host sends an IP datagram to another host on a network connected by a bridge, it sends the datagram directly to the host. The datagram crosses the bridge without the sending IP host being aware of it.

The Virtual I/O Server partition offers broadcast and multicast support. Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP) also work across the Shared Ethernet Adapter.

The Virtual I/O server does not reserve bandwidth on the physical adapter for any of the VLAN clients that send data to the external network. Therefore, if one client partition of the Virtual I/O Server sends data, it can take advantage of the full bandwidth of the adapter, assuming that the other client partitions do not send or receive data over the network adapter at the same time.
# 10

# **Command line interface**

This chapter discusses added enhancements to the command line interface (CLI) . It also provides information about the most common command line options and usage.

On the Hardware Management Console (HMC), you can find a man page for every command. You can also access a PDF that includes all the man pages at:

http://www14.software.ibm.com/webapp/set2/sas/f/hmc/power6/related/hmc\_ man\_7310.pdf

In addition, you can find the current command line specification at:

http://www.ibm.com

From the IBM main site, follow these steps:

- 1. Select Support & downloads  $\rightarrow$  Support by product  $\rightarrow$  Systems and servers. Then, select System p.
- 2. Under Popular Links, select **HMC Updates**. Select the most current release of HMC on this page.
- 3. On the Recovery Media tab, select **Related documentation** and select the command line specification.

# 10.1 CLI enhancements

Many changes have been made to the CLI for HMC V7 R3 to take advantage of the new features that are available in AIX and the POWER6 hardware.

This chapter provides information about changes made to the CLI for the following new features:

- Host Ethernet Adapter (HEA)
- Partition Availability Priority (PAP)
- Shared Pool Usage of Dedicated Processor Capacity for active partitions
- Partitioning Support for Barrier Synchronization Register (BSR)
- System Planning enhancements
- Managed System Dump enhancements
- Partition Processor Compatibility Modes
- Utility Capacity on Demand (CoD)
- ► i5/OS only enhancements
- Other changes in CLI not related to specific features

# 10.1.1 Host Ethernet Adapter

The commands that we list in this section have been enhanced to support Host Ethernet Adapter (HEA), which is a feature of POWER6 servers only.

For more information about Host Ethernet Adapter, see 7.1.1, "Host Ethernet Adapter" on page 221.

#### Ishwres

The HEA added hardware resources to the system. The **1shwres** command adds parameter options that lists the new resources. To list HEA resources (POWER6 servers only), use this command:

```
lshwres -r hea -m managed-system
--rsubtype {logical | phys}
--level {port | port_group | sys}
[-R] [--stat]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

For the parameters in this command:

► --rsubtype logical

Lists the valid HEA resource subtypes for *logical* HEA resources.

► --rsubtype phys

Lists the valid HEA resource subtypes for *physical* HEA resources.

The --rsubtype parameter is required when listing HEA resources.

► --stat

When specified, the port counter statistics for HEA physical ports are listed.

► --level "port" | "port\_group" | "sys"

When specified with the -- stat parameter, this parameter provides information for a particular port, port\_group, or the entire adapter.

--filter "adapter\_ids"

This parameter has been enhanced to support HEA.

► --filter "port\_groups"

This parameter has been added to specify HEA port groups.

Valid filters for 1shwres -r hea include:

- --rsubtype logical --level sys: adapter\_ids, lpar\_ids | lpar\_names
- -- rsubtype logical --level port: adapter\_ids, lpar\_ids | lpar\_names, port\_groups
- --rsubtype phys --level sys: adapter ids
- --rsubtype phys --level port: adapter ids, port groups
- --rsubtype phys --level port\_group: adapter\_ids, port\_groups

#### chhwres

The **chhwres** command changes the hardware resource configuration of the managed system. This command is used to perform dynamic logical partitioning (DLPAR) operations and was updated so that HEA logical ports could be added, removed, or moved or so that the configuration could be updated.

To add, remove, or move an HEA logical port (POWER6 servers only), use this command:

```
chhwres -r hea -m managed-system -o {a | r | m}
{-p partition-name | --id partition-ID}
[{-t target-partition-name | --tid target-partition-ID}]
-1 HEA-adapter-ID
[--physport physical-port-ID]
-g port-group --logport logical-port-ID
[-a "attributes"]
[-w wait-time] [-d detail-level] [--force]
```

To set HEA attributes (POWER6 servers only), use this command:

```
chhwres -r hea -m managed-system -o s
-l HEA-adapter-ID
[--physport physical-port-ID]
-g port-group -a "attributes"
```

For the parameters in this command:

- ▶ -1 HEA-adapter-ID
  - The ID of the HEA to add, remove, or move
  - The DRC index of the slot
- --physport physical-port-ID
  - The ID of the HEA physical port
  - A required option when adding an HEA logical port to a partition
- ► -g port-group
  - The port group that includes the HEA logical port to add, remove, or move
  - The -g option is required for all (and only) HEA operations
  - This option is required when --logport is specified
- --logport logical-port-ID
  - The ID of the HEA logical port to add, remove, or move
- -a lhea\_capabilities
  - Comma separated list of LHEA capabilities
  - Valid formats are *capability* or 5/ieq/nieq/qp/cq/mr

# chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes of the managed-frame. This command supports the += and -= syntax.

To use this command, use this syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

These are the attributes that you can change for partition profiles (-r prof):

- Ihea\_logical\_ports
  - POWER6 servers only.
  - Comma separated list of LHEA logical ports, with each logical port having the format:

adapter-ID/port-group/physical-port-ID/logical-port-ID/allowed-VLAN-IDs

All four slash (/) characters must be present, but optional values can be omitted. Optional values are allowed-VLAN-IDs.

- Ihea\_capabilities
  - POWER6 servers only.
  - Comma separated list of LHEA capabilities, with each capability having one of the following formats:

adapter-ID/capability or adapter-ID/5/ieq/nieq/qp/cq/mr

#### rsthwres

The **rsthwres** command restores the hardware resource configuration of partitions in the managed system. This operation might need to be performed after a DLPAR operation fails. This command was updated to handle the new LHEA resources.

For this command, use the following syntax:

```
rsthwres -r hea -m managed-system
[{-p partition-name | --id partition-ID}]
[-1 HEA-adapter-ID]
[-g port-group --logport logical-port-ID]
```

When restoring HEA resources, specify the adapter ID of the HEA to restore. If this option is omitted and a partition is specified with the -p or --id option, then

all HEA resources, including LHEA and logical ports that are assigned to the specified partition are restored. If this option is omitted and a partition is not specified, then all HEA resources in the managed system are restored. This option is required when the **-g** and **--logport** options are specified to restore a specific logical port.

#### mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile and was updated to accept new parameters in the configuration file to configure HEA resources.

To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The new attributes for this command are:

- Ihea\_logical\_ports
  - POWER6 servers only.
  - Comma separated list of LHEA logical ports, with each logical port having the following format:

adapter-ID/port-group/physical-port-ID/logical-port-ID/allowed-VLAN-IDs

All four slash (/) characters must be present, but optional values can be omitted. Optional values are allowed-VLAN-IDs.

- Ihea\_capabilities
  - POWER6 servers only.
  - Comma separated list of LHEA capabilities, with each capability having one of the following formats:

adapter-ID/capability or adapter-ID/5/ieq/nieq/qp/cq/mr

 Valid values are 0 (base minimum - default), 1 (low), 2 (medium), 3 (high), 4 (dedicated), and 5 (custom).

# lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can also list the attributes of the managed system, and of all of the systems managed by this HMC. This command was updated to handle the attributes associated with LHEA resource attributes.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

In this command:

- ► -F lhea\_capable
  - The -F option is an added option to show if the managed system is LHEA capable.
  - The managed system is LHEA capable only if the hypervisor supports HEA and physical HEA exists.

# **Examples of HEA commands**

Here are some examples of common HEA commands:

► List all physical HEAs on the managed system:

lshwres -r hea -m mySys --rsubtype phys --level sys

► List all port groups for all HEAs on the managed system:

lshwres -r hea -m mySys --rsubtype phys --level port\_group

 List all physical ports belonging to port group 2 for the HEA with adapter ID 23000010:

```
lshwres -r hea -m 9117-MMA*1234ABC --rsubtype phys --level port
--filter "adapter_ids=23000010,port_groups=2"
```

► List all Logical Host Ethernet adapters (LHEA) on the managed system:

```
lshwres -r hea -m mySys --rsubtype logical --level sys
```

List all HEA logical ports assigned to partition p1:

```
lshwres -r hea -m mySys --rsubtype logical --level port --filter
"lpar_names=p1"
```

► Restore all HEA resources in the managed system:

```
rsthwres -r hea -m mySystem
```

Restore all HEA resources for partition p1:

```
rsthwres -r hea -m mySystem -p p1
```

 Restore the logical port with ID 3 in port group 2 of the HEA with an adapter ID of 23000010:

```
rsthwres -r hea -m 9117-MMA*1112223 --logport 3 -g 2 -l 23000010
```

Add logical port 4 for physical port 0 belonging to port group 2 of the HEA with an adapter ID of 23000020 to partition p1. Also set the LHEA capability level to low:

```
chhwres -r hea -m mySystem -o a -p p1 -l 23000020 --physport 0 -g 2 --logport 4 -a "lhea capabilities=1"
```

Remove logical port 1 belonging to port group 2 of the HEA with an adapter ID of 23000020 from the partition with ID 8:

```
chhwres -r hea -m 9117-MMA*123432C -o r --id 8 -l 23000020 -g 2 --logport 1
```

 Set physical port attributes for port group 2 of physical port 1 of the HEA with an adapter ID of 23000020:

```
chhwres -r hea -m mySystem -o s -l 23000020 -g 2 --physport 1 -a
"conn_speed=auto,duplex=auto,flow_control=1"
```

 Set port group attributes for port group 1 of the HEA with an adapter ID of 23000030:

```
chhwres -r hea -m sys1 -o s -l 23000030 -g 1 -a
"pend port group mcs value=4"
```

# **10.1.2 Partition Availability Priority**

The commands that we list in this section have been enhanced to support Partition Availability Priority (POWER6 servers only).

For more information about Partition Availability Priority, see 7.1.3, "Partition availability priority" on page 225.

#### lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can also list the attributes of the managed system, and of all of the systems managed by this HMC and was updated to handle the attributes associated with Partition Availability Priority attributes.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The parameters in this command:

- -F lpar\_avail\_priority\_capable
  - Shows if a managed system supports Partition Availability Priority.
  - Valid values are 0, 1.
- -F lpar\_avail\_priority
  - Displays the current Partition Availability Priority setting.
  - Valid values are 0 through 255.

# mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile and was updated to accept new parameters in the configuration file to configure Partition Availability Priority attributes.

To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The new attribute is:

- Ipar\_avail\_priority
  - Partitions created with a default value of 127.
  - Valid values are:
    - Minimum (0) the lowest priority. This partition is most likely to be affected by recovery events.
    - Low (63) indicates low priority.
    - Default (127) the default setting for most newly created partitions.
    - High (191) the default setting for newly created special partitions types such as Virtual I/O Server partition.
    - Maximum (255) the highest priority setting.
    - Custom (0 255) allows users to enter their custom priority setting.

# chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes of the managed-frame and was updated to handle the new Partition Availability Priority configuration attributes.

To use this command, use the following syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

The new attribute is:

- lpar\_avail\_priority
  - Partitions created with a default value of 127.
  - Valid values are:
    - Minimum (0) this is the lowest priority. This partition is most likely to be affected by recovery events.
    - Low (63) indicates low priority.
    - Default (127) this is the default setting for most newly created partitions.
    - High (191) this is the default setting for newly created special partitions types such as Virtual I/O Server partition.
    - Maximum (255) This is the highest priority setting.
    - Custom (0 255) allows users to enter their custom priority setting.

#### **Examples of Partition Availability Priority commands**

Here are some examples of common Partition Availability Priority commands:

Show if a managed system supports Partition Availability Priority:

lssyscfg -r sys -m system1 -F lpar\_avail\_priority\_capable

► Create a partition with Partition Availability Priority set to default value:

```
mksyscfg -m system1 -r lpar -i
name=part1,profile_name=test,lpar_env=aixlinux,min_mem=512,desired_m
em=512,max mem=512
```

• Display the Partition Availability Priority setting of a partition:

lssyscfg -r lpar -m system1 -F lpar\_avail\_priority

► Set/change Partition Availability Priority of a partition:

```
chsyscfg -r lpar -m system1 -i name=part1,lpar_avail_priority=45
```

# 10.1.3 Shared pool usage of dedicated

This feature allows an active dedicated processor partition to share its unused processors. The commands that we list in this section have been enhanced to support shared pool usage.

You can find more information in 7.1.2, "Shared pool usage of dedicated capacity" on page 223.

# lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can also list the attributes of the managed system and of all of the systems managed by this HMC. The **1ssyscfg** command was updated to handle the attributes associated with Dedicated Processor Shared Pool Usage attributes.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The parameters for this command are:

-F active\_lpar\_share\_idle\_procs\_capable

Displays if the system supports Shared Dedicated Processors.

► -F sharing\_mode

Valid modes include share\_idle\_procs\_always and keep\_idle\_procs.

► -F state

Valid mode includes Running.

# mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile and was updated to accept new parameters in the configuration file to configure Dedicated Processor Shared Pool Usage attributes. To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The new attributes are:

► sharing\_mode

Valid values for partitions using dedicated processors include:

– keep\_idle\_procs

Never share processors.

- share\_idle\_procs\_always

Always share processors (POWER6 servers only).

- share\_idle\_procs

Share processors only when partition is inactive.

- share\_idle\_procs\_active

Share processors only when partition is active (POWER6 servers only).

# chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes of the managed-frame and was updated to handle the new Dedicated Processor Shared Pool Usage configuration attributes.

To use this command, use the following syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

The new attribute is:

▶ sharing\_mode

Valid values for partitions using dedicated processors are:

– keep\_idle\_procs

Never share processors.

- share\_idle\_procs\_always

Always share processors (POWER6 servers only).

- share\_idle\_procs

Share processors only when partition is inactive.

- share\_idle\_procs\_active

Share processors only when partition is active (POWER6 servers only).

#### chhwres

The **chhwres** command changes the hardware resource configuration of the managed-system. It is used to perform dynamic logical partitioning (DLPAR) operations and was updated to handle the new Dedicated Processor Shared Pool Usage configuration attributes.

To use this command, use the following syntax:

```
chhwres -r proc -m managed-system -o s
{-p partition-name | --id partition-ID}
-a "attributes"
```

The new attribute is:

▶ sharing\_mode

Valid values for partitions using dedicated processors are:

– keep\_idle\_procs

Never share processors.

- share\_idle\_procs\_always

Always share processors (POWER6 servers only).

- share\_idle\_procs

Share processors only when partition is inactive.

- share\_idle\_procs\_active

Share processors only when partition is active (POWER6 servers only).

- Can be changed when the partition is in running condition.

#### Ishwres

The **1shwres** command lists the hardware resources of the managed system, including physical I/O, virtual I/O, memory, processing, Host Channel Adapter (HCA), HEA, and Switch Network Interface (SNI) adapter resources. New filters were added for the new Dedicated Processor Shared Pool Usage feature.

To use this command, use the following syntax:

```
lshwres -r proc -m managed-system
--level {lpar | pool | sys} [-R]
[--procunits quantity]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The new attributes are:

- ► -F pend\_sharing\_mode
  - Describes the pending capping mode,
  - Valid modes are capped and uncapped.
- ► -F sharing\_mode
  - share\_idle\_procs\_active

Specifies Donor mode.

- share\_idle\_procs

Specifies Sharing mode.

#### Islparutil

The **lslparutil** command lists utilization data that is collected for a managed system. This command also lists the HMC settings for utilization data collection.

To use this command, use the following syntax:

```
Islparutil -r {hmc | lpar | pool | sys | all}
-m managed-system
[-d number-of-days] [-h number-of-hours]
[--startyear year] [--startmonth month]
[--startday day] [--starthour hour]
[--endyear year] [--endhour hour]
[-n number-of-events] [-s sample-rate]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

A new attribute was added to the <code>shared\_cycles\_while\_active</code> filter that shows the total cycles donated by this LPAR since PHYP IPL.

#### Examples of shared pool usage commands

Here are some examples of shared pool usage commands:

 Display if a managed system is capable of donating idle processor cycles when the partition is in active state:

lssyscfg -r sys -m system1 -F active\_lpar\_share\_idle\_procs\_capable

Modify the Sharing/Donor attribute while creating the profile:

```
mksyscfg -r prof -m system1 -i
"name=prof2,lpar_name=part1,min_mem=256,desired_mem=1024,max_mem=102
4,proc_mode=ded,min_procs=1,desired_procs=1,max_procs=1,sharing_mode
=keep_idle_procs"
```

• Display current value of sharing attribute:

```
lssysfcg -r prof -m system1 --filter "lpar_names=part1" -F
sharing_mode
```

• Change the Sharing/Donor attribute of a profile:

```
chsyscfg -r prof -m system1 -i
"name=prof1,lpar name=part1,sharing mode=share idle procs always"
```

• Change the Sharing/Donor attribute of a partition:

```
chhwres -m system1 -r proc -o s -a
"sharing_mode=share_idle_procs_active" -p part1"
```

• Display the current state of the partition:

lssyscfg -r lpar -m system1 -F name,state --filter lpar\_names=part1

# 10.1.4 Partitioning support for barrier synchronization register

The commands that we list in this section have been enhanced to support barrier synchronization register (POWER6 technology only).

For more information about barrier synchronization register, see 1.4.10, "Barrier Synchronization Register" on page 13.

#### lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can also list the attributes of the managed system and of all of the systems managed by this HMC. The **1ssyscfg** command was updated to handle the attributes associated with barrier synchronization register attributes.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The filter attribute was added:

► -F bsr\_capable

Valid values are 0 and 1.

# mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile and was updated to accept new parameters in the configuration file to configure barrier synchronization register attributes.

To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The new attribute is bsr\_arrays, which accepts an integer value.

# chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes the managed-frame and was updated to accept new parameters in the configuration file to configure barrier synchronization register attributes.

To use this command, use the following syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

The new attribute is bsr\_arrays, which accepts an integer value and supports the += and -+ syntax.

#### Ishwres

The **1shwres** command lists the hardware resources of the managed system, including physical I/O, virtual I/O, memory, processing, HCA, HEA, and SNI adapter resources. New filters were added for the new barrier synchronization register feature.

To use this command, use the following syntax:

```
lshwres -r proc -m managed-system
--level {lpar | pool | sys} [-R]
[--procunits quantity]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

New attributes for this command include:

- New filters
  - -F total\_sys\_bsr\_arrays

The number of BSR arrays that can be assigned to partitions.

- -F bsr\_array\_size

The number of bytes in each assignable array.

- -F curr\_avail\_sys\_bsr\_arrays

The number of arrays that are not currently assigned to any partition.

- ▶ lshwres-r mem --level lpar
  - -F curr\_bsr\_array

The number of BSR arrays that are allocated to a partition.

#### Examples of barrier synchronization register commands

Here are some examples of barrier synchronization register commands:

Show if a managed system is BSR-capable if the hypervisor supports BSR partitioning and a BSR exists:

lssyscfg -r sys -m system1 -F bsr\_capable

Display the number of BSR arrays that can be assigned, the size of each assignable BSR array, and the number of BSR arrays that are currently available for assignment:

```
lshwres -r mem --level sys -m system1 -F
total_sys_bsr_array_size,curr_avail_sys_bsr_arrays
```

► Display the number of BSR arrays that are currently allocated to a partition:

```
lshwres -r mem --level lpar -m system1 --filter lpar_ids=1 -F
curr_bsr_arrays
```

#### 10.1.5 System planning

The commands that we in this section have been added to support new system planning features.

#### defsysplanres

The **defsysplanres** command defines a system plan resource for use by system plans deployed from the HMC:

```
defsysplanres -r osinstall -n resource-name
-v "resource-value" [-d "resource-description"] [--help]
```

#### Issysplanres

The **1ssysplanres** command lists the system plan resources that are defined on this HMC. These resources can be used when deploying system plans from this HMC.

```
lssysplanres -r osinstall
[-F [attribute-names][--header]] [--help]
```

#### rmsysplan

The **rmsysplan** command removes a system plan file from the system plan file directory on the HMC:

rmsysplan -f file-name [--help]

#### 10.1.6 HMC dump commands

The HMC allows users to show and configure the dump policy values. The commands that we list in this section have been enhanced to support the features added to the dump functions.

#### lsdump

The **1sdump** command lists the dumps that are available on the managed system or the managed-frame. It can list the managed system dumps and the managed frame dumps that are available on the HMC and also lists the system dump parameters for the managed system. This command is only supported for POWER6 servers. The syntax for this command is:

```
lsdump -m managed-system -r parm
[-F [attribute-names] [--header]]
```

The attribute for this command is -r parm, which is enhanced to display dump offload parameters.

#### dump

The **dump** command sets the system dump parameters for the managed system. This operation is only supported for POWER6 servers.

The syntax for this command is:

```
dump -m managed-system -t sys -o set -a "attributes" [--help]
```

The attributes for this command are:

- This is a new command added in HMC 7.3.
- The command sets the system dump parameters for a managed system (POWER6 servers only).

# 10.1.7 Partition processor compatibility modes

The commands that we list in this section have been enhanced to support partition processor compatibility mode. Changing modes is supported using command line only.

For more information about partition processor compatibility modes, see 1.4.6, "Processor compatibility" on page 11.

#### lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can list the attributes of the managed system, and of all of the systems managed by this HMC and can also list the attributes of cages in the managed-frame, the attributes of the managed-frame, or the attributes of all of the frames managed by this HMC.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The attributes for this command are:

- Issyscfg -r sys displays two new attributes:
  - lpar\_proc\_compat\_mode\_capable

Displays 0 (not capable), or 1 (capable).

- lpar\_proc\_compat\_modes

Displays only if lpar\_proc\_compat\_mode\_capable value is 1.

Displays value of default or enhanced (POWER6 servers only).

- ► lssyscfg -r lpar displays two new attributes:
  - desired\_lpar\_proc\_compat\_mode
  - Displays default or enhanced.
- curr\_lpar\_proc\_compat\_mode
  - Displays default, POWER6, or enhanced.
- Issyscfg -r prof displays one new attribute
  - lpar\_proc\_compat\_mode
  - Displays default or enhanced (only if plar\_proc\_mode\_capable value is 1).

#### mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile.

To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The new attributes are:

- ► -r {prof | 1par}
  - Accepts the new partition attribute lpar\_proc\_compat\_mode.
  - Valid values are default or enhanced.
  - Valid only if the managed system supports partition processor compatibility modes.
  - Can be set for full system partitions.

# chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes the managed-frame.

To use this command, use the following syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

The new attribute is:

▶ -r prof

lpar\_proc\_compat\_mode

- Valid values are default or enhanced.
- Valid only if the managed system supports partition processor compatibility modes.
- Can be set for full system partitions.

# Examples of partition processor compatibility mode commands

Here are some examples of partition processor compatibility mode commands:

► Show if the managed system is processor compatibility capable:

lssyscfg -m system1 -r sys -F lpar\_proc\_compat\_mode\_capable

 Display all supported partition processor compatibility modes for the managed system:

lssyscfg -m system1 -r sys -F lpar\_proc\_compat\_modes

► Change the processor compatibility mode of the managed system to default:

```
chsyscfg -m system1 -r prof -i
"name=profile-name,lpar_name=partition-name,lpar_proc_compat_mode=de
fault"
```

# 10.1.8 Utility Capacity on Demand

The commands that we list in this section have been enhanced to support Utility Capacity on Demand (CoD).

For more information about Utility CoD, see 13.3.4, "Utility CoD" on page 383.

#### chcod

The **chcod** command performs CoD operations on the managed system. It is used to enter a CoD code for the managed system. This command is used to activate On/Off CoD, Reserve CoD, or Utility CoD resources or to deactivate On/Off CoD, Reserve CoD, Trial CoD, or Utility CoD resources. CoD resources are either memory or processors.

The **chcod** command is also used to set or disable a Utility CoD processor minute usage limit. Reserve CoD is only supported on POWER5 servers. Utility CoD is only supported on POWER6 servers.

To activate or change the number of Reserve CoD or Utility CoD processors, use this syntax:

```
chcod -o a -m managed-system -c {reserve | utility}
-r proc -q quantity-of-processors
```

To deactivate all On/Off CoD, all Reserve CoD, all Trial CoD, or all Utility CoD resources, use this syntax:

```
chcod -o d -m managed-system
-c {onoff | reserve | trial | utility}
-r {mem | proc}
```

To set or disable a Utility CoD processor minute usage limit, use this syntax:

```
chcod -o s -m managed-system -c utility -r proc
-1 number-of-processor-minutes
```

#### lscod

The **1scod** command lists CoD information for the managed system. Reserve CoD is only supported on POWER5 servers. Utility CoD is only supported on POWER6 servers.

To use this command, use the following syntax:

```
lscod -t {bill | cap | code | hist | util}
-m managed-system
[-c {cuod | mobile | onoff | reserve | trial | trialexc |
trialstd | utility | utilityen}]
[-r {mem | proc}]
[-F [attribute-names] [--header]] [--help]
```

The following options and attribute-names were added to valid CoD types:

- ► -c {utility | utilityen}
  - Utility CoD reporting codes | Utility CoD enablement codes
- ► -t cap -c utility -r proc -F attribute-names
  - -F utility\_state
  - -F activated\_utility\_procs
  - -F avail\_procs\_for\_utility
  - -F utility\_days\_left
  - -F proc\_min\_usage
  - -F proc min left
  - -F this\_month\_proc\_min
  - -F last month proc min
  - -F total\_proc\_min
  - -F unreported proc min
  - -F reporting\_threshold
  - -F reporting\_limit
  - -F time\_last\_reported
  - -F proc\_min\_last\_reported
- ▶ -t util -c utility -r proc
  - -F non\_utility\_procs
  - -F utility\_procs
  - -F non\_utility\_procs\_util
  - -F utility\_procs\_util
  - -F sample sys date
  - -F sample\_sys\_time
  - -F sample\_rate

- ▶ -t code -c utility -r proc
  - -F anchor\_card\_ccin
  - -F anchor\_card\_serial\_num
  - -F anchor\_card\_unique\_id
  - -F sys\_type
  - -F sys\_serial\_num
  - -F resource\_id
  - -F activated\_resources
  - -F sequence\_num
  - -F entry\_check
- ► -t code -c utilityen -r proc
  - -F anchor\_card\_ccin
  - -F anchor\_card\_serial\_num
  - -F anchor\_card\_unique\_id
  - -F unreported\_processor\_minutes
  - -F sys\_type
  - -F sys\_serial\_num
  - -F resource\_id
  - -F activated\_resources
  - -F sequence\_num
  - -F entry\_check

#### Islparutil

The **1s1paruti1** command lists utilization data that is collected for a managed-system. This command also lists the HMC settings for utilization data collection.

The HMC collects the following types of utilization data: sampling events, state change events, configuration change events, and Utility CoD processor usage events.

To use this command, use the following syntax:

```
lslparutil -r {hmc | lpar | pool | sys | all}
-m managed-system
[-d number-of-days] [-h number-of-hours]
[--startyear year] [--startmonth month]
[--startday day] [--starthour hour]
[--endyear year] [--endmonth month]
[--endday day] [--endhour hour]
[-n number-of-events] [-s sample-rate]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The attribute that was added for Utility CoD is:

shared\_cycles\_while\_active

This attribute returns the number of dedicated processing cycles shared by this partition while it has been active since the managed system was started.

## **Examples of Utility CoD commands**

Here are some examples of Utility CoD commands:

 Add Utility CoD processors to the shared processor pool or change the number of Utility CoD processors:

```
chcod -o a -m system1 -c utility -r proc -q quantity-of-processors
```

► Remove all Utility CoD processors from the shared processor pool:

chcod -o d -m system1 -c utility -r proc

Display Utility CoD enablement code generation information:

lscod -t code -m system1 -c utilityen -r proc -F "" --header

Display Utility CoD shared processor utilization:

lscod -t util -m system1 -c utility -r proc -F "" --header

# 10.1.9 i5/OS only enhancements

This section includes CLI enhancements that pertain to i5/OS only. The commands that we list here have been enhanced to support various features on HMC 7.3.

#### lssyscfg

The **1ssyscfg** command lists the attributes of partitions, partition profiles, or system profiles for the managed system. It can list the attributes of the managed system and of all of the systems managed by this HMC and can also list the attributes of cages in the managed-frame, the attributes of the managed-frame, or the attributes of all of the frames managed by this HMC.

To use this command, use the following syntax:

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

The following attribute was added for POWER6 servers running i5/OS:

Issyscfg -F "electronic\_err\_reporting\_capable"

#### mksyscfg

The **mksyscfg** command creates partitions, partition profiles, or system profiles for the managed system. It can also be used to save the current configuration of a partition to a new partition profile.

To use this command, use the following syntax:

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system
[{-f configuration-file | -i "configuration-data"}]
[-o save {-p partition-name | --id partition-ID}
-n profile-name]
[--help]
```

The following attribute was added:

```
mksyscfg -i "electronic_err_reporting={0 | 1}
```

Enables or disables Electronic Error Reporting.

The load\_source\_slot attribute is no longer required to be specified when creating an i5/OS partition or partition profile on a POWER6 server.

#### chsyscfg

The **chsyscfg** command changes the attributes of partitions, partition profiles, or system profiles for the managed system. It can also change the attributes of the managed system as well as the attributes the managed-frame.

To use this command, use the following syntax:

```
chsyscfg -r {lpar | prof | sys | sysprof | frame}
{-m managed-system | -e managed-frame}
{-f configuration-file | -i "configuration-data"}
[--help]
```

The following attribute was added:

chsyscfg -i electronic\_err\_reporting={0 | 1}

Changes the Electronic Error Reporting value.

#### chsysstate

The **chsysstate** command changes the state of a partition, the managed system, or the managed-frame. It was updated to enable console service functions on an i5/OS partition.

To perform an operator panel service function on a partition:

```
chsysstate -m managed-system -r lpar
-o {dston | remotedstoff | remotedston |
consoleservice | iopreset | iopdump}
{-n partition-name | --id partition-ID}
```

The option that was added is consoleservice, which enables console service functions for the partition (operator panel function 65 followed by 21).

# 10.1.10 Other changes in CLI that are not related to specific features

The section lists command line options that are not necessarily related to any of the new features that we have listed previously in this chapter.

New options have been added to the **chhmc** command to set the date, time, time zone, and clock on the HMC.

```
chhmc -c date
-s modify
[--datetime date-time]
[--clock {local | utc}]
[--timezone {time-zone | none}]
[--help]
```

Option requirements changed for the lssyscfg command:

Issyscfg -r prof -m managed system now lists all partition profiles for all partitions in the managed system. The --filter option is no longer required.

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame}
[-m managed-system | -e managed-frame]
[--filter "filter-data"]
[-F [attribute-names] [--header]] [--help]
```

A new option has been added to the **chsvcevent** command to close one or all serviceable events on the HMC. The options added were close and closeall.

```
chsvcevent -o {close | closeall}
[-p problem-number -h analyzing-HMC] [--help]
```

A new option has been added to the **mksysplan** command to limit the inventory gathered to just the PCI slot devices. The new option is noprobe. A new option has been added to the **mksysplan** command to display verbose output during command processing in addition to the default message, the new option is **-v**.

```
mksysplan -f file-name -m managed-system
[--check] [-d "description"] [-o noprobe] [-v] [--help]
```

The **lslic** command has been enhanced to display automatic code download status. The new options are -t power and -t syspower.

```
lslic {-m managed-system | -e managed-frame | -w}
[-t {sys | power | syspower | powerfru}]
[-r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint}
[-h host-name] [-u user-ID] [--passwd password] [-d directory]
[-F [attribute-names] [--header]] [--help]
```

▶ lslic -t power | syspower

The **dlslic** command has been removed. The information that was displayed by the **dlslic** command is now displayed by the **lslic** command.

The lsusrtca command has been deprecated.

# 10.2 Most common command line options and usage

In this section, we list some of the most commonly used command line options.

#### Display information about systems, partitions, and profiles

Issysconn

Definition: List system connections

#### Example:

 List connection information for all systems and frames managed by this HMC:

lssysconn -r all

Issyscfg

Definition: List system configuration

#### Examples:

- List all configuration information for systems managed by this HMC:

lssyscfg -r sys

 List all partitions in the managed system and only display attribute values for each partition, following a header of attribute names:

lssyscfg -r lpar -m system1 -F --header

► 1shwres

Definition: Lists hardware resources

#### Examples:

- List all system level memory informations:

```
lshwres -r mem -m system1 --level sys
```

- List all virtual slots for partition part1:

```
lshwres -r virtualio --rsubtype slot -m system1 --level slot
--filter "lpar names=lpar1"
```

#### **Modifying resources**

► chsyscfg

Definition: Modifying system resources

#### Examples:

 Change a partition profile's memory amounts (reduce the profile's current memory amounts each by 256 MB) and number of desired processors:

```
chsyscfg -r prof -m system1 -i
"name=profile1,lpar_name=part1,min_mem=256,desired_mem=256,max_me
m=256,desired_procs=2"
```

- Change a partition profile's memory amounts (reduce the profile's current memory amounts each by 256 MB) and number of desired processors:

```
chsyscfg -r prof -m system1 -i
"name=profile1,lpar_name=part1,min_mem=256,desired_mem=256,max_me
m=256,desired_procs=2"
```

- Change a system profile (add two new partition profiles):

```
chsyscfg -r sysprof -m system1 -i
"name=sysprof1,"lpar_names+=part3,part4","profile_names+=3_prof1,
4 defaultProf""
```

chhwres

Definition: Modifying hardware resources

#### Examples:

- Add a virtual Ethernet adapter to the partition with ID 3:

```
chhwres -r virtualio -m system1 -o a --id 3 --rsubtype eth -a
"ieee_virtual_eth=1,port_vlan_id=4,"addl_vlan_ids=5,6",is_trunk=1
,trunk_priority=1"
```

#### **Creating resources**

▶ mksyscfg

Definition: Create system resources

#### Example:

- Create an AIX or Linux partition:

```
mksyscfg -r lpar -m system1 -i
"name=aix_lpar2,profile_name=prof1,lpar_env=aixlinux,min_mem=256,
desired_mem=1024,max_mem=1024,proc_mode=ded,min_procs=1,desired_p
rocs=1,max_procs=2,sharing_mode=share_idle_procs,auto_start=1,boo
t_mode=norm,lpar_io_pool_ids=3,"io_slots=21010003/3/1,21030003//0
""
```

#### **Removing / restoring resources**

► rmsyscfg

Definition: Remove a system resource

#### Example:

- Remove the partition profile test\_profile for partition lpar3:

rmsyscfg -r prof -m system1 -n test\_profile -p lpar3

rmsysconn

Definition: Remove system connection

#### Example:

Disconnect from the managed system sytem1 and remove it from the HMC:

rmsysconn -o remove -m system1

► rsthwres

Definition: Restore hardware resources

#### Example:

- Restore memory resources for partition p1:

```
rsthwres -r mem -m system1 -p p1
```

#### **Partition communication**

► mkvterm

Definition: Opens a virtual terminal session to a partition

#### Example:

- Open a virtual terminal session for partition p1:

```
mkvterm -m system1 -p p1
```

# Problem determination of the HMC or managed systems

► 1shmc

Definition: Lists HMC configuration information

#### Example:

- List the BIOS level of the HMC

lshmc -b

- List the network settings for the HMC

lshmc -n

- List the VPD information for the HMC lshmc -v
- List the version information for the HMC

lshmc -V

► lspartition

Definition: Lists partition and their states.

#### Example:

- List the status of DLPAR enabled partitions

lspartition -dlpar

► pesh

Definition: Provides PE Shell access

► pedbg

Definition: Product Engineering debug tools

#### Example:

 Collect various logs and javacore. This option can copy the data collected onto DVD or leave a compressed file in the /dump directory.

```
pedbg -c
```

► lssysconn

Example:

List connection information for all systems and frames managed by this HMC:

lssysconn -r all

► lshmcusr

Definition: Lists all users on the HMC

#### Example:

- List all users defined on this HMC:

lshmcusr

Issvcevents

Definition: List console or serviceable events

# Example:

- List the console events that occurred within the past three days:
   lssvcevents -t console -d 3
- List all of the open serviceable events for the system 1:

lssvcevents -t hardware -m system1 --filter "status=open"

# 11

# **Firmware maintenance**

This chapter describes the various options that are available for maintaining both Hardware Management Console (HMC) and managed system firmware levels. We show you, through examples, the main firmware update options.

We discuss the different methods of updating the HMC to a new software level as well as installing individual fix packs. We also cover the temporary and permanent side of the firmware on a POWER6. Finally, we show the various options available to POWER6 system's firmware, either through the HMC or through an AIX service partition.

# 11.1 Critical Console Data backup

Before you begin any firmware upgrade, it is important that you maintain a current Critical Console Data (CCD) backup. This back up can be useful in recovering the HMC in the event of the loss of a disk drive.

When you move to a new version level of HMC or use a Recovery CD to update the HMC, you need to create a new CCD backup immediately following the installation. If you update HMC code between releases using the Corrective Service files downloadable from the Web and then create new CCD backups after the update, you can use those CCD backups and the last-used Recovery CD to rebuild the HMC to the level in use when the disk drive was lost.

Another example where a CCD would be useful is when replacing an FSP or BPC on a POWER6 server. You need to make a fresh CCD backup *before* starting the replacement to preserve the DHCP lease file on the HMC that lists the starting FSP and BPC IP addresses. If for some reason things do not work after you replace the FSP or BPC, you can use the backup to restore the original information. If the replacement is successful, a new IP address is assigned to the new component, and the lease file is updated. At this point, a new CCD backup is created that captures the freshly updated DHCP lease file.

With the HMC, you can back up the following important data:

- User-preference files
- User information
- HMC platform-configuration files
- HMC log files
- HMC updates through Install Corrective Service

Use the archived data only in conjunction with a reinstallation of the HMC from the product CDs.

**Note:** You cannot restore the Critical Console Data backup on different versions of HMC software.

# 11.1.1 Manual back up of Critical Console Data

To back up the HMC, you must be a member of one of the following roles:

- ► Super administrator
- Operator
- Service representative

You must format the DVD in the DVD-RAM format before you can save data to the DVD. To format a DVD, select **HMC Management**  $\rightarrow$  **Format Media** from the HMC workplace window (Figure 11-1).

To back up CCD, click **HMC Management**  $\rightarrow$  **Backup HMC Data**.

Hardware Management Console	
Back up HMC Data	
🗇 Welcom e	HMC Management (HMC Version)
<ul> <li>☑ System s Management</li> <li>☑ Servers</li> <li>☑ 1 Custom Groups</li> <li>☑ System Plans</li> <li>☑ HMC Management</li> </ul>	Operations View HMC Events Shut Down or Restart Schedule Operations Format Media Back up HMC Data
Att ps://hmc2.itsc.austin.ibm.com - HMC: Back up Critical Console	
You selected to back up critical data for the Hardware Management Console (HMC). Select an archive option and click Next.	
<ul> <li>Back up to DVD on local system</li> <li>Back up to mounted remote system</li> <li>Send back up critical data to remote site</li> </ul>	
Next Cancel Help	
ど Done	🔒 🔮 Internet 🛒
	Remote Virtual Lerminal

Figure 11-1 Back up Critical Console Data

Then, select an archive option. You can back up to a DVD on the HMC, back up to a remote system mounted to the HMC file system, or a remote site through FTP. After you select an option, click **Next**.

Follow the instructions to back up the data. Figure 11-2 shows an example to back up Critical Data to DVD.

Back up Critical Data to DVD	
Insert a formatted DVD into the drive. Use the description area to add information specific for this archive. Click OK to back up the data.	
Description:	
CCD backup 0700707	
OK Cancel Help	

Figure 11-2 CCD back up to DVD

You can add specific information related to the Critical Console Data backup.

# 11.1.2 Scheduled Critical Console Data backup

You need to back up the CCD up at least once a week. You should also keep two copies of the CCD backup—one copy from the upgrade or any changes to the HMC and one backup CCD to store in a safe place. For information on how to make a backup, see 11.1, "Critical Console Data backup" on page 304.
To schedule a CCD backup, select **HMC Management**  $\rightarrow$  **Schedule Operations** from the HMC workplace window. Then, follow these steps:

1. In the Customize Scheduled Operations window, select **Options**  $\rightarrow$  **New** (Figure 11-3).

Cust	omize S	Sched	luled	Operation	s
Optio	ons▼	View *	So	ort ▼ Help	•
All sch	eduled	opera	tions	are current	ly displayed.
Select	Target	Date	Time	Operation	Remaining Repetitions

Figure 11-3 Customize Scheduled Operations

- 2. In the Add a Scheduled Operation window, select OK.
- 3. On the Date and Time tab, select the date and time, and time window for the first backup, as shown in Figure 11-4. The scheduled operation will start at that time window.

Set up a Scheduled Operation       Date and Time     Repeat       Options
The scheduled operations will be created for the selected objects listed below: HMC Select the date and time, and select a time window. The scheduled operation will start during the time window that begins at the scheduled date and time. Date $* \frac{01/07/07}{100000000000000000000000000000000000$
Save Cancel Help

Figure 11-4 Set up a Scheduled Operation

4. On the Repeat tab, select the repeat options for the backup (Figure 11-5).

Set up a Scheduled Opera	ation
Date and Time Repeat Op	tions
The scheduled operations objects listed below: HMC	will be created for the selected
<ul> <li>Single or Repeated</li> <li>○ Set up a single schedu</li> <li>⊙ Set up a repeated sche</li> </ul>	led operation duled operation
Days of the Week Monday  Friday Tuesday □ Saturday Wednesday Sunday Thursday	Options Interval 1 1 to 26 Weeks Repetitions 1 1 to 100 Repeat indefinitely
Save Cancel Help	

Figure 11-5 Scheduled CCD Repeat Option

5. On the Options tab, select the options available to backup media (Figure 11-6). The most common option is Local DVD Media.

Set up a Scheduled Operation
Date and Time Repeat Options
Backup critical data to : <ul> <li>Local DVD</li> <li>Remote mounted file system</li> <li>Remote FTP server</li> </ul>

Figure 11-6 Scheduled CCD Options

- 6. After setting all the options, select Save. Then, select OK.
- After you have saved the scheduled operations, you can view the operations by selecting HMC management → Schedule Operations. Select the CCD scheduled operation and then select View.

## **11.2 Restoring Critical Console Data**

There are different ways of restoring CCD, depending on the option that you use to back up the data. This section describes these options.

#### 11.2.1 Restoring data from DVD

You restore Critical Console Data from the menu displayed at the end of the HMC reinstallation. To restore from DVD, you need to insert the DVD that contains the archived console data. On the first boot of the newly installed HMC, the data is restored automatically.

# 11.2.2 Restoring data that was archived to a remote FTP or NFS server

If the critical console data was archived remotely either on a FTP server or remote file system, you need to:

- 1. Manually reconfigure network settings to enable access to the remote server after the HMC is installed. For information about configuring network settings, refer to Chapter 6, "Network configuration and the HMC" on page 195.
- 2. In the HMC workplace window, select **HMC Management**  $\rightarrow$  **Restore HMC Data**. Then, select the type of restoration and click **Next**.
- 3. Follow the directions to restore the CCD. The data restores automatically from the remote server when the system reboots.

Hardware Manageme	nt Console	
Format Media Update Restore HMC	Data	
□ Welcom e □ û i System s Managem ent	HMC Management ( <u>HMC Version</u> )	
🗄 📳 Servers	Operations	
🖽 🗗 Custom Groups	View HMC Events	
System Plans	Shut Down or Restart	
HMC Management	Schedule Operations	
ໍ່ມີ Service Management 🕄 Updates	Format Media Back up HMC Data Restore HMC Data	
You selected to rest Management Conso archive repository ar <i>Remote repository of</i> <i>Restore from ref</i> <i>Restore from ref</i>	tore backup critical data for this Hardware ble (HMC) from a remote source. Select the nd click Next.	
Next Cancel Hel	p	~
ど Done		.::

Figure 11-7 Remote restore

# 11.3 HMC firmware maintenance

The HMC is completely independent from the server. The server and all partitions can remain active while maintenance is performed on the HMC, allowing you to easily keep your HMC at the latest maintenance level.

The HMC software level has to be maintained same as managed system firmware. HMC firmware is packaged as a full Recovery CD set or as a Corrective Service pack/fix image. The HMC recovery CDs are bootable images and can be used to perform a complete recovery of the HMC (scratch install) or an update to an existing HMC version. A corrective fix updates the minor version level of code on the HMC. The HMC update packages are available on CDs or as downloadable, compressed files. The downloadable, compressed files have different naming formats depending on whether they are individual fixes or complete update packages:

MHxxxxx.zip - individual HMC fixes

Where xxxxx is the HMC fix number

HMC\_Update\_VxRyMz\_n.zip - HMC update packages

Where x is the version number, y is the release number, z is the modification number, and n is the image number (if there are multiple images)

#### 11.3.1 How to determine the HMC software version

The level of machine code on the HMC determines the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

To determine the HMC software version, click **Updates** in the HMC workplace window. In the Work area, view and record the information that displays under the HMC Code Level heading, including the HMC version, release, maintenance level, build level, and base versions. See Figure 11-8.

⊟ Welcom e ⊞ ©ii System s Managem en t	Updates HMC Code Level					
Ib System Plans HMC Management 않 Service Management 안 Updates	Version: 7 Release: 3.1.0 Service Pack: 0 Update HMC System Code Levels	Build Level: 20070403.1 Base Version: V7R3.1.0	Ser Mo BIC	rial Number: 10 del Type: 7310 SS: 2AKT38RU:	0362EA C03 S	
	00 **	\$ 2 P B	Tasks ▼			
	Select ^ Name	^	Status ^	Platform ^ IPL Level ^	Activated 、 Level	EC Number
	9117-	MMA-SN10DD4AC-L10	💧 Standby	26	26	01EM310
	9117-	MMA-SN10FFE0B-L9	💧 Standby	26	26	01EM310
		Total: 2 Filtered: 2 S	elected: 0			

Figure 11-8 Shows the Version number of HMC and Managed Systems

#### 11.3.2 Which firmware or fix level is correct for your system

One of the most important tasks is to determine the correct level of firmware or fix level for your system. IBM has an online tool called the *Fix Level Recommendation Tool*. The Fix Level Recommendation Tool assists system administrators in formulating a maintenance plan for IBM System p servers.

For each hardware model that you select, the tool displays fix level information in a report for the following components:

- ► HMC
- System Firmware (SF)
- ► AIX 5L
- Virtual I/O server (VIOS)
- High Availability Cluster Multi-processing (HACMP)
- ► General Parallel File System<sup>™</sup> (GPFS)
- Cluster Systems Management (CSM)
- CSM Highly Available Management Server (CSM-HA)

To connect to the Fix Level Recommendation Tool, go to the following URL:

https://www14.software.ibm.com/webapp/set2/flrt/home

Fix Level Recommendation Tool	Fix Level Recommendation Tool
Feedback	for AIX administrators
Fix download sites	Fix Level Recommendation Tool is a planning tool to help administrators determine what key components of your System p server are at the minimum recommended fix level.
<ul> <li>System firmware</li> <li>HMC</li> <li>Virtual I/O Server</li> <li>Cluster Software</li> </ul>	Recommendations are provided for the system firmware, operating system, hardware management console, virtual I/O server and Cluster software.
Related links	If you are looking for base support level information on adapters, drives or media devices, go to $\underline{\sf IBM \ Prerequisites}$ for Power5.
best practices	
<ul> <li>Subscription services</li> </ul>	Produce a fix level recommendation report
	Select one or more products
	AIX AIX
	System firmware
	✓ Hardware Management Console
	Virtual I/O Server
	High Availability Cluster Multi-processing
	General Parallel File System
	Cluster Systems Management
	CSM Highly Available Management Server
	Submit

Figure 11-9 shows the Fix Level Recommendation Tool Web site main page.

Figure 11-9 Fix Level Recommendation Tool Web site

Only the products that you select on the Fix Level Recommendation Tool entry page are listed on the *inventory page*. The Fix Level Recommendation Tool is most useful for querying the combination of two or more products to ensure that they are at the recommended level and that any interdependencies are met. For example, specific system firmware levels are required for some HMC releases, and VIOS only virtualizes a system with AIX 5L Version 5.3 and higher.

The report that the Fix Level Recommendation Tool produces includes two sections:

- Your selected level
- ► The recommended minimum fix level

To run a report:

 On the Fix Level Recommendation Tool main page, select the products for which you want to check recommended levels and click **Submit**. The Fix Level Recommendation Tool displays the information shown in Figure 11-10.

Fix Level Recommendation Tool	Fix Level Recommendation Tool
Feedback	
	In order for this tool to make recommendations, we need to know the
• AIX • System firmware	versions of software/hardware products currently on your machine. The fields indicated with an asterisk (*) are required.
HMC     Virtual I/O Server     Cluster Software	Produce a recommended minimum report
Related links	1 Specify a name for your report (Optional) Specify a hostname or any value
Service and support best practices     Subscription services	LocalHost
	2 * Select a machine type and model
	3 Enter product levels
	* AIX 5300-05-05
	* System Firmware SF240_219
	* HMC 6.1 🔽
	* VIOS 1.2.1.4 🗸
	4 Create a report
	🕒 Submit

*Figure 11-10 Fix Level Recommendation Tool product options window* 

2. Enter the current details from your system. To find the current fix level of HMC and managed system, refer to 11.3.1, "How to determine the HMC software version" on page 311. Select **Submit**.

The Fix Level Recommendation Tool displays the report, as shown in Figure 11-11.

Fix Level Recommendation Tool Feedback	Fix Level Re for AIX administrato	ecommendation Tool	
Fix download sites • AIX • System firmware • HMC • Virtual I/O Server • Cluster Software	Report: The following consolidi information was obtain documentation. These Model: IBM System	LocalHost ated information is for guidance purposes only. This ned from generally available product support combinations of product levels are supported by IBM. p5 570 with 1.9 GHz	Print this page
Related links • Service and support best practices • Subscription services	Your selected leve Product AIX System firmware HMC Virtual I/O Server	Is Version/Release AIX 5L Service Pack 5300-05-05 System Firmware 240_219 HMC 6.1 Virtual I/O Server Release 1.2.1.4	Status
	Recommended min Product System firmware HMC Virtual I/O Server * Recommendations d	imum fix levels Recommended minimum fix levels System Firmware 240_284 HMC PTF MH00839 Virtual I/O Server Release 1.3.0.0 atabase last updated 2007.03.12	

Figure 11-11 Fix Level Recommendation Tool recommendation window

#### Your selected levels

The report includes information on *Your selected levels*. This information includes the current levels that you entered on the inventory page. This section of the report lists the current levels and displays a check mark if your current level is already at a recommended level. A warning icon displays if the Fix Level Recommendation Tool finds a recommendation for a specific product.

#### **Recommended minimum fix levels**

The report also includes information on *Recommended minimum fix levels*. This information includes the levels that include the latest updates. When you decide what upgrade path to take, links on left side of the page take you to the download location for that firmware or software package.

Look for the check marks in the report. The check marks indicate that the fix level is at the current level under your selected levels. The warning icon indicates that the installed fix level is at a lower level than recommended level. Then, look at the recommended minimum fix levels on the window for the latest fix level available. To download and apply the fixes, refer to Chapter 11, "Firmware maintenance" on page 303.

#### 11.3.3 Obtaining HMC updates and recovery software

You can order Recovery CDs or download packages that contain the files that you need to burn your own Recovery CD. The files that you use to create CDs have a .iso file extension. The CDs created from these packages are bootable. You can download updates to HMC code as well as emergency fixes, and you can order CDs containing the updates and fixes. The CDs containing updates and fixes are *not* bootable.

**Important:** If you are not sure what code level is correct for your machine, then read 11.3.2, "Which firmware or fix level is correct for your system" on page 312.

Use the following URL to download the latest HMC software (Figure 11-12):



http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html

Figure 11-12 Displays the HMC software that is available on the Web site

Select the version of the software that you want to download (Figure 11-13).

Download files via Download	Director				→ System i su	pport
Use Download Director to downloa	ad multiple im	ages simult	taneously.		→ System p si	upport
Download ZIP files for HMC 6.	1.2 Update pa	ackage				
▲ Download ISO files for HMC 6	.1.2 Update p	ackage			for Systems	i and p
Download individual files					Subscription s	ervices
Download individual files from the	following tab	le.			Sign up for en notification of	nail :
The <b>View</b> link provides important installed updates and fixes.	information u	sed to insta	all and verif	ý	→ System i to	pics
Click the <b>Go</b> link to order a packa	ae on CD-RO	м.			→ System p to	pics
Please note that CD-ROMs for	fixes are NC	)T bootabl	e.	_		
File name(s)/Package	Checksum*	APAR#	PTF#	Readme	Date	Order CD
Update packages						
HMC_Update_V6R1.2_1.zip HMC_Update_V6R1.2_2.zip HMC_Update_V6R1.2_3.zip	21967 41469 57832	MB01930	MH00915	View	2007.02.23	<u>Go</u>
HMC_Update_V6R1.2_1.iso HMC_Update_V6R1.2_2.iso HMC_Update_V6R1.2_3.iso Updates HMC V6R1.0 to 6.1.2	13669 30504 16487					
Specific fixes						
MH00971.zip MH00971.iso Fix Virtual Ethernet MAC address change after upgrade	57995 28645	MH00971	MB02018	View	2007.03.29	<u>Go</u>
MH00946.zip MH00946.iso ONLY for System p cluster servers with Cluster Ready Hardware Server on the HMC	03644 39523	MH00946	MB02086	View	2007.03.06	<u>Go</u>

Figure 11-13 HMC software and update files available on IBM Web site

Save the file on your computer and burn it on a DVD or order a CD from IBM as shown in Figure 11-14.

**Note:** To order a DVD, you will need an IBM ID. Select **IBM ID** and follow the instruction to register. After you have registered, log in to the Web site and complete the necessary information.

File name(s)/Package	Checksum*	APAR#	PTF#	Readme	Date	Order CD
Update packages						
HMC_Update_V6R1.2_1.zip HMC_Update_V6R1.2_2.zip HMC_Update_V6R1.2_3.zip	21967 41469 57832	MB01930	MH00915	View	2007.02.23	<u>Go</u>
HMC_Update_V6R1.2_1.iso HMC_Update_V6R1.2_2.iso HMC_Update_V6R1.2_3.iso Updates HMC V6R1.0 to 6.1.2	13669 30504 16487					
Specific fixes						
MH00971.zip MH00971.iso Fix Virtual Ethernet MAC address change after upgrade	57995 28645	MH00971	MB02018	View	2007.03.29	<u>Go</u>

Figure 11-14 Ordering HMC code CD

#### 11.3.4 Obtaining and applying HMC code from an FTP server

If your HMC has a VPN connection to the Internet, you might choose to perform the HMC update directly from the IBM support FTP server.

**Important:** Some of the HMC update packages are large (over 2 GB) and can take time to download.

To perform the HMC update directly from an FTP server:

1. First, back up Critical Console Data as described in 11.1, "Critical Console Data backup" on page 304.

 Then, in the HMC workplace window, click Updates → Update HMC. The Install Corrective Service window opens (Figure 11-15).

To update the system software on your HMC, select one of the following actions: <ul> <li>Apply corrective service from removable media (CD/DVD)</li> <li>Download the corrective service file from a remote system, then apply. Remote site: </li> </ul>
Remote site: * ftp.software.ibm.com
ftp.software.ibm.com
Patch file:
* /software/server/hmc/fixes/XX.zip
User ID:
anonymous Password
*
<b>Note:</b> Do not initiate additional tasks during corrective service installation. To apply the changes, you may need to reboot the HMC after installation completes.

Figure 11-15 Install Corrective Service window

- 3. Select **Download the corrective service file from a remote system, and then apply**, and enter the following information:
  - **Remote site:** ftp.software.ibm.com
  - Patch file: /software/server/hmc/fixes/filename.zip

**Note:** The name of the patch file changes with each new update. Refer to 11.3.2, "Which firmware or fix level is correct for your system" on page 312.

- User ID: anonymous
- Password: Your e-mail address
- 4. Click OK.
- 5. Follow the instructions to install the update.
- 6. Shut down and restart the HMC for the update to take effect.

#### 11.3.5 Applying HMC code from CD or DVD

To apply HMC code from a CD or DVD, follow these steps:

- 1. You can either order a DVD with HMC updates from IBM or download .iso or a compressed file from the IBM software support site. For more information, see to11.3.3, "Obtaining HMC updates and recovery software" on page 316.
- 2. Insert the CD or DVD in the HMC.
- In the HMC workplace window, click Updates → Update HMC. The Install Corrective Service window opens (Figure 11-15 on page 319).
- 4. Select Apply corrective service from removable media (CD\DVD) and click OK.
- 5. Follow the instructions to install the update. If you have more than one CD or DVD, then follow the procedure from step 2 for the second CD or DVD.
- 6. Shut down and restart the HMC for the update to take effect.
- 7. To verify that the HMC machine code update installed successfully, refer to 11.3.1, "How to determine the HMC software version" on page 311.
- 8. If the level of code displayed is not the level that you installed, perform the following steps:
  - a. Retry the machine code update. If you created a CD or DVD for this procedure, use a new media.
  - b. If the problem persists, contact your next level of support.

#### 11.3.6 Upgrading the HMC machine code

**Note:** You cannot use this procedure to upgrade from a POWER4 HMC to a POWER5 HMC. You must do a full installation. To upgrade from Version 6 to Version 7, refer to 11.3.7, "Upgrading HMC from Version 6 to Version 7" on page 324.

To upgrade the HMC machine code, follow these steps:

- 1. Determine the HMC machine code level that is required for your system. Refer to 11.3.2, "Which firmware or fix level is correct for your system" on page 312.
- 2. Obtain the recovery CD or DVD. See 11.3.3, "Obtaining HMC updates and recovery software" on page 316.

3. Back up the managed system's profile data. In the HMC workplace window, select **System Management** → **Servers**. Then, select the server and ensure the state is *Operating* or *Standby*.

Under Tasks, select Configuration  $\rightarrow$  Manage Partition Data  $\rightarrow$  Backup. Enter a backup file name and record this information. Then, click OK.

Repeat these steps for each managed system.

4. Backup critical console data as described in 11.1, "Critical Console Data backup" on page 304.

It is absolutely necessary to backup the CCD.

- 5. Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information as follows:
  - a. In the HMC workplace window, select **HMC Management**. Then, in the tasks list, select **Schedule Operations**. The Scheduled Operations window displays with a list of all managed systems.
  - b. Select the HMC that you plan to upgrade and click **OK**. All scheduled operations for the HMC display.

Note: If you do not have any scheduled operations skip to step 6.

- c. Select  $\textbf{Sort} \rightarrow \textbf{By Object}$ . Select each object and record the following details:
  - Object Name
  - scheduled date
  - Operation Time (displayed in 24-hour format)
  - Repetitive

If Yes, select  $View \rightarrow Schedule Details$ . Then, record the interval information and close the scheduled operations window. Repeat for each scheduled operation.

- d. Close the Customize Scheduled Operations window.
- 6. Record remote command status:
  - a. In the navigation area, select **HMC Management**. Then, in the tasks list, click **Remote Command Execution**.
  - b. Record whether the Enable remote command execution using the **ssh** facility check box is selected.
  - c. Click Cancel.

#### Saving upgrade data

You can save the current HMC configuration in a designated disk partition on the HMC. Only save upgrade data immediately prior to upgrading your HMC software to a new release. This action allows you to restore HMC configuration settings after upgrading.

**Note:** Only one level of backup data is allowed. Each time you save upgrade data, the previous level is overwritten.

HMC Version 7 also gives a option to save upgrade data on DVD media. It is strongly suggested to save a copy on a DVD too. See Figure 11-16.

Save Upgrade Data Wizard				
Save	Save Upgrade Data			
→ <u>Upgrade</u> <u>Data</u> Finish Save Upgrade Data	Select the media on which you want to save upgrade data. If you choose to save to DVD, insert the media in the DVD drive, then select 'Next'. Media: Hard Drive			
	Hard Drive DVD			
< Back Next > Finish Cancel Help				

Figure 11-16 Save Upgrade Data wizard

To save upgrade data:

- 1. In the HMC workplace window, select **HMC Management**. Then, in the tasks list, select **Save Upgrade Data**. Select **Hard Drive** and click **Next**.
- 2. Click Finish.

3. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

**Important:** If the save upgrade data task fails, do not continue the upgrade process.

4. Click OK. Then, click Close.

To upgrade the HMC software:

- 1. Restart the system with Recovery DVD-RAM in the DVD-RAM drive by inserting the HMC RecoveryDVD-RAM into the DVD-RAM drive.
- 2. In the navigation area, select HMC Management  $\rightarrow$  Shutdown or Restart.Then, select Restart the HMC and click OK.
- 3. The HMC restarts and boots from the bootable recovery DVD. The window shows the following option:
  - Install
  - Upgrade

Select Upgrade and click Next.

- 4. When the warning displays, choose from the following options:
  - If you have saved upgrade data during the previous task, continue with the next step.
  - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue.
- 5. Select **Upgrade** from media and click **Next**. Confirm the settings and click **Finish**.
- 6. Follow the prompts as they display.

**Note:** If the window goes blank, press the space bar to view the information. The first DVD can take approximately 20 minutes to install.

- 7. Select option **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC displays status messages as it installs the packages.
- 8. When the second media installation is complete, remove the media from the drive and close the media drawer.
- 9. Select option **2. Finish the installation** and press Enter. The HMC completes the booting process.

10.At the login prompt, log in using your user ID and password.

- 11. Accept the License Agreement for Machine Code twice. The HMC code installation is complete.
- 12. Verify that the HMC machine code upgrade installed successfully. Refer to 11.3.1, "How to determine the HMC software version" on page 311.

You have completed upgrading the HMC machine code procedure.

#### 11.3.7 Upgrading HMC from Version 6 to Version 7

This section shows you how to upgrade your HMC Version 6 to HMC Version 7 while maintaining your configuration data.

**Important:** You must be at a minimum of Version 6 to upgrade to the POWER6 HMC machine code level which is Version 7 Release 4.

To upgrade from Version 6 to Version 7, follow these steps:

- 1. Determine the HMC machine code level that is required for your system. Refer to 11.3.2, "Which firmware or fix level is correct for your system" on page 312.
- 2. Obtain the recovery CD or DVD as described in 11.3.3, "Obtaining HMC updates and recovery software" on page 316.
- 3. Back up the managed system's profile data. In the HMC workplace window, select **System Management** → **Servers**. Select the server and ensure the state is *Operating* or *Standby*.

Under Tasks, select Configuration  $\rightarrow$  Manage Partition Data  $\rightarrow$  Backup. Enter a backup file name and record this information. Then, click OK.

Repeat these steps for each managed system.

4. Backup Critical Console Data as described in 11.1, "Critical Console Data backup" on page 304.

It is absolutely necessary to backup the CCD.

- 5. Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information as follows:
  - a. In the Navigation area, select **HMC Management**. Then, in the tasks list, select **Schedule Operations**. The Scheduled Operations window displays with a list of all managed systems.
  - b. Select the HMC that you plan to upgrade and click **OK**. All scheduled operations for the HMC display.

Note: If you do not have any scheduled operations skip to step 6.

- c. Select Sort  $\rightarrow$  By Object.
- d. Select each object and record the following details:
  - Object Name
  - scheduled date
  - Operation Time (displayed in 24-hour format)
  - Repetitive

If Yes, select View  $\rightarrow$  Schedule Details. Then, record the interval information. Close the scheduled operations window. Repeat for each scheduled operation.

- e. Close the Customize Scheduled Operations window.
- 6. Record remote command status:
  - a. In the navigation area, select **HMC Management**. Then, in the tasks list click **Remote Command Execution**.
  - b. Record whether the Enable remote command execution using the **ssh** facility check box is selected.
  - c. Click Cancel.
- 7. Save the upgrade data as described in "Saving upgrade data" on page 322.

**Important:** If this step is not followed properly, you will lose all your partition information.

8. Upgrade the HMC Software from Version 6 to Version 7.

**Note:** You can only upgrade your HMC from Version 6 to Version 7. If you have an HMC Version 6, you need to upgrade it to Version 6 first. You need a to have a recovery DVD from step 2 in this procedure.

- a. Insert the Version 7 recovery DVD in the DVD drive.
- b. In the navigation area, select HMC Management  $\rightarrow$  Shutdown or Restart. Then, select Restart the HMC and click OK.
- c. The HMC restarts and boots from the bootable recovery DVD. The window shows the following options:
  - Install
  - Upgrade

- d. Select Upgrade and click Next.
- e. When the warning displays, choose from the following options:
  - If you have saved upgrade data during the previous task, continue with the next step.
  - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue. Refer to previous step.
- f. Select **Upgrade** from media and click **Next**. Confirm the settings and click **Finish**. Follow the prompts as they display.

**Note:** If the window goes blank, press the space bar to view the information. The first DVD can take approximately 20 minutes to install.

- g. Select option **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC displays status messages as it installs the packages. When the second media installation is complete, remove the media from the drive and close the media drawer.
- h. Select Option **2. Finish the installation** and press Enter. The HMC completes the booting process.
- i. At the login prompt, log in using your user ID and password.
- j. Accept the License Agreement for Machine Code twice. The HMC code installation is complete.
- k. Verify that the HMC machine code upgrade installed successfully. Refer to 11.3.1, "How to determine the HMC software version" on page 311.

## 11.4 Managed system firmware updates

In this section, we discuss different options that are available to install system firmware. The system firmware is also referred to as *licensed internal code*. It resides on the service processor.

**Important:** The HMC machine code needs to be equal to or greater than the managed system firmware level. Also, if an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level.

#### 11.4.1 Firmware overview

Depending on your system model and service environment, you can download, install, and manage your server firmware updates using different methods. The default firmware update policy for a partitioned system is through the HMC. If you do not have HMC attached to your system, refer to your operating system documentation to upload the code using the operating system.

System firmware is delivered as a *Release Level* or a *Service Pack*. Release Levels support the general availability (GA) of new function or features and new machine types or models. Upgrading to a higher Release Level can be disruptive to customer operations. Thus, IBM intends to introduce no more than two new Release Levels per year. These Release Levels are supported by Service Packs. Service Packs are intended to contain only firmware fixes and are not intended to introduce new functionality. A Service Pack is an update to an existing Release Level.

**Note:** Installing a Release Level is also referred to as *upgrading* your firmware. Installing a Service Pack is referred to as *updating* your firmware

The file naming convention for System Firmware is as follows:

► POWER5

01SF*xxx\_yyy\_zzz* 

where

- xxx is the release level
- yyy is the service pack level
- zzz is the last disruptive service pack level

So, for example, System Firmware 01SF240\_320, as displayed on the Firmware Download page, is Release Level 240, Service Pack 320.

► POWER6

EM*xxx\_yyy\_zzz* 

where

- xxx is the release level
- yyy is the service pack level
- zzz is the last disruptive service pack level

So, for example, System Firmware 01EM310\_026, as displayed on the Firmware Download page, is Release Level 310, Service Pack 026.

The Service Pack maintains two copies of the server firmware. One copy is held in the t-side repository (temporary) and the other copy is held in the p-side repository (permanent):

Temporary side: New firmware updates should be applied to the t-side first and should be tested before they are permanently applied. When you install server firmware updates on the t-side, the existing contents of the t-side should be permanently installed on the p-side first.

We recommend that under normal operations the managed system run on the t-side version of the system firmware.

Permanent side: The permanent side holds the last firmware release that was running on the temporary side. You know that this firmware has been running for a while on the temporary side and is stable. This is also a good way to hold a back up firmware on the system. If for any reason your temporary firmware gets corrupted, you can boot from the permanent side and recover your system.

Before you update your system firmware, move current firmware that is on the temporary side to the permanent side.

We recommend that under normal operations the managed system runs on the t-side version of the system firmware.

When you install changes to your firmware, you have three options:

- Concurrent install and activate: Fixes can be applied without interrupting running partitions and restarting managed system.
- **Concurrent install with deferred disruptive activate:** Fixes can be applied as delayed and activated the next time the managed system is restarted.
- Disruptive install with activate: Fixes can only be applied by turning off the managed system.

You want to choose the option that fits the status of the server that you are updating. For example, you do not want to use a disruptive installation option on a production server. However, on a test server, this option might not be an issue.

#### 11.4.2 Obtaining system firmware

This section describes how to view or to download the firmware fix. Download the fix to your computer with an Internet connection and then create a fix CD that you apply on the server. If necessary, contact service and support to order the fix on CD.

You can download fixes from the following URL (Figure 11-17):

http://www14.software.ibm.com/webapp/set2/firmware/gjsn

Microcode downloads Feedback	Microcode downloads
	Download system firmware, adapter, disk and media microcode for IBM System p, eServer p5, eServer pSeries, eServer OpenPower and RS/6000 servers.
	Firmware and microcode
	Select from one of the following options:
	<ol> <li>Download microcode by machine type and model Includes system firmware, adapters, disks, media devices and other applicable to the MTM you select.</li> </ol>
	9117-570 💌 😡
	2) Download microcode by device type
	Select one 🔽 💿
	3) Search by feature code
	enter code 60
	4) Obtain ISO image for CD use Includes all system firmware, adapters, disks, media devices and other updates for all MTMs (image is over S00MB).
	<u>Obtain ISO image</u>

Figure 11-17 Server firmware download site

Decide what version of the firmware is correct for system as described in 11.3.2, "Which firmware or fix level is correct for your system" on page 312. Use the Fix Level Recommendation Tool to decide the level of firmware that you require for your system.

Then, select your machine type and select Go.

Select the version of the system firmware that is applicable to your system and click **Continue** at the bottom of the window (Figure 11-18).

Microcode downloads						
Machine type and model selected: <b>9117-570</b> Select one or more items, then click the "Continue" button at the bottom of the page. This is a list of updates. Adapters or devices that have not been updated will not appear in this list. Select another machine type and model						
System fir	rmware 9117-570					
Packages	Updated / Version	Desc	Impact / Severity			
System Firr	nware SF230_158					
RPM	Updated 09/25/2006 Version SF230_158	🗗 <u>Desc</u>	다 Impact <u>FUNC</u> 다 Severity <u>HIPER</u>			
System Firr	nware SF235_214					
RPM	Updated 01/03/2007 Version SF235_214	🗗 <u>Desc</u>	Impact <u>FUNC</u> Severity <u>SPE</u>			
System Firr	nware SF240_284					
RPM	Updated 11/30/2006 Version SF240_284	🗗 <u>Desc</u>	Impact <u>FUNC</u> Severity <u>HIPER</u>			
System Firr	nware SF240_298					
	Updated 04/05/2007 Version SF240_298	🗗 <u>Desc</u>	🗗 Impact <u>NA</u> 🗗 Severity <u>NA</u>			
System Firmware SF240_299						
RPM	Updated 04/05/2007 Version SF240_299	🗗 <u>Desc</u>	Impact <u>AVAIL</u> Severity <u>HIPER</u>			
System Firmware SF240_320						
RPM	Updated 05/14/2007 Version SF240_320	🗗 <u>Desc</u>	Impact <u>AVAIL</u> Severity <u>HIPER</u>			

Figure 11-18 System firmware selection window

# 12



This chapter describes the Service Management functions on the Hardware Management Console (HMC).

# 12.1 Service Management area of the HMC

The main view of the Service Management area is divided into two sections, as shown in Figure 12-1.

Service Management (HMC Version)	
Create Serviceable Event	Create a serviceable event to report a problem
Manage Serviceable Events	View, report, repair, or close serviceable events
Load Serviceable Events	* Load or reload serviceable events from an XML file
Manage Remote Connections	View, prioritize, hold, or cancel call-home connections
Manage Remote Support Requests	* View or cancel cal⊦home requests submitted by this HMC
Format Media	Format a DVD, diskette, or high speed memory key
Manage Dumps	Copy, call-home, and delete dumps
Transmit Service Information	* Schedule transmissions or offload service information for your service provider
Connectivity	
Manage Systems Call-Home	· Control whether call-home requests may be created for the HMC or a managed system
Manage Outbound Connectivity	Configure call-home connections between the HMC and your service provider
Manage Inbound Connectivity	Initiate temporary access to the HMC or managed systems for your service provider
Manage Customer Information	View and change administrator, system, and account information
Manage eService Registration	Register a customer user ID with the eService Web site
Manage Serviceable Event Notification	Configure information to enable customer notification when serviceable events occur
Manage Connection Monitoring	Configure timers to detect outages and monitor connections for selected machines
Manage POWER4 Service Agent	* Enable and configure Service Agent Connection Manager for POWER4 systems

Figure 12-1 Service Management, main view

The first Service Management section describes the *management tasks* that can be performed on the HMC. These tasks include:

- Handling service events
- Managing remote connections
- Formatting removable media
- Managing service dumps
- Transmitting service data

The second Service Management section covers *connectivity* with the HMC. These tasks include:

- Managing call home (also known as Service Agent)
- Handling outbound connectivity
- Permitting inbound connectivity
- Specifying customer information
- ► Registering eService
- Setting contact information for serviceable events

- Manage connection monitoring
- Handle previous Service Agent connectivity

# 12.2 Management tasks

The options that can be performed in the top half of the service management area mostly pertain to service events, formatting and using removable media, and sending in service reports to IBM. There are also troubleshooting tools available in this area of the HMC that pertain to troubleshooting not only with managed servers but also with the HMC itself.

#### 12.2.1 Service events

There are three options for service events on the HMC:

- Create event
- Manage events
- Load events

#### **Create event**

Select **Create Serviceable Event** to manually report a hardware failure on a managed server or on the HMC itself (as shown in Figure 12-2).

Create Serviceable Event				
To report a problem, enter the problem description. To test automatic problem reporting, select the check box. You may indicate in the problem description that this is only a test.				
Test automatic problem reporting				
Problem Description           Request Service         Cancel         Help				
🔊 Done				

Figure 12-2 Service Management, creating a serviceable event

Under Problem Description, provide as much information as possible about the problem that you encountered, including the hardware involved and references to any error logs or reports associated with the event.

When completed, select **Request Service**. If your connectivity to IBM is set up as properly as described in 12.3.2, "Manage Outbound Connectivity" on page 353, the error report is sent to IBM.

#### Manage events

Select Manage Serviceable Events to open the window shown in Figure 12-3.

Manage Serviceable Events
Use this window to specify selection criteria for the serviceable events you wish to view or manage. Only events that meet all the criteria that you specify will be displayed.
Event criteria Serviceable event status: * Open
Problem number: * ALL
Error criteria Reporting MTMS: * ALL Failing MTMS: * ALL Reference code: * ALL Number of days to view: *
Field-Replaceable Unit (FRU) criteria Part number: * ALL Location code: * ALL
OK Cancel Help
🙋 Done 🛛 👘 🚰 💓 Internet 🥼

Figure 12-3 Service Management, manage serviceable events

Use the pull-down menus to alter the filters to display the current service events recorded on the HMC. When your selections are complete, select **OK**. Then you have a results window similar to Figure 12-4.

Manage Serviceable Events - Serviceable Event Overview							
Selected	•						
This list sh associated © Compa	This list shows all serviceable events that match your selection criteria. Each event is grouped with all errors that are associated with that event. Use the menu bar above to perform actions on the serviceable event.						
	•••••	/ / /	Select Act	tion 💌			
Select ^	Problem # ^	PMH # ^ Re	eference code ^	Status ^	Last reported time	^ Failing MTMS	^
	5	<u>E3</u>	3D4310A	Open	May 16, 2007 6:26:17 P	PM 7310-C03/104EB	CA
	4	E3	3550046	Open	May 16, 2007 6:31:33 P	PM 7310-C03/104EB	CA
	3	#	25C3902	Open	May 16, 2007 3:31:34 P	PM 9133-55A/10D1FA	AG
	2	<u>B3</u>	3100500	Open	May 16, 2007 6:37:53 P	PM 7310-C03/104EB	CA
	1	<u>E3</u>	3550956	Open	May 14, 2007 5:59:17 P	PM 7310-C03/104EB	CA
Total: 5 Filtered: 5 Selected: 0							
View Search Criteria Cancel Help							
ど Done	🗿 Done						

Figure 12-4 Service Management, serviceable event overview

The codes contained in the *Reference code* column are live links. You can select these codes to get further information pertaining to the service event in question. As shown in figure Figure 12-5, by selecting the reference code E3D4310A, a window displays that shows additional information about this service event.

Code Description
E3D4310A
Error occurred during submission of call home request.
User Response
Close
😂 Done 🛛 👘 👘 🖉 Internet

Figure 12-5 Service Management, event description

Similarly, as shown in Figure 12-6, you can select a service event, and then click **Selected** to choose one of the following menu options:

- ► View Details: Get reference details on service event
- Repair: Connect to ResourceLink to attempt to fix the problem associate with the service event
- ► Call Home: Manually report the service event to IBM
- Manage Problem Data: Send specific files associated with a service event to IBM or offload data to removable storage
- Close Event: Remove the service event from the list

Selecte	d 🔻	_					
View D	etails						
Repair		le events	that match your sel	ection crite	ria. Each event is grouped	with all errors that a	re
Call Ho	me r	Use the m	ienu bar abové to p	errorm acti	ons on the serviceable eve	nt.	
Manage	e Problem Data	Full table	view				
Close F	vent						
			Select Act	ion 💌			
Select ^	Problem # ^ I	PMH # ^	Reference code ^	Status ^	Last reported time ^	Failing MTMS	~
	5		E3D4310A	Open	May 16, 2007 6:26:17 PM	7310-C03/104EBCA	
	4		E3550046	Open	May 16, 2007 6:31:33 PM	7310-C03/104EBCA	
	3		#25C3902	Open	May 16, 2007 3:31:34 PM	9133-55A/10D1FAG	
	2		<u>B3100500</u>	Open	May 16, 2007 6:37:53 PM	7310-C03/104EBCA	
	1		<u>E3550956</u>	Open	May 14, 2007 5:59:17 PM	7310-C03/104EBCA	
		Total:	5 Filtered: 5	Selected	d: 1		
View 5	View Search Criteria Cancel Help						

Figure 12-6 Service Management, reporting options

71

By having a service event selected and clicking **View Details**, a window opens as shown in Figure 12-7.

Manage Serviceable Even	ts - Serviceable Event Deta	ils		
The upper table shows detaile associated with this event. Sel Serviceable event detailed att	d information about the selecte ect a FRU and use the "Selected ributes:	ed serviceable event. The lower t d FRU" pulldown to display more	able shows the FRUs information.	
Field Name	Value			
Problem number	5		<b></b>	
Reference code	E3D4310A			
Reference code extension	0000611A			
System reference code	E3D4310A			
Status	Open			
First reported time	May 16, 2007 6:26:17 PM	2007 6:26:17 PM		
Last reported time	May 16, 2007 6:26:17 PM			
Primary data event timestamp	May 16, 2007 6:26:17 PM			
Failing HMC MTMS	7310-C03/104EBCA			
Serviceable event text	Licensed internal code has det	tected a problem.	▼	
FRUs associated with this serv	iceable event:			
Select Part number Class	FRU description Lo	cation code Previously replace	d Replaced timestamp	
O HMCLIC Symbolic	procedure	No		
Cancel Help				
e Done			🔒 🎯 Internet 🛛 🏼 🏾 🎽	

Figure 12-7 Service Management, view details on service event

In this view, you can see the SRC extensions that are associated with the service event that you selected, as well as take actions associated with the hardware by clicking **Selected FRU** or **Actions**.

You can return to the Serviceable Event Overview window by closing the window.

You can select a service event and then select **Repair** to begin repair actions associated with the service event, as shown in Figure 12-8.

PBCommonInfoCenterRepairSupport
Use the instructions located in ResourceLink to repair problem number 5. The Reference Code for this problem is E3D4310A.
Select an action © Connect to ResourceLink © Delay the repair
Next
🙆 Done

Figure 12-8 Service Management, repair action on service event

If you select **Connect to ResourceLink**, you can get help in resolving the service event or you can delay the repair. If you select **Delay the repair**, you are returned to the Serviceable Event Overview window, as shown in Figure 12-4 on page 335.

When you select a service event and clicking **Manage Problem Data**, the window shown in Figure 12-9 opens.

Manage Serviceable Events - Manage Problem Data Select one or more problem data files from the list and select an action to perform on the selected files. Click View to view the contents of a single selected file. View is not enabled when multiple files are selected or when viewing a selected file type that is not supported.						
Select	File hose and in 1 pin					
	File igyvpd.dat in 1.zip		Call Home			
	File actzuict.dat in 1.zip		Offload to Media			
	File iqyvpdc.dat in 1.zip		View			
	File problems.xml in 1.zip					
Cancel Help						
ē)			🔒 🥑 Internet //.			

Figure 12-9 Service Management, manage problem data

You can select specific files that are associated with the service event with the following possible actions:

- ► Send the file to IBM using the Call Home button.
- Save the associated files to removable media through the Offload to Media button.
- Examine the contents of the associated file with the View button.

Finally, if you select a service event and click **Close Event** a window opens as shown in Figure 12-10.

Manage Serviceable Events - Enter Serviceable Event Comments	
Add comments for the serviceable event or events you are	closing.
Your name:	
Issue resolved, I'm closing this event.	
Close Events Cancel Help	
Done	9.3.5.229 🖰

Figure 12-10 Service Management, close a service event

Here, you provide your name and the reason for closing the associated service event.

**Note:** After you perform the Close Event task, all other options except Manage Problem Data are greyed out for the service event in question on the Serviceable Event Overview window.

#### 12.2.2 Remote access

The remote access options of the Service Management area of the HMC allow you to:

- Manage remote connections by manually configuring the serviceable event queue for transmission to IBM.
- Manage remote support requests by managing the local queue of serviceable events on your HMC.

Figure 12-11 shows the remote access options of the Service Management area.

Manage Remote Connections	* Manually manage HMC remote service connections
Manage Remote Support Requests	* View or manage call-home requests that are in-process

Figure 12-11 Service management, remote access options

#### **Manage Remote Connections**

If the HMC's call-home server service is enabled, use the Manage Remote Connections option to manage the console's remote connections manually.

The console manages its remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, you can use the Manage Remote Connections option to manage the queue manually.

Figure 12-12 shows the Manage Remote Connections window.



Figure 12-12 Manage Remote Connections
Use the Options menu to in this window to:

- Stop transmissions
- Move priority requests ahead of others
- Delete requests

## **Manage Remote Support Requests**

You can use the Manage Remote Support Requests option to view or manage Call-Home requests that are submitted by the HMC that are either being processed or that are waiting to be processed.

Figure 12-13 shows the Manage Remote Support Requests window.

Manage Remote Support Requests
Options  Help
The call home requests submitted by this console are shown below. Active Requests Select Status Call Home Server Date Time Description Waiting Requests Select Date Time Description
🛃 Done 🛛 👘 🚰 💓 Internet 🥢

Figure 12-13 Manage Remote Support Requests

Use the Options menu in this window to:

- View All Call-Home Servers
- Cancel Selected Requests
- Cancel All Active Requests
- Cancel All Waiting Requests

## 12.2.3 Managing HMC service data

The HMC service data area of the HMC allows you to:

- Format media for use with various HMC functions
- Manipulate managed server dump information
- Schedule transmittal of VPD, CoD, and serviceable event information about the HMC

Figure 12-14 the HMC data options area of the Service Management area.

Format Media	* Format a DVD, diskette, or high speed memory key
Manage Dumps	* Copy, call-home, and delete dumps for a selected system
Transmit Service Information	<sup>*</sup> Schedule transmissions of service information to IBM

Figure 12-14 Service Management, HMC data options

## Format Media

To format media:

1. Select Format Media. The window shown in Figure 12-15 opens.

Format Media				
Select the desired media format.				
Format DVD-RAM				
○ Format diskette				
C Format high-speed memory key				
OK Cancel Help				
Done 9.3.5.229 💼				

Figure 12-15 Service Management, Format Media

- 2. Select the media device that you want to format, and select OK.
- 3. Then, either insert or attach the appropriate media device to be formatted.

### **Manage Dumps**

Before you can use the Manage Dumps option, you need create a dump from the server view:

1. Select Systems Management → Servers and then select the name of the *server.* Select Serviceability → Hardware → Manage Dumps.

Tasks: p5+-9133-55A-SN10D1FAG
Properties
<ul> <li>Configuration</li> </ul>
<ul> <li>Hardware (Information)</li> </ul>
Updates     Updates
<ul> <li>Serviceability</li> </ul>
Manage Events Create Event Reference Code History Control Panel Functions
Hardware
Manage Dumps Collect VPD Edit MTMS
<ul> <li>Capacity On Dem and (CoD)</li> </ul>

Figure 12-16 Service Management, initiate dump from server

2. In the Manage Dumps window, select Action  $\rightarrow$  Initiate System Dump, as shown in Figure 12-17.

Manage Dur	ps			
Selected <del>-</del>	Action 👻 Status 👻			
Manage Dun	Initiate System Dump Initiate Service Processor Dur Initiate Power Subsystem Dur	тр		
Reporting HM	System Dump Parameters			
dumps that res	de on the reporting HMC	can be ope ump.	erated against.	ia. Only
Select MTMS	Dump Type Problem Nur	nber Date	Size HMC contain	ning dump
,,			Refresh Can	cel Help
avascript:menultemLa	nchAction();			9.3.5.228 🗧

Figure 12-17 Service Management, initiate system dump

3. Specify the system where you want to initiate the dump (Figure 12-18). Verify the selected server, and then select **OK**.



Figure 12-18 Service Management, initiate system dump

4. If there are no errors associated with the system dump, you get a status message as shown in Figure 12-19. Click **OK**.

Anage Dumps	
The dump requested was successfully initiated. The resulting of automatically be offloaded to the HMC. The amount of time required for the offload will vary based on the system configuration. To view this dump, refresh the main screen accordingly.	dump will uired
HS	CS0130
Done	9.3.5.228 🛅

Figure 12-19 Service Management, system dump complete

- 5. Now that there is a dump available for manipulation in Service Management, select **Service Management** → **Manage Dumps**. The system dump displays in the results window as shown in Figure 12-20.
- 6. Select the dump that you would like to manipulate. Then click **Selected**. From this menu, you can:
  - **Copy Dump to Media**: Allows you to move dump information from the HMC to removable media such as a DVD.
  - Copy Dump to Remote System: Allows you to specify a remote FTP server, ID, and password to which to transmit your system dump.
  - Call Home Dump: Sends your system dump data to IBM.
  - **Delete Dump**: Removes dump data from the HMC.

Mana	Manage Dumps							
Select	Selected  Action  Status							
Сору	Dump to Media							
Сору	Dump to Remote System.							
Call F	Home Dump							
F Delet	e Dump		localho	st.localdomain				
be operated against. Click the Action menu to initiate a new dump.								
Select	MTMS	Dump Type	Problem Number	Date	Size	HMC containing dump		
۲	9133-55A/10D1FAG	SYSDUMP	not assigned	May 4, 2007 5:18:32 PM	96.27 MB	localhost.localdomain		
						Refresh Cancel Help		
Done						9.3.5.228 🗎		

Figure 12-20 Service Management, dump results

## **Transmit Service Information**

This area of Service Management is used to transfer service event information from the HMC to IBM. As shown in Figure 12-21, there are three tabs associated with service data transmission.

Transmit Service Information
Transmit       FTP       Transmit Service Data to IBM         You can transmit information to your service provider immediately or you can schedule the transmission.         Service information transmission:         Schedule when to transmit the service information.         Frequency:       7         Time:       * 2:39:23 PM
To transmit the service information immediately, click Send. Send
□ Schedule when to transmit the performance management information.         Frequency:       1         1
To transmit the performance management information immediately, click Send Send.

Figure 12-21 Service Management, transmit

In the Transmit tab, you can:

- Control the frequency of data transmissions to IBM
- Send service data immediately
- Separate schedules for service information and performance management data transmission

**Note:** Schedules of service information and performance management data be different, and you can also send one to IBM without having to send the other.

When you have made your selections for how often the data is to be sent or when you have made an immediate transfer, select **OK**.

The FTP tab allows for control of where to FTP data when it is sent (Figure 12-22). If the HMC is behind a firewall, the FTP tab allows you to specify the proper settings to transmit service data beyond the firewall.

Transmit Servic	ce Information
Transmit FTP	Transmit Service Data to IBM
Provide configu	uration data to allow the use of FTP to offload service information.
FTP Server	
Enable FT	P offload of service information
Name: te	estcase.boulder.ibm.com Port: 21
Directory: //	hardware/toibm/edddata/
User name: a	inonymous
Password: *	
Passive	n 🔽
Host name: User name: Password: Exclusion list Passive:	a - SITE real.host.name USER user PASS password □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
FTP Test/Rese To perform a To reset all y	a test FTP with your FTP settings, click Test. your FTP settings to their original default values, click Reset. OK Cancel Help

Figure 12-22 Service Management, FTP settings

At the bottom of the FTP tab are the options to test the FTP connection and to reset all of the FTP settings to their original defaults.

**Note:** If your system is enabled for a type of CoD that requires monthly reporting, such as that discussed in 13.3.2, "On/Off CoD" on page 378, it is highly recommended that you test your FTP and firewall settings after set up to ensure that your data is in fact getting to IBM.

The Transmit Service Data to IBM tab allows you to choose which specific sets of data to transmit to IBM (Figure 12-23). You can transmit:

- Hardware management console log: The full log of serviceable event data on the HMC.
- Problem determination data: Information that is specific to serviceable events logged by the HMC.
- Managed systems VPD data collection: The full system inventory of managed servers attached to the HMC.

Transmit Service Information	
Transmit FTP Transmit Service Data to IBM	
Select the data you want and the destination for the data. En	A service Data Destination Service Data Destination IBM service support system Problem Management Hardware Number PMH number Output: Engineering Files Virtual RETAIN Files Virtual retain files for problem number: Select Files Number of files selected:
	OK Cancel Help
	[ · · · ·
Done	9.3.5.229 🗎

Figure 12-23 Service Management, specify data to send

# 12.3 Connectivity

To get to the connectivity options, select **Service Management** in the HMC workplace window. The following options are available:

- ► Systems Call-Home: Formerly called *Service Agent*, Call-Home allows the HMC to dial in to the IBM network through a modem or the Internet to report:
  - Serviceable events
  - CoD usage (On/Off, Reserve Capacity, and Utility Capacity)
  - Hardware failures
- Outbound Connectivity: This window allows for configuration of the HMC modem or for configuration of Ethernet connectivity to the outside Ethernet.

- Inbound Connectivity: Allow your service provider temporary access to your HMC or partitions of a managed system.
- Customer Information: Specify administrator, system, and account information.
- eService Registration: Register a customer user ID with the eService Web site.
- Serviceable Event Notification: Define information to enable customer notification when service events occur.
- Connection Monitoring: Configure timers to detect outages and monitor connections for selected computers.
- POWER4 Service Agent: Activate Service Agent Connection Manager for POWER4 systems.

## 12.3.1 Manage Systems Call-Home

To activate regular system status reporting through Call-Home, select **Service Management**  $\rightarrow$  **Manage Systems Call-Home**. Select any systems on which you want to affect Call-Home, and then select either **Enable** or **Disable** (Figure 12-24). Click **OK** to save your selections or click **Cancel** to negate your selections.

Mana	ge Sys	tems Call-Home			
Manage	d Syste	ems Call-Home			
Select	Name	Machine Type-Model/S	SN State		
	HMC	7310-C03/1052DAA	Enabled		
Enable	е		Disable		
OK Ca	ancel	Help			
					-
ど Done				🔒 🥑 Internet	

Figure 12-24 Service Management, enable Call-Home

Along with enabling your HMC or managed servers for Call-Home, you will want to configure and test your outbound connectivity to make sure that your reports can get to IBM. Refer to 12.3.2, "Manage Outbound Connectivity" on page 353 for more information.

## 12.3.2 Manage Outbound Connectivity

You can achieve outbound connectivity either through a modem on the HMC or through Internet connectivity. First, select **Service Management**  $\rightarrow$  **Manage Outbound Connectivity**.

#### Modem configuration

To set your modem configuration:

1. On the Local Modem tab, Allow local modem dialing for service, and then select Modem Configuration (Figure 12-25).

				-
Manage Out	oound Co	nnectivity		
🗹 Enable loca	system a	s a call-home s	erver	
Local Modem	Internet	Internet VPN	Pass-Through Systems	
Allow local	modem di	aling for servic	e	
Modem				
Dial prefix:		Modem C	Configuration	
Select Teleph	nbers (In hone Num	order of use)	TT-	
Select Teleph	ione num	Der Comment	Down.	
	Diama a	Test	Down	
Add Edits	Kemo	ve Test		
OK Cancel H	elp			-
🛃 Done			🔒 🥑 Internet	

Figure 12-25 Manage Outbound Connectivity, Local Modem

2. Set the modem to tone or pulse dialing and set a dial prefix, if required, as shown in Figure 12-26. Then, select **OK**.

Customize Modem Settings
Dial Type © Tone O Pulse
Other Settings Wait for dial tone Enable speaker Dial prefix:
OK Cancel Help
E Internet

Figure 12-26 Modem configuration

## Internet configuration

To configure your HMC for internet configuration:

- 1. Select the Internet tab as shown in Figure 12-27.
- 2. Select **Allow an existing Internet connection for service**. If your HMC is behind a firewall, you need to select **Use SSL proxy** and provide the address and port for your proxy in the address and port fields.
- 3. When e complete, you can test the configuration by clicking **Test**. If the test completes successfully, select **OK** to save your settings.

Manage Out	tbound Co	onnectivity		•
🗹 Enable loc	al system a	s a call-home s	server	
Local Modem	Internet	Internet VPN	Pass-Through Systems	
☑ Allow an e Note: Review configuration	existing Int help inform is necessar	ernet connectio nation to deter y.	on for service mine if any additional fire	ewall
Proxy for Inte Use SSL Address:	proxy	55	Port: * 0	
Authenti User: Password: Confirm password:	cate with th	ne SSL proxy		
Test OK Cancel	Help			
🞒 Done			🔒 🥥 Internet	

Figure 12-27 Manage Outbound Connectivity, Internet access

#### **Internet VPN**

Use the Internet VPN tab, shown in Figure 12-28, to allow the HMC to use a Virtual Private Network (VPN) over an existing internet connection for service. This option is highly recommended if it is available within your IT infrastructure. By using a VPN for remote connectivity you are encrypting the information as it is transmitted from your HMC to IBM. This helps ensure your systems data is kept private and helps keep your HMC secure.

Manage Ou	tbound C al system	onnectivity as a call-home s	erver	
Local Modem	Internet	Internet VPN	Pass-Through Systems	
Allow a V	PN and an	existing Interne	et connection for service	
OK Cancel	Help			- -
Ē			📄 🔮 Internet	

Figure 12-28 Manage Outbound Connectivity, Internet VPN

## **Pass-Through Systems**

Use the Pass-Through Systems tab to allow other managed servers, systems, and other devices on the same network as the HMC to use it as an access point to the external Internet. This is useful if you have set up a VPN connection as described in "Internet VPN" and want to allow all devices that receive a DHCP lease from the HMC to use the HMC as a point of access to the Internet.

It is recommended, though not required, to have separate network adapters on the HMC for a private (the HMC and all managed servers) and open (the HMC, servers, systems, and the external internet) network. By having separate networks for HMC management and internet connectivity you are helping secure the data transferred between the HMC and managed servers. For information about how to set up open and private networks on the HMC, read 6.2.2, "LAN Adapters" on page 198.

Using the Pass-Through Systems option allows for a single network that is both private and open. It is highly recommended that if you allow the HMC as a pass-through point that you also configure a VPN connection on the HMC as shown in "Internet VPN". By having the pass-through point through a VPN, you are encrypting the data and helping keep it secure.

To use the HMC as a pass-through point:

- 1. Select **Allow pass-through systems for service** (Figure 12-29). Until you select this option, you will not be able to allow systems for pass-through nor will you be able to use the Edit, Remove, and Test options until you have added a server.
- 2. To add servers for pass-through service, select Add.

ocal Modem Int	ernet Internet VPN Pass-Through Systems
Allow pass-th	rough systems for service
ass-Through Sy	tems (In order of use)
Select IP Addre	ss or Host Name Comment
	Dawa
	E Sowin
Add Edit	Remove Test
Add Edit	Remove Test
Add Edit	Remove Test
Add Edit iscovered Call-H IP Address or H	Remove Test
Add Edit scovered Call-F IP Address or H 9.3.5.171	Remove Test
Add Edit scovered Call-F IP Address or H 9.3.5.171 9.3.5.228	Remove Test  Test  Test  Tiogrande Iocalhost Iocalhost
Add Edit scovered Call-F IP Address or H 9.3.5.171 9.3.5.228 9.3.5.229	Remove Test  Come Servers  ost Name Comment  riogrande localhost first

Figure 12-29 Manage Outbound Connectivity, Pass-Through Systems

3. In the "IP address or host name" field, enter either the IP address or the fully qualified host name for the server that you want to add, as well as a comment for the server, then select Add, as shown in Figure 12-30.

Add Pass-Through System
Enter the TCP/IP address or host name of the system or partition hosting a modem or VPN. IP address or host name: * 9.3.5.171
Comment: riogrande
Add Cancel Help
🖉 Done

Figure 12-30 Add servers for pass-through access

4. If your selection is successful, you receive a results window similar to that shown in Figure 12-31. The system that you entered is listed in the area labeled Pass-Through Systems.

- 1

Manage Ou	tbound C al system	onnectivity as a call-hom	e server	unh Sustams	
Allow pas	s-through	systems for (In order of	service use)	ugii Systems	
Select IP A	ddress or	Host Name	Comment		Up
• 9.3.5	0.1/1	1	logrande		Down
Add	Edit	Remov	/e	Test	
Discovered C	all-Home	Servers			
IP Address	or Host Na	ame Comme	nt		
9.3.3.231		riograpy			
9.3.5.229		first	IC .		
510101225		in oc			
OK Cancel	Help				]
Done				🔒 🥑 Internet	

Figure 12-31 Add servers for pass-through access, results

5. Now with a server or servers entered for pass-through, you can use the Edit, Remove, and Test options available on this window.

## 12.3.3 Manage Inbound Connectivity

The Manage Inbound Connectivity task allows the HMC to receive a connection from an outside source through the Internet or over modem. First, select **Service Management**  $\rightarrow$  **Manage Inbound Connectivity**.

In the Manage Inbound Connectivity window, you use the Remote Service tab to allow an Internet connection through PPP or VPN (Figure 12-32). Under Connection Type are the access types. You can allow local console and managed server partition access. To save your settings on this tab, select **OK**.

Manag	je Inbou	Ind Connectivity
Remote	e Service	Call Answer
Specify remote	the conr service s	nection type and system access in order to prepare an attended ession.
Connec O PPI	tion Type P addres	e s:
Access All All Manag	ow acces ow acces jed syste	ss to the local console ss to managed system partitions m: 9124-720/10018DA
Partitio	ons: Numbo	r Namo
Select	0	POWER Hypervisor
	8	VIO open
	8192	Service Processor (Primary) 172.16.255.254
Ргера ОК Са	ncel He	lp
Done		lnternet

Figure 12-32 Manage Inbound Connectivity, Remote Service

You use the Call Answer tab to allow a modem that is inside or connected to the HMC to answer incoming calls on the phone line to which it is connected. If you select **Allow local modem call answering** and then select **OK**, then the HMC will answer automatically on the phone line to which it is connected and will negotiate a connection with the other end if it is a modem. See Figure 12-33.

Note: As a general security guideline, you should turn off this option.

You should refrain from activating this setting unless you have approval from your local IT infrastructure's management and administrators. Many IT departments have rules and restrictions governing the use of modems over phone lines in their environment, and allowing the modem on your HMC to answer phone calls might be a security violation in your environment.

Manage Inbound Connectivity	-
Remote Service Call Answer	
Allow local modem call answering	
OK Cancel Help	
E Internet	

Figure 12-33 Manage Inbound Connectivity, Call Answer

## 12.3.4 Manage Customer Information

The Manage Customer Information tasks allows you to enter contact information that pertains to the HMC ownership. On the Administrator tab, you can enter a primary and secondary phone number as well as the owning e-mail address and fax number (Figure 12-34).

Manage Customer Information
Administrator System Account
Contact Information         Company name:         Administrator name:         ibm         Administrator name:         ibm         Email address:         Phone number:         ibm         Alternate phone number:         Fax number:         Alternate fax number:
Mailing Address   Street address:   \$ggg   Street address 2:   City or locality:   *   Country or region:   *   United States (of America)   \$State or province:   *   Alabama   Postal code:   *   ffff
ど Done 🕒 📔 😧 Internet

Figure 12-34 Manage Customer Information

On the System tab, you can enter the postal address at the HMC location (Figure 12-35). This information can be used to send you fixes and patches through mail and also can provide an address for service technicians for when the HMC needs to be serviced.

Manage Customer Information	
Administrator System Account	
System Location	
Use the administrator mailing address	
Street address: * ggg	
Street address 2:	
City or locality: *	
Country or region: *United States (of America)	
State or province: *Alabama	
Postal code: * fffff	
OK Cancel Help	
👌 🚺 Internet	Ī

Figure 12-35 Manage Customer Information, System

Finally, on the Account tab, you enter the fields for the account that owns the HMC (Figure 12-36). If you do not know your customer number, enterprise number, and so forth, contact your sales representative who can provide this information to you.

The information about this window can be useful for IBM representatives to gather inventory and account data associated with your HMC and your enterprise.

Manage Customer Information	
Administrator System Account	
Account Information Customer number: Enterprise number: Sales branch office:	]
Area:	
OK Cancel Help	
🙆 📄 📄 🔮 Internet	

Figure 12-36 Manage Customer Information, Account

## 12.3.5 Manage eService Registration

The Manage eService Registration task allows you to add the HMC and managed servers to your IBM Electronic Services profile. By enabling eService registration you can:

- View the latest IBM Electronic Services news
- Customize the Web page with links that apply to your systems
- View reports that are created from the Electronic Service Agent information that your system sent to IBM
- Submit a service request for hardware and software
- Search for information to solve your system problems
- ► Find services available in your country

Before proceeding with registering your HMC, you first need to visit the following Web site:

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

On this Web site, select Register as shown in Figure 12-37.

**Note:** If you already have an ID, then skip to "Registering eService from the HMC" on page 366.



Figure 12-37 Electronic services Web site

Create an IBM ID as shown in Figure 12-38. When you have completed all the fields on this window, select **Continue**.



Figure 12-38 Electronic services, registration

### **Registering eService from the HMC**

When you have an IBM ID, select **Service Management**  $\rightarrow$  **Manage eService Registration**. Then, follow these steps:

1. Enter the e-mail address that you used to create your IBM ID and then select **OK** (Figure 12-39).

Manage eService Registration
IBM provides personalized Web functions that use information collected by IBM Electronic Service Agent. To use these functions, such as to download fixes directly to your HMC or servre firmware, you must have an e-mail address registered on the IBM Registration website at https://www.ibm.com/account/profile. If you already have an e-mail address at that site, enter it below. Else, create an account profile first.
Now, enter the e-mail address below to associate this system with the IBM Website.
Web authorization e-mail ID 1 * e-mail ID 2 (optional)
You may use the following website to view any or all systems that you have registered to IBM with the account profile above: http://www.ibm.com/support/electronic. OK Cancel Help
🙆 Done

Figure 12-39 Enter e-mail addresses to associate HMC with eService

2. When you have registered your HMC successfully, revisit the Web site:

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

3. Then select **My Systems** as shown in Figure 12-40 to view the servers that are associated with your IBM ID on the Electronic Services Web site.



Figure 12-40 Electronic services registration

## 12.3.6 Manage Serviceable Event Notification

This option allows you to set up e-mail addresses to be contacted for hardware notices or all serviceable events.

To set up e-mail addresses to be contacted for serviceable events, select **Service Management**  $\rightarrow$  **Manage Serviceable Event Notification**. On the Email tab, click Add to enter an e-mail address (Figure 12-41).

Manage Serviceable Event Notification
Email SNMP Trap Configuration
Add the email addresses that will be notified when problem events occur on your system.
Enable email notification for problem events
server:
Email addresses to be notified:
Add Edit Remove Test Emeil
OK Cancel Help
🙆 Done

Figure 12-41 Manage Serviceable Event Notification

You can enter an e-mail address to be contacted and then select to choose to have this e-mail address contacted for either all problem events or just Call-Home hardware events (Figure 12-42). You can enter multiple e-mail addresses one at a time and select **Add**. When you have added all the e-mail addresses that you want contacted for serviceable events, select **Cancel** to close this window and to return to the main HMC view.

Add Email Address	-			
* Email address: * john.doe@nospam.com				
O all-home problem events only				
All problem events	_			
🖉 Done				

Figure 12-42 Add Email Address for notification

## 12.3.7 Manage Connection Monitoring

Connection monitoring generates serviceable events when communication problems are detected between the HMC and managed systems. If you disable connection monitoring, no serviceable events are generated for networking problems between the selected machine and this HMC.

To enable connection monitoring with a managed server, select **Service Management**  $\rightarrow$  **Manage Connection Monitoring**. The Manage Connection Monitoring window opens as shown in Figure 12-43.

Manage Connection Monitoring							
Connection Monitoring Time	er Setting	15					
Number of disconnected m	inutes co	nsidered an o	outage	1	5		
Number of connected minutes considered a recovery							
Number of minutes between outages considered a new incident 20							
Select one or more machine	s. Then o	lick Enable o	r Disable	to enable	or disable		
customer notification of connection monitoring errors from this HMC to the selected							
machines. Enabling this capability allows connection monitoring errors to be							
Agent to handle those notifi	cations.	on. However,	, you mus	st suir con	ligure service		
Select Machine Name	State	Machine Tvr	pe-Mode	/SN			
720 Tuning TEAM04	Enabled	9124-720/10	0018DA				
				En	able Disable		
				- Lin	Disable		
OK Cancel Help							
🛃 Done				🔒 🎯 Inte	emet //		

Figure 12-43 Manage cOnnection Monitoring

Here, you can manipulate:

- Number of disconnected minutes considered an outage: Set the number of minutes of disconnect that are considered an outage. If connectivity is restored before this threshold is met, the managed server is considered recovered and no serviceable event is reported.
- Number of connected minutes considered a recovery: Specify the number of minutes of required connectivity required to put a managed server in a recovered state. This is directly associated with the disconnected minutes threshold, in that this value is monitored when the outage threshold is met.
- Number of minutes between outages considered a new incident: Specify the amount of time required between outages required to report a new outage report

Select the managed server that you want and then select either **Enable** or **Disable** to manipulate connection monitoring. To save your settings, select OK.

## 12.3.8 Manage POWER4 Service Agent

If your IT environment has POWER4 servers attached to an HMC, you can use the Manage POWER4 Service Agent option to have your V7 HMC act as a focal point for Service Agent reporting.

To use this option, select **Service Management**  $\rightarrow$  **Manage POWER4 Service Agent**. Then, in the window that opens, select **Enable Service Agent Connection Manager** as shown in Figure 12-44.

Next, you can manipulate settings for:

- Secure Mode: If cleared, data transmission is unencrypted. If selected, then data between the HMC and the POWER4 HMC is encrypted through the HTTPS protocol.
- URL for configuration download
- Password for configuration updates: It is highly recommended that you change the password from its default value for security purposes.

When you have finished with your selections, select OK.

Manage Power4 Service Agent	
The Service Agent Connection Manager service provides a communications path by which IBM POWER4 Service Agent clients and HMCs can call home their Performance and Vital Product Data, report problems or download updates using the connectivity features of this HMC.	
Enable Service Agent Connection Manager Port: * 1198	
☑ Use Secure Mode (HTTPS)	
Change URL for Configuration Download URL: https://www-306.ibm.com:443/support/electronic/its	
Change Password for Configuration Update Password: password password	
OK Cancel Help	•
🔄 Done	

Figure 12-44 Manage POWER4 Service Agent

# 13



This chapter discusses the various types of Capacity on Demand (CoD), how to acquire enablement and activation codes, and finally how to enter these enablement and activation codes on your HMC to gain the benefits of the various CoD types.

# 13.1 Advantages of CoD

CoD provides several advantages to IBM customers:

Customers can plan for later expansion.

An IBM customer can order a POWER5 or POWER6 16-way system now with 8-way active and then can scale their system performance granularity to a 16-way without CE intervention or additional hardware installation.

Similarly, customers can order a 590 or 595 with 256 GB of system memory and 128 GB active, and then can bring up their memory capacity without additional hardware installation.

Customers can work around budget constraints by taking advantage of CoD.

A customer might want a 16-way 570 now but can only afford an 8-way within the current budget. In this scenario, the customer could buy the 16-way with 8-way active, and then when the budget allows, the customer can activate the additional processors without having to order additional hardware, schedule a CE, and so forth.

Customers can plan for emergencies and system outages.

CoD resources can be turned on or off on the fly to cover for system outages or emergency business needs. The Capacity BackUp (along with HACMP/XD) offering can be set up to have a full system in reserve in the event of an outage.

 Customers can plan for scaled usage or billing of POWER5 and POWER6 servers.

Customers can use On/Off CoD, Reserve Capacity, or Utility Capacity to have resources in reserve and can save money on servers by paying just for what they use.

**Note:** Reserve Capacity is available on POWER5 systems that support CoD functions. Utility Capacity is available on POWER6 systems that support CoD.

Customers can take advantage of increased RAS (reliability, availability, serviceability).

By delivering resources for later activation, customers can activate additional system horsepower without any system downtime or interruption. Processor sparing allows for inactive processors to be activated on the fly in the event of a processor failure. Processor sparing incurs no activation charge to the customer.

In addition to these advantage, the latest version of the HMC code introduces a new type of CoD which we discuss in detail in 13.3.4, "Utility CoD" on page 383.

Furthermore, there have been some enhancements and changes to the CoD Web site, as well as changes to the HMC interface in how to activate and enable the various CoD types.

## 13.2 Permanent types of CoD

Permanent types of CoD are permanent activations of inactive resources. On some models, all system resources are turned on by default, but on some larger scale POWER systems, resources (processors and sometimes memory) can be delivered inactive. For these inactive resources, permanent activations can be purchased either on initial order or through an upgrade. The types of permanent activation for these resources are:

- Capacity Upgrade on Demand (CUoD)
- Mobile CoD

## 13.2.1 Capacity Upgrade on Demand

CUoD references acquiring full processor or memory activations for inactive CoD resources. CUoD allows for customers to plan for later expansion with their POWER servers, and allows for flexibility with system pricing. By purchasing systems with inactive resources customers can get around budget constraints, or have resources in reserve for increased demand later in their server ownership.

#### 13.2.2 Mobile CoD

Mobile CoD is the ability to move, at no charge, resource (processor *and* memory) activations between systems with the same system type, and it is currently handled by the CoD Project Office at pcod@us.ibm.com.

#### **Guidelines for Mobile CoD**

Movement of activations can only be done between the same system types. For example, you can move activations from one 9117-570 to another 9117-570, but not from a 9117-570 to a 9119-590 since the 570 and 590 systems are not only different models but different system types. Not only do the system types have to match between the source and target server, but the processor speed activations also have to match.

Another requirement for Mobile CoD is that the final configuration of both the source and the target server must be a valid configuration. For example, a 9119-595 server with 32 processors and 16 activations could not be a source server to move activations to another 595, because a 595 server might not have fewer than 50% of its processors activated. Furthermore, *both* the source and target servers must be in the same country in the same enterprise to be eligible for Mobile CoD.

#### **Requesting a Mobile CoD transfer**

Getting an activation moved from one system to another requires co-operation with both the sales team involved with the customer and the CoD Project Office.

The following are the necessary steps to request a transfer:

- 1. The customer must provide the system type and serial numbers for both the source and target servers to their sales representative.
- RPO MES configurations must be done within eConfig by your sales representative on both the source and target servers representing which resources and how much of each are being deallocated and reallocated.
- 3. These RPO MES configuration files are then sent to the System p CoD Project Office at pcod@us.ibm.com.
- 4. When the RPO MES order files have been approved by the CoD Project Office you will receive resource de-activation codes. For documentation on entering deactivation/activation codes on your HMC see 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395.

**Note:** The source server must be at firmware level SF235-160 or higher in order to implement step 4.

- Collect VPD at the source server for the appropriate resources using the following commands using the HMC CLI interface as shown in Figure 13-1 on page 377:
  - processors: lscod -m system\_name -t code -r proc -c cuod
  - memory: lscod -m system\_name -t code -r mem -c cuod

**Note:** The **1scod** command can only be executed if the managed system is in either *Standby* or *Operating* state.

After you collect VPD, send the output to pcod@us.ibm.com.



Figure 13-1 Capacity on Demand, example of Iscod command

6. When the CoD Project Office has received the VPD for the appropriate resource deactivation from the source server, they will then send you the appropriate activation codes for activation on the target server. You can enter these codes on your HMC using the steps outlined in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395.

# 13.3 Temporary types of CoD

On some system types some resources (processors, and sometimes memory) can be temporarily activated for brief or extended periods of time. This allows for greater resource allocation flexibility, as well as provide more choices to customers in how to pay for resource usage by allowing them to pay for just what they use.

The types of temporary CoD are:

- ► Trial CoD
- On/Off CoD
- Reserve Capacity
- Utility CoD (formerly Reserve Capacity)
- Capacity BackUp (CBU)

## 13.3.1 Trial CoD

Any system purchased with inactive system resources (processors or memory) can have resources temporarily activated using Trial Capacity on Demand. This allows for customers to test various processor or memory configurations before purchasing permanent or temporary resource activations. Similarly, customers can request full or partial trials for their resources to meet emergency performance needs. By doing this they can bridge the time gap between immediate performance needs and activation code delivery.

There are two types of Trial CoD:

- Standard Trial
- Exception Trial

#### **Standard Trial**

A Standard Trial allows for up to two processors and also four gigabytes of system memory to be temporarily activated for up to thirty days. If after thirty days the customer decides to fully activate those resources, additional trials for their other inactive resources become available to them.

#### **Exception Trial**

An Exception Trial allows for up to 100% of processors or memory to be temporarily activated for up to thirty days. Unlike the Standard Trial, an Exception Trial is one time only, and after the Exception Trial expires after thirty days no more Exception Trials can be requested.

To learn how to receive activation codes for either a standard or exception trial, see 13.4.2, "Requesting trial activation" on page 390.

## 13.3.2 On/Off CoD

On/Off Capacity On Demand is used to activate resources temporarily to cover for the demands of business peaks. As long as on On/Off resource (1 processor or 1 GB of memory) is active, at the end of every twenty four hours a resource day is charged against the customer. On/Off CoD is post-paid only, and allows for system administrators to anticipate peak business demands by activating resources appropriately.

#### **Contract requirements**

There are both contract and reporting requirements for On/Off CoD. The contract requirements for On/Off CoD can be found at:

http://www-912.ibm.com/supporthome.nsf/document/28640809
As shown in Figure 13-2, there are links for both the sales channel and customers to review the contract requirements associated with On/Off CoD.

	Country/region [select	ct]   Terms of use
Home Products	Services & industry solutions   Support & downloads   My account	
IBM Systems	On/Off Capacity on Demand	
Why IBM Systems	Sales Channel contracts/registration	
BladeCenter	Note: The Sales Channel contracts (registration page is intended for	Activities
Cluster servers	Sales Channels only. All other individuals should return to the CoD main	
Mainframe	page.	Channel Registration
System i	Step 1: Contracts	Cm View and work with
System p	1. Review contract requirements for the Sales Channel.	
System x	<ol> <li>Review contract requirements for the client.</li> </ol>	Search for contracts received by IBM
UNIX	Step 2: Register	·
Solutions		Your profile
Storage	<ol> <li>The Sales Channel (IBM Business partner, IBM Direct or OEM who is closest to the customer) must register one time to participate in the</li> </ol>	င္စ္ကာ Change your IBM
Support	enablement/billing for temporary capacity.	Registration profile
Operating systems	Step 3: Work with machine records	c∞ Update your Sales
Alerts		information
Developers	<ol> <li>You must record machine information the first time an Enablement Feature is ordered for a customer machine. Without this information.</li> </ol>	
Education	the order will not be fulfilled.	Change password
Literature	<ol> <li>You can view and work with machine records that you have previously entered.</li> </ol>	
News and events	providually entered	Help
		→ Having problems? Need help?
e)		Scal intranet

Figure 13-2 Capacity on Demand, On/Off CoD contract requirements

To obtain contract requirements for the sales channel, you must select your country and relationship with IBM as shown in Figure 13-3.



Figure 13-3 Capacity on Demand, On/Off CoD contract requirements for the sales channel

To obtain contract requirements for customers, you must select your country, as shown in Figure 13-4.

	For e	nd users of IBM	Required: IBM Customer Agreement,	machine records
System p	produ	uct who have an	Attachment for On/Off Capacity On	
System x	IBM C	Customer	Demand. Required: IBM Supplement for Op/Off	N 61-
	equiv	alent, in place	Canacity On Demand.	Tour profile
UNIX	cquit	along in place	Optional: IBM Addendum for On/Off	C= Change your IBM
Solutions			Capacity On Demand Alternative Reporting.	Registration profile
Storage	For e	nd users of IBM	Required: IBM Agreement for On/Off	C-Update your Sales
Support	produ	uct who do not	Capacity On Demand.	Channel contact
	have	an ICA, or	Required: IBM Supplement for On/Off	information
Operating systems	equiv	alent, in place	Capacity On Demand.	
Alerts			Capacity On Demand Alternative Reporting.	CmChange password
Developers	For O	EMa pating pape	Required IRM OFM Agreement Attachmen	•
Education	CoD	consolidation	for On/Off Capacity On Demand.	Help
	point	for all	Required: IBM OEM Supplement for On/Off	F Naving problems?
Literature	down	stream end-users	Capacity On Demand.	Need help?
News and events			Optional: IBM OEM Addendum for On/Off	
			Capacity On Demand Alternative Reporting.	
	The above co	ntract documents	are available through your IBM	Legend
Related links	representativ	e. After being sigr	ned by IBM and the client, the original must b	e 🖙 Denotes a password is
Warranty info	returned to th	ne IBM CSO organ	ization. In addition, a copy must be faxed to	required
<ul> <li>alphaWorks</li> </ul>	CoD Administ	trator at 1-507-25	3-4553 (World Wide support structure) befor	e
IBM Business Partners	the order for	the Enablement Fe	eature will be fulfilled.	
1	For more i	nformation abou	ut how to obtain a particular contract	
1	Country			
1	Country	Select a countr	γ <u>·</u>	
1		Select a countr	у	
1		United States		
		Albania	~ V	
About IBM   Privacy	Contact	Algeria		-
	American Samoa (USA)			
Andorra Andorra				
Cone Done		Angola		

Figure 13-4 Capacity on Demand, On/Off CoD contract requirements for customers

Finally, as shown in Figure 13-29 on page 409 there is a click-through agreement when the customer activates On/Off CoD on their managed server.

#### **Reporting requirements**

IBM customers have three options for reporting their On/Off CoD usage:

- ► Fax
- E-mail
- Service Agent (call home)

For fax reporting, send your usage reports to:

Capacity on Demand Administrator Fax number: 507-253-4553 Location: Rochester, Minnesota USA

For e-mail reports, send your usage reports to pcod@us.ibm.com.

The usage reports for both e-mail and fax must contain the following data:

- Customer company name
- Customer contact name
- Customer address
- Customer phone number
- Customer fax number
- Processor days used
- Memory days used

Furthermore, usage reporting can be done by activating Service Agent in the Service Management windows on your HMC. For instructions on enabling Call Home (also known as Service Agent) on your HMC, see 12.3.1, "Manage Systems Call-Home" on page 352.

Failure to report the billing data results in an estimated bill for 90 processor or memory days of temporary capacity.

#### Acquiring enablement codes

Before using On/Off capacity on your server, you must *enable* your server. To do this, engage your sales channel for an enablement feature (available as an upgrade feature only) and sign the required contracts.

IBM generates an enablement code, mails it to you, and posts it on the Web for you to retrieve and enter on your server.

To read about how you can access your enablement codes on the Web see 13.4, "CoD Web site navigation" on page 385, and to read about how to enter your enablement codes on the HMC see "Entering enablement and activation codes on the HMC" on page 395.

A On/Off processor enablement code lets you activate up to 360 processor days (360 days x 1 processor) of temporary capacity. If you have reached the limit of 360 processor days, place an order for another processor enablement code to reset the number of processor days you can request to 360.

A On/Off memory enablement code (if the customer opts for On/Off memory) lets you activate up to 999 memory days (999 days x 1 GB of memory) of temporary capacity. If you have reached the limit of 999 memory days, place an order for another memory enablement code to reset the number of memory days you can request to 999.

## 13.3.3 Reserve Capacity

Reserve Capacity is used to manage short workload peaks by temporarily activating inactive processors. This offering is only for POWER5 servers, and requires an HMC to enter the enablement code or to turn this feature on or off.

Reserve Capacity is pre-paid only, and it is purchased in 30 day blocks of processor days. A processor day can be used by any processor, and 30 processor days could mean:

- One processor for thirty days
- Two processors for fifteen days
- Three processors for ten days, and so forth

The shared processor pool will contain both non-reserve and reserve processor capacity. The reserve processor capacity will only be utilized if the non-reserve capacity is fully utilized from the shared processor pool.

A processor that is enabled through a Reserve Capacity enablement code is added to the shared processor pool. This additional processor capacity will be utilized in a partition when an uncapped partition requests additional processor resources from a 100% utilized shared processor pool.

A Reserve CoD processor day is consumed when the non-reserve processors become 100% utilized (all active non-Reserve processors available to the pool are being fully utilized), and 10% of a Reserve CoD processor is put into use for more than 30 consecutive seconds. When a Reserve CoD processor day is consumed within a 24 hour period against a specific Reserve CoD processor, no additional Reserve CoD processor days will be charged against that Reserve CoD processor within the same 24 hour period.

Reserve Capacity also requires the system to be licensed for Advance POWER Virtualization. This is because Reserve Capacity can only be used with uncapped partitions, which are then monitored for utilization. When the shared pool of processors reaches 100% utilization only then are reserve processors activated and processor days removed from the reserve capacity.

#### 13.3.4 Utility CoD

The shared processor pool will contain both non-reserve and Utility CoD capacity. The Utility CoD capacity will only be utilized if the non-reserve capacity is fully utilized from the shared processor pool.

A processor that is enabled through a Utility CoD enablement code is added to the shared processor pool. This additional processor capacity will be utilized in a partition when an uncapped partition requests additional processor resources from a 100% utilized shared processor pool.

Utility CoD allows for processors to be held in reserve and activated when system utilization hits a pre-determined peak performance threshold. In the event of a system peak where all the fully active processors reach 100% utilization, inactive processors can be activated on the fly by the HMC to add additional processing horsepower to cover for the increased performance need. When the business peak has ended, these processors are then returned to the shared resource pool until they are required again.

Utility CoD replaces Reserve Capacity on POWER6 servers, and it offers more flexibility and granularity than its predecessor. The major points of difference from Reserve Capacity are:

- Capacity is measured on a per processor minute, not processor day, basis
- Capacity can be paid for either before or after usage
- Resource usage reporting is required

Much like Reserve Capacity (which is still offered on POWER5 servers with the HMC), Utility CoD only works with uncapped partitions, and also requires the use of an HMC for both enablement and for managing the number of Utility CoD processors that are available for use in the shared processor pool monitoring of utilization.

There are no contract requirements for Utility CoD, but there is a pop-up window where the customer has to agree on the reporting requirements associated with Utility CoD.

#### 13.3.5 Capacity BackUp (CBU)

Capacity BackUp (CBU) is available for System p enterprise class servers to provide a production system backup capability at an attractive price.

With IBM HACMP V5 and HACMP/XD software (5765-F62) installed, Capacity BackUp processors can be automatically activated to provide round-the-clock business continuity and disaster recovery with no loss of data. HACMP can be configured to recognize a failing server and activate Capacity BackUp resources upon failover.

CBU systems are configured and shipped with a full compliment of processors installed with four active processors and the remaining processors inactive CoD. With the p5-590 and p5-595 systems CoD memory can also be purchased and activated when needed.

Each processor book ships with 450 On/Off days, and when these expire the customer must move to the On/Off CoD model as detailed in 13.3.2, "On/Off CoD" on page 378. As such, CBU has the exact same contract and reporting requirements as On/Off CoD.

Finally, beyond the initial four processor activations, the other processors on a CBU system can never be permanently activated.

#### Software licensing

There are no AIX, HACMP, or GPFS licensing fees associated with disaster recovery, however there are associated software licensing fees with activating CBU processors for testing purposes and production emergencies. Software licensing is done on a per processor day basis, and you should contact your sales representative to licence your system appropriately for such usage. There might be additional fees associated with your Linux distribution. Check with your Linux vendor to see if there are any licensing fees that are associated with your distribution and CBU usage.

# 13.4 CoD Web site navigation

The System p CoD Web site is available at:

http://www-03.ibm.com/systems/p/cod/

On this Web site, shown in Figure 13-5 on page 386, you can find:

- Documentation on the various types of CoD
- Activation codes for CoD offerings you are eligible for
- Hardware specific documentation for CoD

The three tabs in the center of the window as shown in Figure 13-5 on page 386 provide information about CoD, documentation on the different types of CoD, and an area where you can get activations for both CoD and Advanced POWER Virtualization (APV).

Under the Learn More section you can find hardware specific documents that discuss how CoD is handled and delivered on the various releases of the POWER hardware set.



Figure 13-5 Capacity on Demand, main Web site

# 13.4.1 Acquiring activation codes

To acquire your CoD activation codes online, visit the URL:

http://www-03.ibm.com/systems/p/cod/activation.html

Select Activation codes by machine serial number, as shown in Figure 13-6.

	Country/region [select	t]   Terms of use
		Search
Home Products	Services & industry solutions   Support & downloads   My account	
System p servers • About System p	IBM Systems > System p > Capacity on Demand	
Hardware	Overview Types Activation	Activation tools
Operating systems	Fasy to order, easy to use	→ VPD profile entry tool
Software Solutions Success stories	IBM's Capacity on Demand offerings for eServer p5 and pSeries are straightforward and easy to implement. There is never a requirement to activate any inactive processors. In fact, systems with inactive Capacity	→ Activation codes by machine serial number
Storage	Upgrade on Demand processors can be resold as is.	→ Trial Capacity on
Services Support Developers	The activation process is quick and easy. Just place an order, supply the necessary system configuration data when needed, and you will receive an encrypted key via the Web and by mail. There is no requirement to set up electronic monitoring of your configuration by IBM.	→ CoD Temoprary Processor and Memory activation Contract
Education Library	p5-520, p5-550, and p5-570 use the Capacity on Demand activation process to activate Advanced POWER Virtualization for those clients who order this feature as an MES after the initial order of the server. Activation of the	Guidance
Press	HMC.	•
é		Second Intranet

Figure 13-6 Capacity on Demand, activation codes

Then, enter the four digit system type, two digit factory code, and five digit serial number in the fields provided, and select **Submit** (Figure 13-7).



Figure 13-7 Capacity on Demand, entering system type and serial number

If all the data that you entered is valid, a results window opens, as shown in Figure 13-8. The top half are the codes that are already available for the system type and serial number you provided, as well as the dates the codes were made available. Below is a key for the acronyms of the various types of CoD offered.

TBLE		Country/region [select
<u>≞≕</u> ⊒₹∎⊚		
Home Products	Services & industry solutions 🔰 Support & downloa	ds My account
IBM Systems	Capacity on Demand	
Why IBM Systems	Activation code	
BladeCenter		
Cluster servers	To search for an activation code for a specific syste below and click <b>Submit</b> .	em, enter the information
Mainframe		
System i	Search results	
System p	System Type: 9117 Serial Number: 10-FFE0	Posted Date
System x	Type Activation Code	(MM/DD/YYYY)
UNIX	POD CDD49AE4625A1EBF54030000004004163	01/11/2007
Solutions	MOD   1F39EC74A007EE6B5680000000480041F9	01/11/2007
Storage	Activation type definitions	
Support	POD: CUoD Processor Activation Code	
	MOD: CUoD Memory Activation Code	
• Operating systems	On/Off CoD Processor Day Activation Co	de
Alerts	TMOD: On/Off CoD Memory Enablement Code	
Developers	PAID: Reserve CoD Prepaid Code	
Education	VET: Virtualization Technology Code	Cada
Literature	STDP: Standard Trial CoD Processor Activation STDM: Standard Trial CoD Memory Activation C	ode
News and events	EXCP: Exception Trial CoD Processor Activation	Code
	EXCM: Exception Trial CoD Memory Activation C	Code 🗾
•		
E Done		Local intranet

Figure 13-8 Capacity on Demand, activation codes results window

# 13.4.2 Requesting trial activation

To make either a *standard request* (described in "Standard Trial" on page 378) or *exception request* (described in "Exception Trial" on page 378), visit the URL:

https://www-912.ibm.com/tcod\_reg.nsf/TrialCod?OpenForm

Select the appropriate trial request. See Figure 13-9.



Figure 13-9 Capacity on Demand, request types

For the next step, you need to gather information from the HMC or in the Advanced System Management interface windows. To gather the trial code information off the HMC, proceed to "Gathering trial information off the HMC" on page 392. Otherwise, continue with the next section.

# Gathering trial information off of Advanced System Management interface

Select **Systems Management** and select the name of the server. Then, select **Operations**  $\rightarrow$  **Advanced System Management**. On the Advanced System Management interface window, select **On Demand Utilities**  $\rightarrow$  **CoD Processor Information** to see the information displayed in Figure 13-10.

Advanced System Management		
Log out User ID: admin	9117-MMA-SN10FFE0B-L9	EM310_026
<ul> <li>Expand all menus</li> <li>Collapse all menus</li> <li>Collapse all menus</li> <li>System Service Aids</li> <li>System Information</li> <li>System Configuration</li> <li>Network Services</li> <li>Performance Setup</li> <li>On Demand Utilities</li> <li>CoD Order Information</li> <li>CoD Activation</li> <li>CoD Processor Information</li> <li>CoD VET Information</li> <li>CoD VET Information</li> <li>CoD Concurrent Maintenance</li> <li>Login Profile</li> </ul>	CoD Processor Information           System type: 9117           System serial number: 10-FFE0B           Card type: 52AD           Card serial number: 00-6000396           Card serial number: 00-6000396           Card ID: 7009121624337B79           Resource ID: 5403           Activated Resources: 0004           Sequence number: 0041           Entry check: 2B           Installed processors: 0004           Permanent processors: 0004           Configuration index value: 0000           Processor CCIN: 53CE	
https://9.3.5.129:8443/asmproxy/action1.jsp?port=8443&host=9.3.5.129&jpasm=172.16.254.255⟨=0&form=22 9.3.5.129:8443		

Figure 13-10 Capacity on Demand, gathering information to request a trial

#### Gathering trial information off the HMC

To gather the required data off your HMC, select **Capacity on Demand**  $\rightarrow$  **Processor**  $\rightarrow$  **Trial CoD**  $\rightarrow$  **View Code Information** to open the window as shown in Figure 13-11.

Trial CoD Processor Code Information	: 9117-MMA-SN10FFE0B-L9 - Microsoft Internet Explorer			
Trial CoD Processor Code Information: 9117-MMA-SN10FFE0B-L9				
The information shown below is selected type for this system. If y	s used to generate a Trial processor code of the you want to save this information to a file, click Save.			
CoD code type:	Trial CoD Standard Request			
System type:	9117			
System serial number:	10-FFE0B			
Anchor card CCIN:	52AD			
Anchor card serial number:	00-6000396			
Anchor card unique identifier:	7009121624337B79			
Resource identifier:	5555			
Activated resources:	0000			
Sequence number:	0040			
Entry check:	23			
Save Close				

Figure 13-11 View code settings for trial CoD

**Note:** The data for Resource identifier changes depending on whether you are requesting an *exception* or *standard* request.

Now with this information available, you can enter the data in the form for the trial page as shown in Figure 13-12.

Trial Capacity on Demand		
You have selected to activate		
The fields indicated with an asterisk (*) are required to complete this transaction. If you do not want to provide us with the required information, please use the Back button on your browser, or close the window or browser session that is displaying this page, to return to the previous page.		
CoD information collected	from the machine	
How do I get my vital product	t data (CoD information)?	
System type*	9117	
System serial number*	10-FFE0B	
Anchor card CCIN*	52AD	
Anchor card serial number*	00-6000396	
Anchor card unique identifier*	7009121624337B79	
Resource identifier*	5403	
Activated resources*	4	
Sequence number*	0041	
Entry check*	2	
Customer information		
Company name*	IBM	
Company address*	1507 LBJ	
Company city*	Dallas	
State or province, Country*	Tx	
Company postal code*	75234	
Contact name*	John	
Contact phone*	555 222 1234	
Contact e-mail*	jdoe@nospam.com	

Figure 13-12 Capacity on Demand, requesting a trial

When you have completed the form, review the terms and conditions for trial capacity as shown in Figure 13-13, confirm that you have reviewed and agree with them, and then select **Submit**.

#### Terms and conditions

Based on your CoD request, a code will be provided that will activate a limited amount of inactive capacity on your machine. Once the code is entered, the capacity is activated and the trial period begins for 30 powered on server days. It is the responsibility of the customer to assign the capacity to partitions for use and to remove the capacity from the partitions prior to the expiration of the trial period. Frequent messaging will provide the customer with clear warning relative to the pending expiration of the trial period to ensure proper action is taken. To ensure, compliance with these terms and conditions the client requesting the no-charge access to trial capacity, must agree to provide IBM and/or its partners with sufficient access to the client's machine, if requested, to ascertain if trial capacity is still being used beyond the entitled period of time.

I agree with the terms and conditions associated with making a Trial Cool request.

This data may be used by IBM or selected organizations, such as Lenovo, to provide you with information about other offerings. To receive this via e-mail, check the first box below. Alternatively, if you would prefer not to receive such information by any means, check the second box.

Please use e-mail to send me information about other offerings.

 $\square$   $\;$  Please do not use this data to send me information about other offerings.

By clicking "submit" you agree that IBM may process your data in the manner indicated above and as described in <u>Privacy</u>.

🔁 Submit

Figure 13-13 Capacity on Demand, agree to terms and conditions

You then get a confirmation page, and your activation codes display on the Web as described in 13.4.1, "Acquiring activation codes" on page 387.

# 13.5 Entering enablement and activation codes on the HMC

In this section, we discuss entering enablement codes, deactivation, and activation codes on your HMC. To read about how to acquire these codes, see 13.4.1, "Acquiring activation codes" on page 387.

#### 13.5.1 Entering an activation, enablement, or deactivation code

On the HMC workplace window, select **Systems Management**  $\rightarrow$  **Servers** and the name of the server. Then, select **Capacity on Demand**  $\rightarrow$  **Enter CoD Code** to open the window shown in Figure 13-14.

Enter CoD Code: 9117-MMA-SN10FFE0B-L9		
* Code: B6F6D4BBEF7F14BBRPMA00	000001004222	
OK Cancel Help		
Done	hmc2.itsc.austin.ibm.com 😑	

Figure 13-14 Capacity on Demand, entering activation/deactivation codes

Deactivation codes can only be acquired from the CoD project office and can be obtained by contacting pcod@us.ibm.com.

Activation and enablement codes are purchased through your sales channel. You can obtain them on the Web as described in 13.4.1, "Acquiring activation codes" on page 387, and they are mailed to you after they are purchased.

**Note:** Enablement, activation, and deactivation codes only work once. If you require additional code, you have to work with the System p CoD project office at pcod@us.ibm.com.

When your code is entered, select **OK**. If your code is valid, you receive a confirmation window as shown in Figure 13-15.



Figure 13-15 Capacity on Demand, deactivation successful

After this point the resources that you either activated or deactivated are changed on the managed server. If you entered an enablement code, the code that is associated with your CoD type allows you to manipulate the CoD offering on your managed server.

# 13.5.2 Activating and managing Utility CoD

You can acquire your Utility CoD activation code online as described in 13.4.1, "Acquiring activation codes" on page 387 and enter the activation code for Utility CoD as described in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395.

When you enter your activation code, a results window displays as shown in Figure 13-16.



Figure 13-16 Capacity on Demand, activation Utility CoD

When activated, you can now manage your system's **Utility** CoD usage from the Systems Management area. Select **Systems Management**  $\rightarrow$  **Servers** and the

name of the server. Then, expand **Capacity on Demand (Cod)**  $\rightarrow$  **Processor**  $\rightarrow$  **Utitlity CoD** to see the view shown in Figure 13-17.

Serviceability		
Capacity On Demand (CoD)		
Enter CoD Code		
View History Log		
Processor		
View Capacity Settings		
CUoD (perm anent)		
On/Off CoD     On     Off CoD     On     Off     On      On     Off     O     Off     O     Off     O     Off     O		
Trial CoD		
Utility CoD		
Manage		
View Capacity Settings		
View Code Information		
View Shared Processor Utilization		
Mem ory     Mem ory		
Advanced POWER Virtualization		
Enterprise Enablement		
Other Advanced Functions		

Figure 13-17 Capacity on Demand, Utility CoD view

From this view, you can:

- Manage: Set the number of processors eligible for Utility usage as well as set a processor minute limit.
- ► View Capacity Settings:
  - View the number of processors currently eligible for utility usage.
  - See the current minute usage limit.
  - View processor minutes that have been used by the server.
  - Examine how many processor minutes have been reported back to IBM.
- View Code Information: View system information associated with Utility CoD registration and activation.
- View Shared Processor Utilization: View utilization numbers for the shared processor pool, both Utility CoD and Non-Utility CoD processors.

#### Manage

Under the **System Management** view for a specific managed server, select **Capacity on Demand (CoD)**  $\rightarrow$  **Processor**  $\rightarrow$  **Utility CoD**  $\rightarrow$  **Manage** to open the window as shown in Figure 13-18. On this window, you can add inactive processors to be used with Utility CoD and set an upper limit of processor minutes to be used. Confirm your selections and select **OK**.

Manage Utility CoD: e68fsp1			
To change the number of Utility CoD processors in the shared processor pool, enter the new number of Utility CoD processors you want. To set a processor minute usage limit, enter the new limit.			
Utility CoD state: Code Not	Entered		
Processors			
Utility CoD processors cannot be requested be enabled.     Inactive processors available:	ecause Utility CoD is not		
Utility CoD processors:			
Processor minute usage limit			
Enable processor minute usage limit Processor minutes remaining: Current limit: New limit:			
OK Cancel Help			
Done Done	santenay.austin.ibm.com 🙆 🛒		

Figure 13-18 Capacity on Demand, manage utility capacity

#### View capacity settings

Under the **System Management** view for a specific managed server select **Capacity on Demand (CoD)**  $\rightarrow$  **Processor**  $\rightarrow$  **Utility CoD**  $\rightarrow$  **View Capacity Settings** to open the window as shown in Figure 13-19. Here you can see the number of Utility CoD processors and are configured for Utility processor minute usage, as well as:

- The upper limit of processor minutes set
- ► The remaining processor minutes unused
- The stats for the previous month, the current month, and total minutes used to date
- ► The total number of processor minutes that have been reported to IBM

9117-MMA-SN10FFE0B-L9	During		
Juinty GOD state:	Running		
Days remaining for Utility CoD:	365		
Processors			_
Inactive processors available:	0		
Utility CoD processors:	1		
- Processor minute usage limit ——			
Processor minutes remaining:	360		
Limit:	360		
- Processor minutes used ————			
This month: 0			
Last month: 0			
Total to date: 0			
- Reporting			
Unreported processor minutes	:	0	
Reporting threshold (processo	r minutes):	500	
Reporting limit (processor mine	utes):	1000	0
Close Help			
lana			hmc? itec austin ihm co

Figure 13-19 Capacity on Demand, view capacity settings

#### View code information

Under the **System Management** view for a specific managed server, select **Capacity on Demand (CoD)**  $\rightarrow$  **Processor**  $\rightarrow$  **Utility CoD**  $\rightarrow$  **View code information**. You can view the registration and serial codes associated with your Utility CoD activation as shown in Figure 13-20. You can also select your view for either the reporting or enablement codes associated with Utility CoD and your managed server.

Utility CoD Code Information: 9117-MMA-SN10FFE0B-L9			
The information shown below is used to generate a Utility CoD code of the selected type for this system. If you want to save this information to a file, click Save.			
CoD code type: Utility CoD reporting code			
System type:	Utility CoD reporting code		
System serial number:	Utility CoD enablement code		
Anchor card CCIN:	52AD		
Anchor card serial number:	00-6000396		
Anchor card unique identifier:	7009121624337B79		
Resource identifier: 4444			
Activated resources:	0000		
Sequence number:	0040		
Entry check:	23		
Unreported processor minutes: 0			
Save Close			
javascript:CSBUpdateInputFromOption('W41bf3aec_opt_0',' hmc2.itsc.austin.ibm.com 😑			

Figure 13-20 Capacity on Demand, view code information

### View shared processor utilization

Under the **System Management** view for a specific managed server select **Capacity on Demand (CoD)**  $\rightarrow$  **Processor**  $\rightarrow$  **Utility CoD**  $\rightarrow$  **View Shared Processor Utilization**. You can see the number of processors and their utilization both in and outside Utility CoD, as shown in Figure 13-21.

Information about th shown below.	e processors in the sha	red processor pool is	
Type of processors	Number of processors	Utilization (percent)	
Non-Utility CoD	0	0	
Utility CoD	1	0	
Close Help	]1	0	

Figure 13-21 Capacity on Demand, view shared processor utilization

#### Viewing Utility CoD usage

On the HMC V7 you can view the logs to examine how many Utility CoD minutes have been used by your managed server. Select **Server Management**  $\rightarrow$  **Servers** and the name of the server. Then, select **Capacity on Demand**  $\rightarrow$  **View History Log**. See Figure 13-22.

CoD History Log: 9	9117-MMA-SN10FFE0B-L9
Time Stamp	Log Entry
05/09/2007:21:58:16	HSCL0336 Utility CoD processor minutes used during last hour: 1.
05/09/2007:20:51:42	HSCL0336 Utility CoD processor minutes used during last hour: 1.
05/04/2007:23:10:51	HSCL0333 Utility CoD processors activated, number activated: 1, new total: 1.
05/04/2007:23:10:50	HSCL033B Utility CoD processor minute usage limit set, number of processor minutes: 360.
05/04/2007:23:00:39	HSCL0330 Utility CoD enablement code entered, reporting threshold: 500, reporting limit: 1000.
05/04/2007:22:43:14	HSCL0327 Remove processor code entered, number of permanent processors: 1, index: 0000.
Close Help	

Figure 13-22 Capacity on Demand, view Utility CoD usage log

# 13.5.3 Activating and managing Reserve CoD

Before you can use the management options for reserve CoD, you have to enter an enablement code on the HMC. To acquire your Reserve CoD enablement code online, refer to 13.4.1, "Acquiring activation codes" on page 387 and enter the enablement code for Reserve CoD by following the directions in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395. Reserve CoD is only available on POWER5 servers and can be accessed by clicking **Server Management**  $\rightarrow$  **Servers** and the name of the server. Then, select **Capacity on Demand**  $\rightarrow$  **Processor**  $\rightarrow$  **Reserve CoD** to see the view shown in Figure 13-23.

Tasks: p5+-9133-55A-SN10D1FAG
Properties
Operations
Configuration
Hardware (Information)
Updates     Updates
Capacity On Demand (CoD)
Enter CoD Code
View History Log
Processor
View Capacity Settings
CUoD (perm anent)
Reserve CoD
Manage View Capacity Settings View Code Information View Shared Processor Utilization
Advanced POWER Virtualization
Enterprise Enablement
Other Advanced Functions

Figure 13-23 Capacity on Demand, Reserve Capacity

Here you can:

- Manage reserve capacity settings: Add processors to the resource pool
- View capacity settings: View the values you have set through the management windows
- View code settings: View codes
- View shared processor utilization

#### View capacity settings

Select **Capacity on Demand**  $\rightarrow$  **View Capacity Settings**. Here you can view the processors that can be used for Reserve Capacity, as well as the prepaid processor days that remain for usage, as shown in Figure 13-24.

Reserve CoD Capacity Settings: p5-	+-9133-55A-SN10D1FAG
Reserve CoD state:	Code Not Entered
Activated Reserve CoD processors:	0
Inactive processors available for Reserve CoD:	0
Prepaid processor days remaining for Reserve CoD:	0
Activated Reserve CoD Processor Hours Remaining	
Total: 1	
Close Help	
Cone	Internet

Figure 13-24 Reserve capacity, view capacity settings

#### View code settings

Select **Capacity on Demand**  $\rightarrow$  **View Code Settings**. Here you can view the codes that are associated with your Reserve Capacity enablement. You can offload this information to remote system or removable media by using the **Save** function. See Figure 13-25.

Reserve CoD Code Information:	p5+-9133-55A-SN10D1FAG	
The information shown below is used to generate a Reserve capacity prepaid code for this system. If you want to save this information to a file, click Save.		
System type:	9133	
System serial number:	10-D1FAG	
Anchor card CCIN:	52A1	
Anchor card serial number:	00-5000675	
Anchor card unique identifier:	619318501795229A	
Resource identifier:	7215	
Activated resources:	0000	
Sequence number:	0040	
Entry check:	5A	
Save Close		
E Done	l 📄 📄 🔮 Internet	

Figure 13-25 Reserve capacity, view code information

#### View shared processor utilization

Select **Capacity on Demand**  $\rightarrow$  **View Shared Processor Utilization**. Here you can check the state of reserve and non-reserve processors, as shown in Figure 13-26. If your system has hit a peak performance threshold as outlined in 13.3.3, "Reserve Capacity" on page 383, you can view the inactive processors that have become activated and made available for Reserve Capacity usage.

Shared Processor Pool Utilization: p5+-9133-55A-SN10D1FAG Information about the processors in the shared processor pool is shown below.			
Type of processors	Number of processors	Utilization (percent)	
Non-Reserve CoD	7	0	
Reserve CoD	0	0	
Close Help			Internet /

Figure 13-26 Reserve capacity, view shared processor utilization

# 13.5.4 Activating and managing On/Off CoD

Before you can use the management options for On/Off CoD, you have to enter an enablement code on the HMC. To acquire your On/Off CoD enablement code online refer to 13.4.1, "Acquiring activation codes" on page 387 and enter the enablement code for Reserve CoD as described in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395. On/Off CoD is available on POWER5 and POWER6 servers, and can be accessed by clicking **Server Management**  $\rightarrow$  **Servers** and the name of the server. Then, select **Capacity on Demand**  $\rightarrow$  **Processor**  $\rightarrow$  **On/Off CoD** to see the view shown in Figure 13-23.

Tasks: 9117-MMA-SN10FFE0B-L9	
Properties	
Configuration	
<ul> <li>Hardware (Information)</li> </ul>	
Updates     Updates	
Capacity On Demand (CoD)	
Enter CoD Code	
View History Log	
E Processor	
View Capacity Settings	
E CUOD (permanent)	
On/Off CoD	
Manage View Capacity Settings View Billing Information View Code Information	
Trial CoD	
Utility CoD	
Advanced POWER Virtualization	
Enterprise Enablement	
Other Advanced Functions	

Figure 13-27 Capacity on Demand, managing On/Off CoD

### Manage on/off CoD

Select **Manage** under **On/Off CoD** to open the window shown in Figure 13-28. Here you can specify

- How many inactive processors you want to activate for On/Off CoD
- ► The number of days you want these processors active for use by partitions

Manage Op/Off CoD Processors: 9117-MMA-SN10EFE0B-L 9		
To activate On/Off CoD processors, enter the number of On/Off CoD processors you want and the number of days you want them for.		
Number of On/Off CoD processors:	1	
Number of days:	22	
On/Off CoD state:	Available	
Activated On/Off CoD processors:	0	
Inactive processors available for On/Off CoD:	1	
Processor days remaining in the current On/Off CoD request:	0	
Hours remaining in the current processor day:	0	
Processor days available for new On/Off CoD requests:	360	
OK Cancel Help		

Figure 13-28 Manage on/off settings

After you have entered your selections, select **OK**. The window shown in Figure 13-29 opens. Verify your entries and agree to the terms and conditions for On/Off processor usage. If your entries are correct, and you agree with the terms and conditions, select **OK**.

Manage On/Off CoD Processors Confirmation: 9117-N SN10FFE0B-L9	MMA-
New number of On/Off CoD processors:	1
New number of days:	22
New number of On/Off CoD processors:       1         New number of days:       22         After you confirm this request for On/Off CoD capacity, by clicking 'Ok', the newly activated processors will be made available for use by uncapped partitions. You can choose to assign these processors to a partition(s) of your choice. If there are no uncapped partitions, then you must assign these processors to a partition(s) to actually begin using them. Accounting for billing purposes begins when you confirm this request. Before the requested days have passed, you must make the temporarily activated processors available by removing the processors from partitions so that they can be reclaimed by the system. In the event you fail to make such capacity available to be reclaimed, the system will continue to account for unreturned processor days, and you will be billed for those unreturned processor days, pursuant to the terms and conditions of the agreement for On/Off Capacity on Demand (CoD).         OK       Cancel	

Figure 13-29 On/off confirmation and agreement

16

In the confirmation window, select **OK** (Figure 13-30).



Figure 13-30 On/off CoD results window

#### View capacity settings

The View Capacity Settings option allows you to review your managed server's On/Off CoD usage, as well as view how many processors are exercising On/Off processor days. Select **View Capacity Settings** under **On/Off CoD** to open the window shown in Figure 13-31. To return to the main HMC view, select **Close**.

On/Off CoD Processor Capacity Settings: 9117-MMA- SN10FFE0B-L9	
On/Off CoD state:	Running
Activated On/Off CoD processors:	1
Inactive processors available for On/Off CoD:	0
Processor days remaining in the current On/Off CoD request:	21
Hours remaining in the current processor day:	23
Unreturned On/Off CoD processors:	0
Processor days available for new On/Off CoD requests:	338
Close Help	

Figure 13-31 On/off CoD, view capacity settings

#### View billing information

The view billing area on the HMC under On/Off CoD allows you to review all of the billing information for On/Off CoD associated with your managed server. Select **View Billing Information** under **On/Off CoD** to open the window shown in Figure 13-32. You have the option to offload billing data to an FTP server or removable media. To do so, select **Save**. Otherwise, select **Cancel** to return to the main HMC view.

On/Off CoD Processor Billing Information: 9117-MMA-SN10FFE0B-L9		
The information shown below is used to manually information. If you want to save this information to	y report On/Off CoD processor billing a file, click Save.	
System type:	9117	
System serial number:	10-FFE0B	
Anchor card CCIN:	52AD	
Anchor card serial number:	00-6000396	
Anchor card unique identifier:	7009121624337B79	
Resource identifier:	7951	
Sequence number:	0041	
Activated On/Off CoD resources:	0001	
Inactive resources available for On/Off CoD:	0000	
History of expired resource days:	0001	
History of unreturned resource days:	0000	
Collection date:	2007-05-15	
Collection time:	22:42:33	
Total system run time hours:	000011	
Signature:	FFEB95FFDA29FA71	
Entry check:	34	
Status:	01	
Save Cancel		

Figure 13-32 On/off CoD, view billing information

#### View code information

The view code area under On/Off CoD allows you to view all of the code information tied to the On/Off enablement on your managed server. Select **View Code Information** under **On/Off CoD** to open the window shown in Figure 13-33. You have the option to offload the code information to removable media or an FTP server. To do so, select **Save** and specify a location. Otherwise, select **Close** to return to the main HMC view.

On/Off CoD Code Information: 9117-MMA-SN10FFE0B-L9		
The information shown below is used to generate an On/Off processor enablement code for this system. If you want to save this information to a file, click Save.		
System type:	9117	
System serial number:	10-FFE0B	
Anchor card CCIN:	52AD	
Anchor card serial number:	00-6000396	
Anchor card unique identifier:	7009121624337B79	
Resource identifier:	7951	
Activated resources:	0360	
Sequence number:	0041	
Entry check:	21	
Save Close		

Figure 13-33 On/off CoD, view code information

# 13.5.5 Activating and managing Trial CoD

Before you can use the management options for Trial CoD, you have to enter an enablement code on the HMC. To acquire your Trial CoD enablement code online refer to 13.4.1, "Acquiring activation codes" on page 387 and enter the enablement code for Trial CoD as described in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395.

Trial CoD is available on POWER5 and POWER6 servers and can be accessed by clicking **Server Management**  $\rightarrow$  **Servers** and the name of the server. Then, select **Capacity on Demand**  $\rightarrow$  **Processor**  $\rightarrow$  **Trial CoD** to see the view shown in Figure 13-34.

Tasks: 9117-MMA-SN10FFE0B-L9
Properties
Operations
Configuration
Hardware (Information)
Serviceability
Capacity On Demand (CoD)
Enter CoD Code View History Log
Processor
View Capacity Settings
CUoD (perm anent)
Trial CoD
Stop View Capacity Settings View Code Information Utility CoD
■ Memory
Advanced POWER Virtualization
Other Advanced Functions

Figure 13-34 Capacity on Demand, managing Trial CoD
You can view the current Trial CoD capacity settings by clicking **Capacity on Demand**  $\rightarrow$  **Processor**  $\rightarrow$  **Trial CoD**  $\rightarrow$  **View Capacity Settings**. Then the window displays as shown in Figure 13-35.

Trial CoD Processor Capacity Settings: 9117-MMA-SN10FFE0B- L9		
Trial CoD state:	Not Running	
Activated Trial CoD processors:	0	
Days/Hours remaining in the current Trial CoD period:	0/0	
Close Help		

Figure 13-35 Capacity on Demand, view trial capacity settings

This window shows you the current state of your trial, how many processors are active, and how many days are left on the current trial period.

Select Capacity on Demand  $\rightarrow$  Processor  $\rightarrow$  Trial CoD  $\rightarrow$  View Code Information to open a window that presents all the information that is associated with logging your trial usage (Figure 13-36).

Trial CoD Processor Code Information: 9117-MMA- SN10FFE0B-L9		
The information shown below is used to generate a Trial processor code of the selected type for this system. If you want to save this information to a file, click Save.		
CoD code type:	Trial CoD Standard Request	
System type:	9117	
System serial number:	10-FFE0B	
Anchor card CCIN:	52AD	
Anchor card serial number:	00-6000396	
Anchor card unique identifier:	7009121624337B79	
Resource identifier:	5555	
Activated resources:	0000	
Sequence number:	0040	
Entry check:	23	
Save Close		

Figure 13-36 Capacity on Demand, view trial code information

If you want to take the information contained on this window and save it to removable media or a remote system, select **Save** to open the window shown in Figure 13-37. Click **OK**.

	•	
Save CoD Code Information: 9117-MMA-SN10FFE0B-L9		
Select an option for saving the information used to generate a CoD code for this system.		
Save to a file on a remote system		
Remote system :		
File name :		
User ID :		
Password :		
Save to Media		
OK Cancel Help		
	-	

Figure 13-37 Capacity on Demand, saving trial code information

If you select **Save to Media**, the window shown in Figure 13-38 opens. Select the destination of the save, and then select **OK**.

**Note:** The Save function only works on formatted media. To read about how to format your removable media on your HMC, refer to "Format Media" on page 344.

Select Media Device		
Select one of the media devices listed below and press OK to continue the task, otherwise press Cancel. If you add or remove devices, press Refresh to update the device list.		
This task supports the following devices: Diskette Drive, DVD-RAM Drive, USB Flash Memory Drive		
Select		
<ul> <li>Diskette Drive (No media found)</li> </ul>		
<ul> <li>DVD-RAM Drive (Media label is CDROM)</li> </ul>		
OK Refresh Cancel Help	•	
🛎 Done		

Figure 13-38 Capacity on Demand, save code information

#### 13.5.6 Advanced System Management CoD interface

Select **Systems Management** and the name of the server. Then, select **Operations**  $\rightarrow$  **Advanced System Management**. From the Advanced System Management interface window that opens (Figure 13-39), you can:

- ► Get order information
- Enter an activation code for a CoD offering
- Put your managed server into CoD recovery mode
- ► Enter a CoD command
- Gather processor related CoD code information
- Gather memory related CoD code information
- ► Get VET information
- View CoD capacity settings

LEM. Advanced Sys	stem Management	Copyright © 2002, 2007 IBM Corporation. All rights reserved.
Log out User ID: admin	9117-MMA-SN10FFE0B-L9	EM310_026
<ul> <li>Expand all menus</li> <li>Collapse all menus</li> <li>Power/Restart Control</li> <li>System Service Aids</li> <li>System Information</li> <li>System Configuration</li> <li>Network Services</li> <li>Performance Setup</li> <li>On Demand Utilities CoD Order Information CoD Activation CoD Recovery CoD Command CoD Processor Information CoD WET Information CoD VET Information CoD Capability Settings</li> <li>Concurrent Maintenance</li> <li>Login Profile</li> </ul>	Welcome         Machine type-model: 9117-MMA         Serial number: 10FFE0B         Date: 2007-5-1         Time: 21:15:16 UTC         Service Processor: Primary         Current users         User ID         Location         admin         172.16.0.1         User Status         User ID         Status         dev         Enabled         celogin         Enabled         celogin1	
Done		9.3.5.129:8443 🗎

Figure 13-39 Capacity on Demand, ASMI windows

# Gathering processor code information through the Advanced System Management interface

For various types of CoD requests you need to provide the processor code information of your system to IBM to complete the request.

To get the information, select **CoD Processor Information** under **On Demand Utilities**, as shown in Figure 13-40.

<b>LEM.</b> Advanced Sys	Copyright © 2002, 2007 IBM Corporation. All rights reserved.	
Log out User ID: admin	9117-MMA-SN10FFE0B-L9	EM310_026
Expand all menus Collapse all menus System Service Aids System Information System Configuration Network Services Performance Setup On Demand Utilities CoD Order Information CoD Recovery CoD Command CoD Command CoD Processor Information CoD VET Information CoD Capability Settings Concurrent Maintenance Login Profile	CoD Processor Information System type: 9117 System serial number: 10-FFE0B Card type: 52AD Card serial number: 00-6000396 Card ID: 7009121624337B79 Resource ID: 5403 Activated Resources: 0004 Sequence number: 0041 Entry check: 2B Installed processors: 0004 Permanent processors: 0004 Inactive processors: 0000 Configuration index value: 0000 Processor CCIN: 53CE	
https://9.3.5.129:8443/asmproxy/action1 jsp?port=8443&host=9.3.5.129&ipasm=172.16.254.255⟨=0&form=22 9.3.5.129:8443 (2010)		

Figure 13-40 Gather processor code information

# Gathering memory code information through the Advanced System Management interface

For various types of CoD requests you need to provide the memory code information of your system to IBM to complete the request. To get the information, select **CoD Memory Information** under **On Demand Utilities**, as shown in Figure 13-41.



Figure 13-41 Gather memory code information

# Advanced System Management interface use of activation, deactivation, and enablement codes

You can enter your activation codes using the HMC windows as discussed in 13.5.1, "Entering an activation, enablement, or deactivation code" on page 395, or you can use the Advanced System Management interface to enter your codes.

To use the Advanced System Management interface to enter your codes, select **CoD Activation** under **On Demand Utilities**, as shown in Figure 13-42.



Figure 13-42 Enter CoD activation, deactivation, or enablement code

# 14

# Advanced System Management Interface

In this chapter, we describe how to set up and use the Advanced System Management Interface (ASMI). The ASMI provides a terminal interface through a standard Web browser to the service processor that allows you to perform general and administrator level service tasks. The ASMI allows you to perform service functions and various system management functions.

# 14.1 Connecting to ASMI

There are three different methods to gain access to the ASMI:

- Access through the Hardware Management Console (HMC)
- Access through a Web browser
- Access through ASCII terminal

#### 14.1.1 Connection to ASMI using the HMC

If you have an HMC attached to your managed system, connecting the ASMI using the HMC is the simplest way to connect. If this is a new system, refer to 3.3, "Connecting managed systems to the HMC" on page 130 for information about how to connect your managed system to the HMC.

To connect to ASMI using the HMC:

- 1. In the HMC workplace window, select System Management  $\rightarrow$  Servers.
- In the contents area select the server to which you want to connect ASMI (Figure 14-1).

3.	Select O	perations $\rightarrow$	Advanced	System	Manag	gement (	ASM)	1.
----	----------	-------------------------	----------	--------	-------	----------	------	----

Cor	Contents of: Servers							
				*			_ 1	
	Ø					isks▼ Views		
Sel	lect ^	Name	^	Status	^	Available Processing ^ Units	Available Memory ^ (GB)	Reference 🔨 Code
		9117-MMA-SN	10DD4AC-L10		Operating	0	0.3125	
		9117-MMA-SN	110FFE0B-L9₽	Δ	Operating	1.7	4.5	
			Total: 2 Filt	ered: 2 S	Selected: 1			
-								
Tas	KS: 91	17-MMA-SN10FF	E0B-L9					
	Properties							
	Operations							
	Power Off							
	ED Status							
	Schedule Operations							
	Advanced System Management (ASM)							

Figure 14-1 Connection to ASMI using HMC

#### 14.1.2 Connecting to ASMI through a Web browser

The Web interface to the ASMI is accessible through Microsoft® Internet Explorer 6.0, Netscape 7.1, or Opera 7.23 and Mozilla Firefox 1.0.7 running on a PC or mobile computer that is connected to the service processor. The Web interface is available during all phases of system operation, including the initial program load (IPL) and run time. However, some of the menu options in the Web interface are unavailable during IPL or run time to prevent usage or ownership conflicts if the system resources are in use during that phase.

To set up the Web browser for direct or remote access to the ASMI, complete the following tasks:

- 1. Connect the power cord from the server to a power source, and wait for the control panel to display 01.
- 2. Select a PC or a mobile computer that has Microsoft Internet Explorer 6.0, Netscape 7.1, or Opera 7.23 and Mozilla Firefox 1.0.7 to connect to your server. You can use this PC or mobile computer temporarily or permanently to access ASMI.
- 3. Connect an Ethernet cable from the PC or mobile computer to the Ethernet port labeled HMC1 on the back of the managed system. If HMC1 is occupied, connect an Ethernet cable from the PC or mobile computer to the Ethernet port labeled HMC2 on the back of the managed system. You can use cross over cable or standard Ethernet cable, both are supported.
- 4. Configure the Ethernet interface on the PC or mobile computer to an IP address and subnet mask within the same subnet as the server so that your PC or mobile computer can communicate with the server. Use Table 14-1 to help you determine these values.

Sever Connector	Subnet Mask	IP address
HMC1	255.255.255.0	169.254.2.147
HMC2	255.255.255.0	169.254.3.147

Table 14-1 Default IP address for server connectors HMC1 and HMC2

If you are not sure how to configure your PCs IP settings, then consult your network administrator.

5. Use Table 14-1 to determine the IP address of the Ethernet port to which your PC or mobile computer is connected, and enter the IP address in the Address field of your PC's or mobile computer's Web browser.

For example, if you connected your PC or mobile computer to HMC1, enter https://169.254.2.147 in your PC's or mobile computer's Web browser.

#### 14.1.3 Accessing the ASMI using an ASCII terminal

The ASCII interface to the ASMI provides a subset of the Web interface functions. The ASCII terminal is available only when the system is in the platform standby state. It is not available during the IPL or run time. The ASMI on an ASCII terminal is not available during the other phases of system operation, including the IPL and run time.

To set up the ASCII terminal for direct or remote access to the ASMI, complete the following tasks:

1. Use a null modem cable to connect the ASCII terminal to system connector S1 on the back of the server or to system port S1 on the control panel using an RJ-45 connector.

**Note:** Both system port 1 connections are not available simultaneously; when one is connected, the other is deactivated.

- 2. Connect the power cord from the server to a power source.
- 3. Wait for the control panel to display 01.
- 4. Ensure that your ASCII terminal is set to the following general attributes. These attributes are the default settings for the diagnostic programs:

Line Speed-19200,word length-8,parity- none,stop bit-1

5. Press a key on the ASCII terminal to allow the service processor to confirm the presence of the ASCII terminal.

You should get the ASMI login window.

### 14.2 Log in to ASMI

To connect successfully to the ASMI, the ASMI requires password authentication.

- The ASMI provides a Secure Sockets Layer (SSL) Web connection to the service processor. To establish an SSL connection, open your browser using https://.
- The browser-based ASMI is available during all phases of the system operation, including IPL and run time. Some menu options are not available during the system IPL or run time to prevent usage or ownership conflicts if corresponding resources are in use during that phase.

 The ASMI that is accessed on a terminal is available only if the system is at platform standby.

After you have connected to the ASMI as described in 14.1, "Connecting to ASMI" on page 424, the login display opens. Enter one of the default user ID and passwords, as shown in Table 14-2.

Table 14-2 Defau	ult login user ID and password	

User ID	Delault Password	Authority Level
general	general	general user
admin	admin	administrator
celogin	contact ibm for password	Authorised service provider

As soon as you login to ASMI, you are asked to change the default password. You will not be allowed to proceed unless you change the password.

#### 14.2.1 ASMI login restrictions

The following restrictions apply to ASMI users:

- Only three users can login at any one time.
- If you are logged in and inactive for 15 minutes, your session expires and you have to login again.
- If you make five invalid login attempts, your user ID is locked out for five minutes.

The ASMI window shown in Figure 14-2 opens after a successful login.

<b>IEM.</b> Advanced Syste	m Management
Log out User ID: admin	9117-MMA-SN10FFE0B-L9
<ul> <li>Expand all menus</li> <li>Power/Restart Control</li> <li>System Service Aids</li> <li>System Information</li> <li>System Configuration</li> <li>Network Services</li> <li>Performance Setup</li> <li>On Demand Utilities</li> <li>Concurrent Maintenance</li> <li>Login Profile</li> </ul>	Welcome         Machine type-model: 9117-MMA         Serial number: 10FFE0B         Date: 2007-5-13         Time: 0:54:54 UTC         Service Processor: Primary         Current users         User ID       Location         admin       192.168.255.222         User Status         User ID       Status         dev       Enabled         celogin       Enabled         celogin1       Disabled

Figure 14-2 Advanced System Management menus

## 14.3 Power and restart control

You can use the power and restart control feature to control the system power manually and automatically. In this section, we also discuss different options that are available to turn on the system. See Figure 14-3.

We describe the following options in detail:

- Fast and slow boot
- Temporary and Permanent boot side
- Normal and permanent operating mode

IEM. Advanced Sy	ystem Management
Log out User ID: admin	9117-MMA-SN10FFE0B-L9
<ul> <li>Expand all menus</li> <li>Collapse all menus</li> <li>Collapse all menus</li> <li>Power/Restart Control Power On/Off System Auto Power Restart Immediate Power Off System Reboot Wake On LAN</li> <li>System Service Aids</li> <li>System Service Aids</li> <li>System Configuration</li> <li>Network Services</li> <li>Performance Setup</li> <li>On Demand Utilities</li> <li>Concurrent Maintenance</li> <li>Login Profile</li> </ul>	Power On/Off System         Current system power state: Off         Current firmware boot side: Temporary         Current system server firmware state: Not running         System boot speed: Fast ♥ ⑦         Firmware boot side for the next boot: Temporary ♥ ⑦         System operating mode: Normal ♥ ⑦         Boot to system server firmware: Standby ♥ ⑦         System power off policy: Automatic ♥ ⑦         Save settings ⑦
	Save settings and power on <sup>®</sup>

Figure 14-3 System power on and off options

#### 14.3.1 Power On/Off System

When you select this option, on the right hand side of the menu gives you the current system power state, Current firmware boot side, and system server firmware state. You can select the following boot options:

System boot speed: Select the speed for the next boot (*Fast* or *Slow*). Fast boot results in some diagnostic tests being skipped, and shorter memory tests being run during the boot. Slow boot will go through all diagnostic tests

and memory test. Normally you take this option if you are experiencing some system errors or when you have made some system changes for example CPU and Memory upgrades.

- Firmware boot side: Select the side from which the firmware will boot: permanent or temporary. When you upgrade your system firmware, typically, firmware updates are tested on the temporary side before being applied to the permanent side. So the temporary side should always have the latest firmware. The permanent side has the previous revision.
- System operating mode: Select the operating mode (Manual or Normal). Manual mode overrides various automatic power-on functions, such as auto-power restart, and enables the power button which allows you to select power options from the control panel. You can also set this option from the control panel.
- Boot to system server firmware: Select the state for the server firmware: Standby or Running. When the server is in the server firmware standby state, partitions can be set up and activated. The running option restarts your partitions automatically.
- System power off policy: Select the system power off policy. The system power off policy is a system parameter that controls the system's behavior when the last partition (or the only partition in the case of a system that is not managed by an HMC) is powered off. The choices are:
  - Power off: When the last partition is powered down, the system turns off.
  - Stay on: When the last system is powered down, the system stays on.
  - Automatic: Is the default setting, if the system is not partitioned, the system is turned off. If the system is partitioned, it stays on.

Make your selections and select Save settings and power on.

#### 14.3.2 Auto Power Restart

You can set your system to restart automatically. This function is useful when power is restored after an unexpected power line disturbance causes the system to shut down unexpectedly. Select either **Enable** or **Disable**. By default, the auto power restart value is set to *Disable*. In many cases, you might not want the system to restart automatically, unless you are reasonably certain that the power problem has been resolved.

#### 14.3.3 Immediate Power Off

You can power off the system quickly using the Immediate Power Off function. Typically this option is used when an emergency power off is needed. The operating system is not notified before the system is powered off.

**Attention:** To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system prior to performing an immediate power off

#### 14.3.4 System Reboot

You can reboot the system quickly using the reboot function. The operating system is not notified before the system is rebooted.

**Attention:** Rebooting the system shuts down all partitions immediately. To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system prior to performing a reboot.

## 14.4 System Service Aids

Figure 14-4 shows the System Service Aids menu. From this menu, you can:

- Display system error, event logs.
- Initiate a system dump.
- Initiate a service processor dump.
- Reset the service processor.
- Reset your system to the factory-shipped configuration settings.

System Service Aids
Error/Event Logs
Serial Port Snoop
System Dump
Service Processor Dump
Partition Dump
Serial Port Setup
Modem Configuration
Call-Home/Call-In Setup
Call-Home Test
Reset Service Processor
Factory Configuration

Figure 14-4 System Service Aids menu

The following features are not available when your system is connected to the HMC. These features are part of the Service Management on the HMC:

- Serial port snoop
- Partition dump
- Serial port set up
- Modem configuration
- Call home/call in setup
- Call home test

#### 14.4.1 Error/Event Logs

From the System Service Aids menu, select **Error/Event Logs**. You can view error and event logs that are generated by various service processor firmware components. The content of these logs can be useful in solving hardware or server firmware issues. You see a selection panel as shown in Figure 14-5.

E	Error/Event Logs											
LCD C COLOR		Error logs										
	F	Log ID	Time		Failing subsystem	Severity	SRC					
		50A55314 2007-05-11 16:11:12			Memory Controller	Predictive Error	B121E550					
				In	formational logs							
	F	Log ID	Time	Faili	ng subsystem	Severity	SRC					
		50243CCC	2007-05-14 16:35:56	CEC	Hardware Subsystem	Informational Event	B150CA01					
	50243CCA 2007-05-14 16:35:56				Hardware Subsystem	Informational Event	B150CA16					
		50243CCB	2007-05-14 16:35:56	Hardware Subsystem	Informational Event	B150CA02						

Figure 14-5 Error and event logs

Select the event log that you wish to view and scroll to the bottom of window to select **show details**. The details provide the description of the system reference code (src).

#### 14.4.2 System Dump

Use the System Dump procedure only under the direction of your service provider. You can initiate a system dump to capture overall system information, system processor state, hardware scan rings, caches, and other information. This information can be used to resolve a hardware or server firmware issue. A system dump can also be initiated automatically after a system malfunction, such as a checkstop or hang.

Select System Dump to open the window shown in Figure 14-6.



Figure 14-6 Capturing overall system information with System Dump

From this window, you set the following information:

Dump policy: Select the policy to determine when system dump data is collected. If you select Enable, the service processor (SP) collects system dump data only when the SP determines it is necessary, typically only when a specific failure has not been identified.

If you select **Disable**, the SP never collects any dump data, unless explicitly requested by the user.

The default is *Enabled*.

Hardware content: Select the policy to determine how much hardware data is collected for a system dump. If you select Automatic (default), the SP collects the hardware data that it determines is necessary, depending on the particular failure.

If you select **Maximum**, the SP collects the maximum amount of hardware data. Note that if you choose this selection, the collection of hardware data can be quite time consuming, especially for systems with a large number of processors.

Server firmware content: Select the policy to determine how much server firmware data is collected for a system dump. If you select Automatic, the SP collects the minimum amount of data necessary to debug server firmware failures. Automatic is the default policy. In some cases, your support engineer might want you to override the default policy.

If you select **Physical I/O**, the SP collects the minimum firmware data plus the firmware data associated with physical I/O operations.

If you select **Virtual I/O**, the SP collects the minimum firmware data plus the firmware data that is associated with I/O operations that do not involve physical I/O devices.

If you select **High performance switch HPS Cluster**, the SP collects the minimum firmware data plus the firmware data that is associated with high performance switch operations between this server and other servers in the cluster.

If you select **HCA I/O**, the SP collects the minimum firmware data plus the firmware data associated with the host channel adapter I/O operations.

If you select **Maximum**, the SP collects the maximum amount of server firmware data.

Make your selections and click Save settings.

#### 14.4.3 Service Processor Dump

You use the Service Process Dump option to enable or disable the service processor dump function. The default value is *Enabled*. A service processor dump captures error data after a service processor failure, or upon user request. User request for service processor dump is not available when this policy is set to disabled

The save settings and initiate dump button is visible only when an SP dump is allowed (that is, when SP dumps are enabled and the previous SP dump data has been retrieved). Press this button to initiate an SP dump.

#### 14.4.4 Reset Service Processor

Typically, rebooting of the SP is done only when instructed by IBM service personnel (Figure 14-7).

Reset Service Processor
Continuing will result in the rebooting of the Service Processor. Current sessions, including hardware management console (HMC) connections, will be terminated.
Continue

Figure 14-7 Reset service processor

This function is not available if your system is turn on. Clicking **Continue** causes the service processor to reboot. Because the service processor reboots, your ASMI session is dropped, and you have to reconnect your session to continue.

#### 14.4.5 Factory Configuration

Use this procedure only under the direction of your IBM service personnel (Figure 14-8 on page 437).

In critical systems situations, you can restore your system to the factory default settings. Doing so results in the loss of all system settings (such as the HMC access and ASMI passwords, time of day, network configuration, and hardware deconfiguration policies) that you have to set again through the service processor interfaces. Also, you lose the system error logs and partition-related information.

**Important:** Before continuing with this operation, make sure you have manually recorded all settings that need to be preserved.

Factory Co	nfiguration
• Reset all	settings
O Reset ser	vice processor settings
O Reset ser	ver firmware settings
O Reset PC	I bus configuration
Continuing wit	ill result in the loss of system settings that you may have set via user interfaces. Before th this operation make sure you have manually recorded all settings that need to be preserved
Continue	0

Figure 14-8 Factory configuration reset

In this window, you have the following options:

- Reset all settings: Resets everything. It is a combination of all the others. To complete this operation, the system will be powered on and then off, and the service processor will be reset.
- Reset service processor settings: Resets the settings of the service processor that include passwords, network addresses, time of day, hardware configuration policies, and so forth. Any sessions currently active in the network interfaces will be disconnected, and the service processor will be reset.
- Reset server firmware settings: Resets the firmware settings only. Partition data will be lost.
- Reset PCI bus configuration: Resets the PCI bus and the firmware settings. To complete this operation, the system is turned on and then off.

Make the appropriate selection and then select Continue.

## 14.5 System Information

The System Information menu gives you the following options (Figure 14-9):

- Display vital product data.
- ► Perform an SPCN power control network trace and display the results.
- Display the previous boot indicator.
- Display the progress indicator history.
- Display the Real-time Progress Indicator



Figure 14-9 System Information menu

#### 14.5.1 Vital Product Data

Select **Vital Product Data** to view manufacturer's vital product data (VPD) that is stored from the system boot prior to the one in progress now (Figure 14-10).



Figure 14-10 Display details of VPD

If you want to view only selected manufacturer's VPD, such as serial numbers and part numbers, select the feature that you want to vies and select **Display details**.

Vital Product Data										
Build name: fips310/b0313a_0711.310										
System brand: P0										
System serial number: 10FFE0B										
Machine	type-model: 9	117-MMA								
FRU ID	Part number	Serial number	FRU number	CCIN	RID	Location code				
EV	42R7352	YL3126355GF3	42R7352	293B	0x1e00	U789D.001.DQDVWZK				
EI	42R7352	YL3126355GF3	42R7352	293B	0xa200	U789D.001.DQDVWZK				
BP	42R7352	YL3126355GF3	42R7352	293B	0x800	U789D.001.DQDVWZK-P1				
CU	42R7352	YL3126355GF3	42R7352	293B	0x2900	U789D.001.DQDVWZK-P1-T1				
CU	42R7352	YL3126355GF3	42R7352	293B	0x2901	U789D.001.DQDVWZK-P1-T2				
P2	42R7352	YL3126355GF3	42R7352	293B	0x4300	U789D.001.DQDVWZK-P1				
P5	42R7352	YL3126355GF3	42R7352	293B	0x3700	U789D.001.DQDVWZK-P1				
PI	42R7352	YL3126355GF3	42R7352	293B	0x3600	U789D.001.DQDVWZK-P1				

To view details of all the features, select **Display all details** to open the display shown in Figure 14-11.

Figure 14-11 Display all VPD detail

#### 14.5.2 Power Control Network Trace

You can perform a system power control network (SPCN) trace and display the results. This information is gathered to provide additional debug information when working with your hardware service provider.

**Note:** Producing a trace can take an extended amount of time based upon your system type and configuration. This is a normal delay due to the amount of time the system requires to query the data.

#### 14.5.3 Previous Boot Progress Indicator

You can display the previous boot progress indicator that was displayed in the control panel during the previous failed boot by selecting this option. During a successful boot, the previous progress indicator is cleared. If this option is selected after a successful boot, nothing is displayed.

The progress indicator information is stored in nonvolatile memory. If the system is powered off using the power-on button on the control panel, this information is retained. If the ac power is disconnected from the system, this information is lost.

#### 14.5.4 Progress Indicator History

With this option, you can review the progress of codes that displays in the control panel during the previous boot. The codes display in reverse chronological order, as shown in Figure 14-12. (The first entry seen is the most recent entry.) This information is gathered to provide additional debug information when working with your hardware service provider.

	Progress Indicator	Time				
]	C1001FFF	2007-05-14 23:52:54				
C1001F0F		2007-05-14 23:51:29				
]	C1001F00	2007-05-14 23:50:53				

Figure 14-12 Progress Indicator History

	C1001FFF
Created at :	2007-05-14 23:52:54
SRC Version :	0x02
Virtual Progress SRC :	False
15/OS Service Event Bit :	False
Hypervisor Dump Initiated :	False
Power Control Net Fault :	False
Additional Sections :	Disabled
Hex Word Count :	9
Error Status Flags :	None declared
Module Id :	0x00
Reference Code :	C1001FFF
Hex Words 2 - 5 :	000000F0 00000000 C1001FFF 00000000
Hex Words 6 - 9 :	0000000 0000000 0000000 0000000

Select the code that you want to display and select show details. Figure 14-13 shows the details of the code.

Figure 14-13 Details of the Progress Indicator History code

#### 14.5.5 Real-time Progress Indicator

You can view the progress and error codes that currently display on the control panel. Viewing progress and error codes is useful when diagnosing boot-related issues. To perform this operation, your authority level must be one of the following possibilities:

- General
- Administrator
- Authorized service provider

Select this option to open the window shown in Figure 14-14. This window shows the real-time progress of the system and displays what you have on the systems display.

C700406E	
	294×95

Figure 14-14 Real-time Progress Indicator

# 14.6 System Configuration

Figure 14-15 shows the expanded System Configuration menu. Using this menu, you can:

- Change the system name.
- ► Configure I/O Enclosure.
- Change the time of day.
- Establish the firmware update policy.
- ► Establish the Detailed PCI error injection policies.
- Change the Interposer Plug Count.
- ► Enable I/O Adapter Enlarged Capacity.
- ► View Hardware management Consoles connection.
- Change floating point unit commutation test values.

System Configuration
System Name
Configure I/O Enclosures
Time Of Day
Firmware Update Policy
PCI Error Injection Policy
Interposer Plug Count
I/O Adapter Enlarged Capacity
Hardware Management Consoles
Virtual Ethernet Switches
Floating Point Unit Computation Test
Hardware Deconfiguration
Program Vital Product Data
Service Indicators

Figure 14-15 System Configuration menu

#### 14.6.1 System Name

From the System Configuration menu, you can select the system name option to display the current system name and change the system name if you choose to do so. The system name is a value used to identify the system or server. The system name might not be blank and might not be longer than 31 characters. To change the system name, enter a new value and click **Save settings**.

System Name	
System Name: 9117-MMA-SN10FFE0B-L9	0
Save settings	

Figure 14-16 System Name

This example shows changes the system name. The valid characters are [a-Z], [0-9], hyphen (-), underscore (\_), and period (.).

The system is shipped with the default system name initialized to a 31 character value as follows (Server-*tttt-mmm*-SN000000). In this default system name:

- ► *tttt* = Machine type
- mmm = Model number
- ► 0000000 = Serial number

#### 14.6.2 Configure I/O Enclosures

This function normally is used by your hardware service provider. After the server firmware has reached the *standby* state, you can configure I/O enclosure attributes as follows:

- Display the status, location code, rack address, unit address, power control network identifier, and the machine type and model of each enclosure in the system.
- Change the identification indicator state on each enclosure to on (identify) or off.
- Update the power control network identifier, enclosure serial number, and the machine type and model of each enclosure.

- Change the identification indicator state of the SPCN firmware in an enclosure to *enable* or *disable*.
- ► Remove rack and unit addresses for all inactive enclosures in the system.

When you select this option, the window shown in Figure 14-17 opens.

Configure I/O Enclosures										
Enclosure Configuration										
	Status	Rack address	Unit address	Power Control Network Identifier	Power Control Network Firmware Update Status	Power Control Network Firmware Version	Start Time	Type - Model	Serial number	Location code
0	Active	0x3C00	0x1	0xE0	Not Applicable			789D- 001	DQDVWZK	U789D.001.DQDVWZK
Identify enclosure ⑦										
	Change settings ⑦									
	Collect	SPCN IO	Trace	0						

Figure 14-17 Configure I/O Enclosures

In this window, you have the following options:

- Identify enclosure: Turns on the indicator on the selected enclosure. Led flashes to identify the enclosure.
- ► Turn off indicator: Turns off the indicator on the selected enclosure.
- Change settings: Changes the settings for the selected enclosure. The next page displays options for changing configuration ID, machine type-model, and serial number.
  - Power Control Network Identifier: Enter a hexadecimal number for the power control network identifier.

**Note:** The system server firmware must be in *standby* state or the expansion unit must be turned off when this operation is performed.

 Type - Model: Enter the enclosure machine type and model in the form *TTTT-MMM*:

*TTTT*: The four characters of the enclosure machine type.

MMM : The three characters of the enclosure model.

The enclosure machine type cannot be 0000. All alphanumeric characters are valid.

- Serial number: Enter seven characters for the enclosure serial number. All alphanumeric characters except o, i, and q are valid. All lowercase letters are converted to uppercase letters.
- ► Collect SPCN I/O Trace: Displays SPCN I/O trace for selected enclosure.

**Note:** The remaining options described here do not display in Figure 14-17 because that screen capture is a partial screen capture of the Configure I/O Enclosure panel.

- Clear inactive enclosures: Clears the rack and unit addresses of all inactive enclosures.
- Start SPCN Firmware Update : Starts pending SPCN firmware downloads if allowed by the SPCN firmware update policy. SPCN firmware downloads cannot all be attempted at the same time, some downloads can remain in a pending state before starting while others complete. Starting SPCN downloads is done asynchronously and can be monitored using the table above showing the power control network firmware update status.
- Stop SPCN Firmware Update: Stops SPCN firmware downloads that are currently in progress. SPCN firmware downloads that are stopped will move to a pending state. These SPCN firmware downloads can be restarted from the beginning either automatically by the system or by using Start SPCN Firmware Update, if allowed by the SPCN firmware update policy.

Stopping the SPCN downloads is done asynchronously and can be monitored showing the power control network firmware update status.

SPCN Firmware Update Policy: If *Disabled*, no SPCN firmware downloads will be allowed to start. Changing the SPCN firmware update policy to disabled will not impact SPCN firmware downloads currently in progress.

If *Enabled*, SPCN firmware downloads will only be allowed over the high speed link (HSL) interface. Changing the SPCN firmware update policy to enabled will not impact SPCN firmware downloads over the serial interface that are currently in progress.

Changing the SPCN firmware update policy setting to *Enabled* from *Disabled* will not automatically cause SPCN Firmware downloads over the HSL interface to begin immediately.

If *Expanded*, SPCN firmware downloads are allowed over both the HSL and serial interfaces. Changing to the SPCN firmware update policy to *expanded* will not cause SPCN firmware downloads to begin immediately.

#### 14.6.3 Time of Day

You can display and change the system's current date and time. This function is available if your system is turn on or off. When you select this option, the window shown in Figure 14-18 opens.

Power/Restart Control     System Service Aids     System Information     System Configuration     System Name     Configure I/O Enclosures     Time Of Day     Firmware Update Policy     PCI Error Injection Policy     Interposer Plug Count	Time Of Day         Date: 11       May         2007       ⑦         Time 0       03       29       UTC ⑦         Attention: Time must be entered in coordinated Universal Time (UTC         Save settings

Figure 14-18 Time of Day

From this window, you have the following options:

- Date: Enter the current date. Any change to the current date or time is applied to the service processor only, and is independent of any partition.
- Time: Enter the current time in Coordinated Universal Time (UTC) format. UTC is the current term for what was commonly referred to as Greenwich Meridian Time (GMT). Zero (0) hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal (or prime) meridian.

Universal time is based on a 24 hour clock. Local time is expressed as a positive or negative offset from UTC, depending on whether the local time zone is east or west of the prime meridian.

To convert local time to UTC, use 24 hour notation, then algebraically add the time zone offset to the local time. For instance, a user in the Central Daylight-savings Time zone (CDT) would add 5 hours (UTC offset -5 hours) to the local time to obtain the time in UTC. Example: 07:00 PM CDT equals 00:00 UTC.

Enter the date and time and select Save settings.

#### 14.6.4 Firmware Update Policy

This policy defines whether firmware updates are allowed from an operating system when the system is managed by a HMC. The default setting of this policy is to not allow firmware updates through the operating system. Note that this policy only takes effect when a system is HMC managed. When a system is not HMC-managed, firmware updates can only be made through the operating system, so this policy setting is ignored.

When this policy is set to allow firmware updates from the operating system, firmware updates from an HMC are not allowed, unless the system is turned off.

When a system is turned off, firmware updates can be performed from an HMC, regardless of the setting of this policy. However, care should be taken when updating firmware from both an HMC and the operating system.

When you select this option, the window shown in Figure 14-19 opens.

Firmware Update Policy				
Update Policy:	Hardware management console (HMC) 🗹 🕐			
	Hardware management console (HMC)			
Note: This polid Operating systemigurations. Some system configurations may				
cause the firmware to override this policy.				
When the system is powered off: Firmware update is possible only from the HMC.				
When the operating system is running: Firmware update is allowed only from the HMC.				
Save setting:	3			

Figure 14-19 Firmware Update Policy

#### 14.6.5 PCI Error Injection Policy

This option controls the PCI error injection policy. If enabled, utilities on the host operating system can inject PCI errors.

#### 14.6.6 I/O Adapter Enlarged Capacity

This option controls the size of PCI memory space allocated to each PCI slot. When enabled, selected PCI slots, including those in external I/O subsystems, receive the larger DMA and memory mapped address space. Some PCI adapters might require this additional DMA or memory space, per the adapter specification. This option increases system mainstore allocation to these selected PCI slots.

Enabling this option might result in some PCI host bridges and slots not being configured because the installed mainstore is insufficient to configure all installed PCI slots.

#### 14.6.7 Hardware Management Consoles

You can use this option to disconnect the HMC from your server. When you select this option, the window shown in Figure 14-20 opens.

	C	urrent HMC Connections	
F	Connection Id	Address ( IP )	State
	7310C03*10362EA	172.16.0.1	Connected

Figure 14-20 Hardware Management Consoles

Select the **Remove Connection** button.

#### 14.6.8 Virtual Ethernet Switches

To use this option, enter a number between 0 to 16 for Virtual Ethernet switches. This value controls the number of virtual Ethernet switches allocated by system server firmware. Most users leave this value set to its default of 0. A value of 0 enables the HMC to control the number of virtual Ethernet switches allocated by system server firmware.

For advanced configuration, this number can be set higher to cause system server firmware to create that many virtual Ethernet switches during platform power on, and disables the ability of the HMC to configure the number of virtual Ethernet switches.

If this is done, when a virtual Ethernet adapter is created using the HMC, the adapter will be connected to a particular virtual switch depending on the virtual slot number chosen during creation.

The adapter's virtual slot number will be divided by the number of virtual Ethernet switches, and the remainder of this division operation will be used to determine with which switch the adapter will be associated.

Each virtual Ethernet adapter will only be able to communicate with other virtual Ethernet adapters on the same virtual switch. For example, if the number of virtual Ethernet switches is set to 3, virtual Ethernet adapters in virtual slot 3, 6 and 9 are assigned to the same switch. A virtual Ethernet adapter in virtual slot 4 would be assigned to a different switch, and would not be able to communicate with the adapters in slots 3, 6, and 9.

#### 14.6.9 Floating Point Unit Computation Test

This option allows you to set the floating point unit test policy or to run the test immediately. You can set one of the following:

- > Disabled: Test never runs except when choosing to run the test immediately.
- Staggered: Test is run once on every processor in the platform over a 24 hour period. This is the default setting.
- Periodic: Test runs at specified time, sequentially through all processors in the system.

When choosing to run the test immediately, the current policy setting is overridden but not changed, and the test is executed sequentially on all the processors in the system. This feature is only available when the system is turned on.

#### 14.6.10 Hardware Deconfiguration

You can set various policies to deconfigure processors and memory in certain situations (Figure 14-21). *Deconfiguration* means that the resource is taken from a state of being available to the system, to a state of being unavailable to the system.

Deconfiguration Policies		
Deconfigure on predictive failure: Enabled 💌 🕐		
Deconfigure on functional failure: Enabled 💌 ?		
Deconfigure on system bus failure: Enabled 💌 🕐		
Save settings		

Figure 14-21 Deconfiguration Policies

From this window, you have the following options:

Deconfigure on predictive failure: Select the policy for deconfigure on predictive failures. This applies to run time or persistent boot time deconfiguration of processing unit resources or functions with predictive failures, such as correctable errors over the threshold.

If enabled, the particular resource or function affected by the failure is deconfigured.

Deconfigure on functional failure: Select the policy for deconfigure on functional failures. This applies to run time or persistent boot time deconfiguration of processing unit resources or functions with functional failures, such as checkstop errors or uncorrectable errors.

If enabled, the particular resource or function affected by the failure is deconfigured.

Deconfigure on system bus failure: Select the policy for deconfigure on system bus failures. Applies to run time or persistent boot time deconfiguration of processing unit resources or functions with system bus failures, such as check stop errors or uncorrectable errors.
This policy is not applicable for systems with one processing unit node. If enabled, the particular resource or function affected by the failure is deconfigured.

This applies to resource types such as processor, L2 cache, L3 cache, and memory.

#### **Processor deconfiguration**

In the event of a single processor failure, it might be possible to continue operating, with degraded performance, on fewer processors. You can use the panel shown in Figure 14-22 on page 452 to start the process of removing processors that might have failed or are beginning to generate errors. You can also see processors that might have become deconfigured due to some error condition that the system was able to detect and isolate.

All processor failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic dial-out for a service repair action. To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window can be found, processors with a failure history are marked *deconfigured* to prevent them from being configured on subsequent boots. Processors marked as deconfigured remain offline and will be omitted from the system configuration.

A processor is marked *deconfigured* under the following circumstances:

- If a processor fails built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- If a processor causes a machine check or check stop during run time, and the failure can be isolated specifically to that processor (as determined by the processor run-time diagnostics in the service processor firmware).
- If a processor reaches a threshold of recovered failures that results in a predictive call to the service provider (as determined by the processor run-time diagnostics in the service processor firmware).

The deconfiguration policy also provides the user with the option to manually deconfigure a processor or re-enable a previous manually deconfigured processor.

To begin the process, use a panel similar to the one shown in Figure 14-22. Select the processing unit with which you want to work (one or more processing units can be shown) and click **Continue**.

Fotal	system processors: 4			
Total	system configured pro	cessors: 2		
Total	system deconfigured p Processing unit	rocessors: 2 Total processors	Configured	Deconfigured

Figure 14-22 Processor Deconfiguration

Processing un	iit: 0			
Processor ID	Location code	State	Error type	Change settings
0	U789D.001.DQDVWZK-P2- C1	Configured	None (0)	Configured 🗸
1	U789D.001.DQDVWZK-P2- C1	Configured	None (0)	Configured 💌
2	U789D.001.DQDVWZK-P2- C2	Manually deconfigured	None (0)	Deconfigured 💙
3	U789D.001.DQDVWZK-P2- C2	System deconfigured	Predictive (E9)	Deconfigured 💙
		aeconingured	(E9)	<u>v</u>

Select the setting to configure or deconfigure for the processors and select **Save** settings.

Figure 14-23 Processor Deconfiguration window

#### Memory deconfiguration

Most System POWER6 systems will have several gigabytes (GB) of memory. Each memory bank contains two DIMMs (dual inline memory module). If the firmware detects a failure, or predictive failure, of a DIMM, it deconfigures the DIMM with the failure, as well as the other one. All memory failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic dial-out for a service repair action.

To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window can be found, memory banks with a failure history are marked *deconfigured* to prevent them from being configured on subsequent boots. Memory banks marked as deconfigured remain offline and will be omitted from the system configuration.

A memory bank is marked *deconfigured* under the following circumstances:

- If a memory bank fails built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- If a memory bank causes a machine check or check stop during run time, and the failure can be isolated specifically to that memory bank (as determined by the processor run-time diagnostics in the service processor firmware).
- If a memory bank reaches a threshold of recovered failures that results in a predictive call to the service provider (as determined by the processor run-time diagnostics in the service processor firmware).

The deconfiguration policy also provides the user with the option to manually deconfigure a memory bank or re-enable a previous manually deconfigured memory bank.

If you select **Memory Deconfiguration** from the **Hardware Configuration** menu, you see a panel similar to the one shown in Figure 14-24 which allows you to view the total memory installed on your system. From this panel, you can select the Processing Unit (one or more processing units can be shown). The reason you see processing unit is because the memory is installed on CPU board. Click **Continue** to advance to the next panel.

Memory Deconfiguration					
Total	system memory: 12288	MB			
Total	system configured memo	ory: 11776 MB			
Total	system deconfigured me	emory: 512 MB			
	Processing unit	Total memory	Configured	Deconfigured	
0	0	12288 MB	11776 MB	512 MB	
Cor	ıtinue				

Figure 14-24 Memory Deconfiguration

A new panel similar to the one shown in Figure 14-25 displays. You can then see any Memory Banks that might have become deconfigured due to some error condition that the system was able to detect and isolate. You can select either configured or deconfigured for each memory bank and select **Save settings**.

Memory Deconfiguration					
Processing u	mit: 0				
Memory dimm	Location code	Size	State	Error type	Change settings
0	U789D.001.DQDVWZK-P2- C1-C6	512 MB	Configured	None (0)	Configured 💌
1	U789D.001.DQDVWZK-P2- C1-C3	512 MB	Manually deconfigured	None (0)	Deconfigured 💌
2	U789D.001.DQDVWZK-P2- C1-C9	512 MB	Configured	None (0)	Configured 💌
3	U789D.001.DQDVWZK-P2- C1-C12	512 MB	Configured	None (0)	Configured 💌

Figure 14-25 Memory deconfiguration memory bank selection

#### 14.6.11 Program Vital Product Data

The ASMI allows you to program the system (VPD such as system brand, system identifiers, and system enclosure type (Figure 14-26). To access any of the VPD-related panels, your authority level must be administrator or authorized service provider.

**Note:** You cannot boot the system until valid values are entered for the system brand, system identifiers, and system enclosure type.



Figure 14-26 Program Vital Product Data

#### System Brand

Enter a two-character brand type. The first character must be one of the following:

- D IBM Storage
- I IBM System i
- N OEM IBM System i only
- O OEM IBM System p only
- P IBM System p

The second character is reserved. A value of zero means that there is no specific information associated with it. This entry is write once only, except in the case where it is all blanks, or when changing from a System p system to an IBM Storage system. Any other changes are disallowed. A valid value is required for the machine to boot. Additionally, for IBM Storage, each of the systems that constitutes the storage facility must have the first character set to D for storage to be accessible online.

#### System Keyword

You can set the system-unique ID, serial number, machine type, and machine model (Figure 14-27). If you do not know the system-unique ID, contact your next level of support.

System Keywords		
Machine type-model: 9117-MMA		
System serial number: 10FFE0B		
System unique ID: 0004AC0E8E24		
World Wide Port Name: C050760002ED		

Figure 14-27 System Keyword

#### **Machine type-model**

Enter a machine type and model in the form *TTTT-MMM*, where *TTTT* is the 4-character machine type and *MMM* is the 3-character model. A valid value is required for the machine to boot. Additionally, for storage to be accessible online, this value must match exactly both systems that constitute the storage facility. This entry is write once only.

#### System serial number

Enter a system serial number in the form *XXYYYYY*, where XX is the code for the plant of manufacture and *YYYYY* is the unit sequence number. Valid characters are 0 to 9 and A to Z. A valid value is required for the machine to boot. This entry is write once only.

#### System unique ID

Enter a system-unique serial number as 12 hexadecimal digits. The value should be unique to a given system anywhere in the world. A valid value is required for the machine to boot.

#### World wide port name

Enter a 16-digit hexadecimal number for the worldwide node name. This value is an IEEE-assigned 64-bit identifier for the storage facility. A valid value is required for the machine to boot. This entry is write once only.

#### System enclosure

When setting the system enclosure type, ensure that the enclosure serial number field matches the original value, which can be found on a label affixed to

the unit. Updating the enclosure serial field keeps the configuration and error information synchronized, and this information is used by the system when creating the location codes. This task must be done using the ASMI, not with the control panel. However, if you do not have access to the ASMI, the system will still operate without updating this information. See Figure 14-28.

System Enclosures
Enclosure location: U789D.001.DQDVWZK
Feature Code/Sequence Number: 789D-001
Enclosure serial number: DQDVWZK

Figure 14-28 System Enclosures

#### Feature code/sequence number

Enter a feature code and sequence number in the form *FFFF-SSS*, where *FFFF* is the 4-character feature and *SSS* is the 3-character sequence number. The Feature Code/Sequence Number is used to uniquely identify the type of the enclosure attached to the system. A valid value is required for the machine to boot. When this value is changed, the service processor reboots so that the location codes can be updated accordingly.

#### **Enclosure serial number**

Enter an enclosure serial number in the form *XXYYYYY*, where *XX* is the code for the plant of manufacture and *YYYYY* is the unit sequence number. Valid characters are 0 to 9 and A to Z. This serial number must be different from the serial number on the machine. A valid value is required for the machine to boot. When this value is changed, the service processor will reboot so that the location codes can be updated accordingly.

#### Service Indicators

From this menu you can turn off system attention indicator, enable enclosure indicators, change indicators by location code, and perform an LED test on the control panel.

The service indicators alert you that the system requires attention or service. It also provides a method for identifying a field-replaceable unit (FRU) or a specific enclosure within the system. A hierarchical relationship exists between FRU indicators and enclosure indicators. If any FRU indicator is in an identify state, then the corresponding enclosure indicator will change to an identify state

automatically. You cannot turn off the enclosure indicator until all FRU indicators within that enclosure are in an off state.



Figure 14-29 Service Indicators menu

#### System attention indicator

Click this button to turn off the system attention indicator. If the indicator is off, you cannot use this option to turn the system attention indicator on again. See Figure 14-30.

System Attention Indicator
Currently: On
Turn off the system attention indicator

Figure 14-30 System Attention Indicator

#### Enclosure indicators

You can turn on or off the identify indicators in each enclosure. An enclosure is a group of indicators. For example, a processing unit enclosure represents all of the indicators within the processing unit and an I/O enclosure represents all of the indicators within that I/O enclosure. Enclosures are listed by their location code. See Figure 14-31. Select the check box and select **Continue**.

Enclosure	Indicators	
OU789D.0	01.DQDVWZK	
Continue	0	

Figure 14-31 Enclosure Indicators

Select to off or identify as appropriate and select **Save settings**. Alternatively, select **Turn off all indicators** to reset the leds.

U789D.001.DQDVWZK-P2:	Off	~			
U789D.001.DQDVWZK-P3:	Off Identify				
U789D.001.DQDVWZK-P4:	Off	~			
U789D.001.DQDVWZK-E1:	Off	<b>~</b>			
U789D.001.DQDVWZK-E2:	Off	•			
U789D.001.DQDVWZK-A1:	Off	~			
U789D.001.DQDVWZK-A2:	Off	~			
U789D.001.DQDVWZK: Off					
Save settings					
Turn off all indicators	D				

Figure 14-32 Enclosure Identify window

#### Indicators by location code

You can specify the location code of any indicator to view or modify its current state. If you provide the wrong location code, the advanced system manager attempts to go to the next higher level of the location code. The next level is the base-level location code for that FRU. For example, a user types the location code for the FRU located on the second I/O slot of the third enclosure in the system. If the location code for the second I/O slot is incorrect (the FRU does not exist at this location), an attempt to set the indicator for the third enclosure is initiated. This process continues until a FRU is located or no other level is available.

#### Lamp test

You can perform an LED test on the control panel to determine if one of the LEDs is not functioning properly. Select **Lamp Test**. Click **Continue** to perform the lamp test. The test changes all indicators to the identify state for a short time (approximately 4 minutes).

# 14.7 Network Services

Use this menu option to configure the number and type of network interfaces according to the needs of your system (Figure 14-33). You can configure network interfaces on the system. The number and type of interfaces vary according to the specific needs of your system.



Figure 14-33 Network Services menu

#### 14.7.1 Network Configuration

This operation can be performed when the system is turned on and off. Because network configuration changes occur immediately, existing network sessions, such as HMC connections, are stopped. If a firmware update is in progress, do not perform this operation. The new settings must be used to re-establish any network connections. Additional errors can also be logged if the system is turned on. See Figure 14-34.

Network Configuration				
i contra comparator				
Network in few and				
Configure this interface?				
MAC address: 00:14:5E:4F:10:EE				
Type of IP address: Dynamic 💌 🕐				
Host name: (2)				
Domain name:				
IP address: 192.168.255.253				
Subnet mask: 255.255.128.0 2				
Default gateway:				
IP address of first DNS server:				
IP address of second DNS server:				
IP address of third DNS server:				

Figure 14-34 HMC Ethernet port configuration

From this window, you have the following options:

- Configure this interface: Configures this interface. If not selected, then the corresponding fields will be ignored.
- Type of IP address: Select the IP address type for this interface. If dynamic is selected, then network configuration data is obtained from the DHCP server. Typically your HMC is your DHCP server connected to FSP Ethernet port1.

• Host name: Enter a new value for the host name.

The valid characters are: hyphen (-) and period (.) , uppercase and lowercase alphabetics (A to Z and a to z), and numeric (0 to 9).

The first character must be alphabetic or numeric and the last character must not be a hyphen or a period. However, if the host name contains a period, then the preceding characters must have an alphabetic character. This input is required for the static type of IP address.

- Domain name: Enter a new value for the domain name. All alphanumeric characters and the symbols hyphen (-), underscore (\_), and period (.) are valid.
- ► **IP address**: Enter a new value for the IP address. This input is required for the static IP address type.
- Subnet mask: Enter a new value for the subnet mask. This input is required for the static IP address type.
- **Default gateway**: Enter a new value for the default gateway.
- ► IP address of first DNS server: Enter a new value for the first DNS server.
- IP address of second DNS server: Enter a new value for the second DNS server.
- ► IP address of third DNS server: Enter a new value for the third DNS server.
- Reset Network Configuration: Resets the Network Configuration settings to their default factory settings.
- Network Configuration: Select service processor to be configured. The default is the current service processor

Selecting **Save Settings** causes the network configuration changes to be made and the service processor to be rebooted. As the service processor reboots, your ASMI session drops and you have to reconnect your session to continue. When you reconnect, you are then using the new settings.

#### 14.7.2 Network Access

When you configure network access, you specify which IP addresses can access the service processor. You can specify a list of allowed IP addresses and a list of denied IP addresses. See Figure 14-35.

**Note:** The allowed list takes priority over the denied list, and an empty denied list is ignored. *ALL* is not allowed in the denied list if the allowed list is empty

Network Access				
IP address: 192.168.255.122				
Allowed IP addresses ⑦	Denied IP addresses ⑦			
1.	1.			
2.	2.			
3.	3.			
4.	4.			
5.	5.			
6.	6.			
7.	7.			

Figure 14-35 Network Access

In this window, you have the following options:

 Allowed IP addresses: Enter up to 16 complete or partial IP addresses. A complete IP address contains all four octets.

A partial IP address has only 1, 2, or 3 octets, and must end in a period. If a login is received from an IP address which matches a complete or partial IP address in the allowed list, access to the service processor is granted.

To allow access to the service processor from any IP address, enter ALL in the allowed list. An empty allowed list is ignored and access is granted from any IP address.

 Denied IP addresses: Enter up to 16 complete or partial IP addresses to be denied. Access to the service processor is not allowed if a login is received from an IP address listed in this list.

To deny access from any IP address, enter ALL in the list. If an incorrect IP address is entered in the allowed list and the denied list contains ALL, access to the service processor can be permanently denied. In this case, reset the network parameters by using the network reset parameters switch on the service processor card. Note that an empty denied list is ignored and the allowed list takes priority over the denied list. For these reasons, ALL is not allowed in the denied list if the allowed list is empty.

## 14.8 Performance Setup

You might enhance the managed system performance by manually or automatically changing the logical memory block size. The system kernel uses the memory block size to read and write files. By default, the logical memory block size is set to Automatic. This setting allows the system to set the logical block memory size based on the physical memory available. You can also manually change the logical memory block size. See Figure 14-36.



Figure 14-36 Performance Setup

To select a reasonable logical block size for your system, consider both the performance desired and the physical memory size. Use the following guidelines when selecting logical block sizes:

- On systems with a small amount of memory installed (2 GB or less), a large logical memory block size results in the firmware consuming an excessive amount of memory. Firmware must consume at least 1 logical memory block. As a general rule, select the logical memory block size to be no greater than 1/8th the size of the system's physical memory.
- On systems with a large amount of memory installed, small logical memory block sizes result in a large number of logical memory blocks. Because each logical memory block must be managed during boot, a large number of logical memory blocks can cause boot performance problems. As a general rule, limit the number of logical memory blocks to 8 K or less.

**Note:** The logical memory block size can be changed at run time, but the change does not take effect until the system is restarted

Select **Logical Memory Block Size**. select the logical memory block size and click **Save settings**.

#### 14.8.1 System Memory Page Setup

Improve your system performance by setting up the system with larger memory pages. You can improve your system performance by setting up the system with larger memory pages. Performance improvements vary depending on the applications running on your system. Only change this setting if advised by service and support.

To change the system memory page setup, select **System Memory Page Setup**. In the right pane, select the settings that you want, and then click **Save settings**.

### 14.9 On Demand Utilities

Activate inactive processors or inactive system memory without restarting your server or interrupting your business. Capacity on Demand (CoD) allows you to permanently activate inactive processors or inactive system memory without requiring you to restart your server or interrupt your business. You can also view information about your CoD resources.Important: Use this information if a hardware failure causes the system to lose its Capacity On Demand or Function On Demand purchased capabilities, and if there has never been an HMC

managing the system. If an HMC is managing the system, use the HMC to perform the following tasks instead of the ASMI.

**Important:** To decide whether you need Capacity on Demand, refer to Chapter 13, "Capacity on Demand" on page 373.

#### 14.9.1 CoD Order Information

After you determine that you want to permanently activate some or all of your inactive processors or memory, you must order one or more processor or memory activation features. You then enter the resulting processor or memory-activation key that is provided by your hardware provider to activate your inactive processors or memory.

To order processor or memory activation features select **On Demand Utilities**  $\rightarrow$  **Select CoD Order Information**. The server firmware displays the information that is necessary to order a Capacity on Demand activation feature. Record the information that is displayed and click **Continue**. See Figure 14-37.

	Advanced Syste	em Management
Log out User ID: ad	lmin	9117-MMA-SN10FFE0B-L9
<ul> <li>Expand all menus</li> <li>Collapse all menu</li> <li>Collapse all menu</li> <li>System Service</li> <li>System Informat</li> <li>System Configu</li> <li>Network Service</li> <li>Performance Set</li> <li>On Demand Uti</li> <li>CoD Order Info</li> <li>CoD Activation</li> <li>CoD Recovery</li> <li>CoD Recovery</li> <li>CoD Memory In</li> <li>CoD Capability</li> <li>Concurrent Main</li> <li>Login Profile</li> </ul>	s Control Aids tion uration es etup lities rmation formation normation Settings ntenance	CoD Order Information System type: 9117 System serial number: 10-FFE0B Card type: 52AD Card serial number: 00-6000396 Card ID: 7009121624337B79

Figure 14-37 CoD Order Information

#### 14.9.2 CoD Activation

To activate this feature click **On Demand Utilities**  $\rightarrow$  **CoD Activation**. Enter the activation key into the field and click **Continue** to perform the specified operation (Figure 14-38).



Figure 14-38 CoD Activation

#### 14.9.3 CoD Recovery

This process is to resume the booting process of the server firmware after the CoD activation keys are entered. Resuming the server firmware causes the CoD key to become recognized and the hardware to become activated. This option allows the server to complete the startup process that has been delayed up to one hour in order to place the server into the On Demand Recovery state that was needed to enter the CoD activation keys.

Select **On Demand Utilities**  $\rightarrow$  **CoD Recovery**. Enter the activation key into the field and click **Continue** to perform the specified operation (Figure 14-38).

#### 14.9.4 CoD Command

Select **On Demand Utilities**  $\rightarrow$  **CoD Recovery**. Enter the command into the field and click **Continue**.

#### 14.9.5 Viewing Information about CoD Resources

When CoD is activated on your system, you can view information about the CoD processors, the memory that is allocated as CoD memory, and Virtualization Engine<sup>™</sup> technology resources.

Select **On demand Utilities**. Then, select one of the following options for the type of information that you want to view:

- ► CoD Processor Information to view information about the CoD processors.
- ► CoD Memory Information to view information about available CoD memory.
- CoD Vet Information to view information about available Virtualization Engine technologies.
- CoD Capability Settings to view information about the CoD capabilities that are enabled.

# 14.10 Login Profile

In this section, we look at how to change passwords, view login audits, change the default language, and update the installed languages.

#### 14.10.1 Change Password

You can change the general user, administrator, and HMC access passwords. If you are a general user, you can change only your own password. If you are an administrator, you can change your password and the passwords for general user accounts. If you are an authorized service provider, you can change your password, the passwords for general and administrator user accounts, and the HMC access password.

Passwords can be any combination of up to 64 alphanumeric characters. The default password for the general user ID is general, and the default password for the administrator ID is admin. After your initial login to the ASMI and after the reset toggle jumpers are moved, the general user and administrator passwords must be changed. The HMC access password is usually set from the HMC during initial login. If you change this password using the ASMI, the change takes effect immediately.

**Note:** As a security measure, you are required to enter the current user's password into the Current password for current user field. This password is not the password for the user ID you want to change

To change the password, select Login Profile  $\rightarrow$  Change password. In the window that opens, enter the appropriate information and click Continue.

#### 14.10.2 Retrieve Login Audits

You can view the login history for the ASMI to see the last 20 successful logins and the last 20 logins that failed. To view login audit, Select Login Profile  $\rightarrow$  Retrieve Login Audits.

#### 14.10.3 Change Default Language

You can select the language that is displayed on the ASMI welcome window prior to login and during your ASMI session if you do not choose an alternative language at the time of login. You must provide all requested input in English-language characters regardless of the language selected to view the interface.

To change the default language, select Login Profile  $\rightarrow$  Change Default Language. Select the language and click Save Settings.

#### 14.10.4 Update Installed Languages

A maximum of five languages can be supported on the service processor at any given time. By default, English is always installed. Languages installation changes take effect when the firmware is updated. See Figure 14-39.

Update Installed Languages
Currently Installed Languages:
English
French
German
Italian
Spanish
Check which languages to install on next firmware update:
🗹 English
Portuguese
✓ French
🗹 German
🗹 Italian
Japanese
Korean
Simplified Chinese
Spanish
Traditional Chinese

Figure 14-39 Update Installed Languages

To select which language to install at the next firmware update, select **Login Profile**  $\rightarrow$  **update installed language**  $\rightarrow$  select five languages  $\rightarrow$  **Save Settings**.

#### 14.10.5 User Access Policy

This menu enables the admin user to grant or deny the access to service and development personnel by enabling or disabling dev, celogin, celogin1, and celogin2. Enabling access policy for celogin1 and celogin2 requires new passwords to be set even they have been set before.

To enable user access, select **Login Profile**  $\rightarrow$  **user access policy**. Then, select the user ID and policy setting and click **Continue**. Enter the admin password and new password for the user.

You have the following password options:

- Current password for user ID: As a security measure, the current password must be supplied.
- New password for user: Enter the new password for the user whose password you want to change.
- ► New password again: Enter the new password for the user again for verification.

# Α

# An example of backing up HMC Critical Console Data

You can back up Critical Console Data to a mounted remote system using the HMC option. This appendix provides an example of how to use this option.

### Using the HMC option to back up Critical Console Data

A Network File System (NFS) is the only supported file system for this HMC option. The IBM i5/OS has an NFS that can be used to save the HMC's Critical Console Data. The HMC uses standard NFS communications. The NFS uses UDP by default, not TCP/IP.

To ensure communications through the network, ports 111 and 2049 must be opened on all network equipment between the HMC and the IBM i5/OS partition for UDP. The NFS Server on i5/OS partition must be started and a directory should be created in the root file system then exported.

Perform the following steps to prepare back up critical console data to an IBM i5/OS partition:

1. Ensure that the NFS server is running on the i5/OS. To check whether NFS server is running, you can see if port 111 and 2049 are listening for UDP by enter the command **NETSTAT \*CNN** as shown in Figure A-1. The port name for port 111 is *sunprc*.

		Work with	TCP/IP Co	nn	ection Stat	us	
Tune	ontions, press	s Enter.				System	RCHAS60
	Enable debug	4=End 5=Die	nlau deta	i 1.	e 6=Dieab	le debug	
8-	Dienlau jobe	4-Ena 5-D13	prog acro		3 0-DI30D	te debag	
0-	bisping jobs						
	Remote	Remote	Local				
Opt	Address	Port	Port		Idle Time	State	
-	*	*	ftp-con	>	070:11:47	Listen	
_	*	*	telnet		000:01:05	Listen	
_	*	*	smtp		070:11:01	Listen	
_	*	*	89 .		070:11:42	Listen	
_	*	*	sunrpc		014:22:52	Listen	
_	*	*	sunrpc		014:43:04	*UDP	_
_	*	*	netbios	>	070:11:04	Listen	_
_	*	*	netbios	>	000:00:21	*UDP	
_	*	*	netbios	>	000:00:20	*UDP	
_	*	*	netbios	>	016:12:55	Listen	
_	*	*	snmp		000:02:35	*UDP	
_	*	*	ldap		015:40:53	Listen	
_							More
F3=E	xit F5=Refre	sh F9=Comman	d line	F1:	l=Display b	yte counts	F12=Cancel
F20=	Work with IPv6	connections	F22=Disp	la	y entire fi≀	ēld F24=Mor	e keys



- Work with TCP/IP Connection Status System: RCHAS60 Type options, press Enter. 3=Enable debug 4=End 5=Display details 6=Disable debug 8=Display jobs Remote Remote Local Idle Time 070:11:47 000:01:05 070:11:01 070:11:42 Opt Address Port Port State 21 23 25 Listen Listen \* \* \* \_ Listen \* \* \_ Listen 89 \* \* 014:22:52 014:43:04 070:11:04 \* \* 111 \*UDP Listen \* 111 137 ж \* ж \* 000:00:21 \*UDP 137 \* \* 138 000:00:20 \*UDP Listen \*UDP Listen 016:12:55 000:02:35 \* 139 \* ж \* 161 389 015:40:53 \_ More.. F3=Exit F5=Refresh F9=Command line F11=Display byte counts F12=Cancel F15=Subset F20=Work with IPv6 connections F24=More keys
- 2. You can check the port number by pressing F14 as shown in Figure A-2.

Figure A-2 Work with TCP/IP Connection Status - port number

3. Ensure that port 2049 is also available for UDP by scrolling down the page, as shown in Figure A-3.

1							
	_	Work Wit	th TCP/I	IP Connect:	ion Status		
						System:	RCHAS60
Tune	ontions. nres	s Enter.				_	
	Epable debug	4-End 5-F	lienlau	detaile	6-Disable	debug	
8-	Display iska	4-2110 3-2	rsprug	acturts	0-01300(C	acbag	
0-	Display jobs						
	Remote	Remote	Local				
Opt	Address	Port	Port	Idle Time	State		
	*	*	990	070:11:45	listen		
- 1	*	*	992	070.11.49	Listen		
- 1	*	*	2001	047.02.24	Listen		
I —	*	*	2001	047:03:34	Listen		
L _	*	*	2002	047:03:34	Listen		
_	*	*	2049	014:43:14	*UDP		
	*	*	2301	070:11:53	Listen		
	*	*	2809	070:10:00	Listen		
- 1	*	*	3000	070.11.54	Listen		
- 1			4444	070.10.22	Listen		
l —	*	*	4111	070:10:33	Listen		
l —	*	*	4620	070:09:31	Listen		
L _	*	*	4621	070:09:31	Listen		
	*	*	4625	070:09:29	Listen		
							More
E3=E	vit E5=Refre	sh E9=Com	and lir	e E11=Di	isnlau hute	- counts	E12=Cancel
E15-	Subset E20-W	onk with ID.	6 conne	actions F	2/1-Mone k		. 12 Sandet
113-	Subset 120-w	OIK WITH IFT		ections i	24-HOTE K	-ys	

Figure A-3 Work with TCP/IP Connection Status - next page

If the NFS server is not running, you can start the NFS server by typing the command QSYS/STRNFSSVR SERVER (\*ALL).

4. Creating and exporting a directory to be used for the back up in i5/OS partition. After the NFS server is started, a directory needs to be created and the exported to the NFS. Enter the command mkdir hmcdata to create the directory, and then confirm the directory was created by entering wrklnk as shown in Figure A-4.

	Work with	Object Links		
Directory / Type options, press Enter. 2=Edit 3=Copy 4=Remove	5=Disp	lay 7=Renam	° ne 8=Displaı	y attributes
11=Change current director	y			
Opt Object link bin dev etc fixes garymu hmcdata home lib logs	Type DIR DIR DIR DIR DIR DIR DIR DIR DIR	Attribute	Text	More
Parameters or command				<ul> <li>nore</li> </ul>
===>				
F3=Exit F4=Prompt F5=Ref F22=Display entire field	resh F9 F2	Retrieve F 3=More option	F12=Cancel f ns	17=Position to

Figure A-4 Work with Object Links

5. Make sure that for the directory, user \*public has read, write, and execute authority by typing option **9** (Work with Authority) for the directory, as shown in Figure A-5.

Object	Work	with Au /hmcda DIR ITSOAU *NONE *NONE	uthorit ata US01	ty.			
Type options, pres 1=Add user 2=C	ss Enter. Change user auth	ority	4=Remo	ove us	er		
Opt User A	DataObj Authority Exist	ect Autl Mgt i	horitie Alter	Ref			
_ *PUBLIC * _ ITSOAUS01 * _ QDIRSRV *	KRWX X KRWX X KX	××	x x	××			
Parameters or comm	nand						More
F3=Exit F4=Promp F11=Display detail (C) COPYRIGHT IBM	ot F5=Refresh l data authoriti CORP. 1980, 200	F9 es F1 5.	=Retrie 2=Cance	eve el F	24=More	keys	

Figure A-5 Work with Authority

 After the directory has been created, you can export the directory to the NFS by using IBM System i Navigator. In the System i Navigator window, open Network, then Servers, and then click TCP/IP. In the right pane, right-click NFS and select Exports as shown in Figure A-6.



Figure A-6 System i Navigator

7.	In the NFS	Exports	window,	click	ΟΚ	(Figure	A-7)	
•••				00	••••	(1 19010	,	•

NFS Exports - Rchas60.rchland.ibm.com							
Current exports:							
Directory	Anonymous User	Mapping					
/hmcdata	QNFSANON		New				
			Remove				
			Properties				
C List currently exported direct	ctories						
C List exports permanently de	fined in /etc/exports	Export All					
		ОК	Help				

Figure A-7 NFS Exports

- 8. Perform the HMC Back up Critical Console Data to a mounted file system by clicking **HMC Management**, and then **Back up HMC Data** in the HMC window.
- 9. Select **Back up to mounted remote system** in the Back up HMC Data window (Figure A-8) and then click **Next** to continue with next window.

🚰 https://9.3.5.231 - localhost: Back up HMC Data - Microsoft Internet Explorer 📃 🔲 🗙
Back up HMC Data
You selected to back up critical data for the Hardware Management Console (HMC). Select an archive option and click Next.
Critical data archive options O Back up to DVD on local system Sack up to mounted remote system O Send back up critical data to remote site
Next Cancel Help
🖉 Done

Figure A-8 Back up Critical Console Data

10.Enter the server name and the directory as shown in Figure A-9. Click **OK** to start HMC Back up Critical Console Data.

Back un Critical Data to Romoto Sustem								
Back up Gritical Data to Keniote System								
Type the information required to acce area to add information specific for th	ess the remote system. Use the description is archive. Click OK to back up the data.							
Remote server:	* myi5partition							
Resource:	* //hmcdata							
Filesystem type:	NFS							
Remote directory (optional):								
Other mount options:								
Description:								
OK Cancel Help								
E Done	📄 📄 🚔 💓 Internet 🏼 🏸							

Figure A-9 Back up Critical Data to Remote System

11. The Backup Critical Console Data Progress window displays as shown in Figure A-10. The backup can take several minutes to complete.

Bac	:kup Crit	ical C	onso	ole Dat	a Proar	ess	<b>^</b>
=1							
Elaps	;ed time:			00:00:	01		
The prog cons	backup o iress. Thi: iderable	f the H s opera amour	IMC c ation it of t	onsole may ta ime.	data is ir ke a	n	
DK	Details	Ca	ncel	Help			-
ど Done				<u>a</u>	Internet		

Figure A-10 Backup Critical Console Data Progress

You can also check the Backup Critical Console Data progress for the creation of the file by entering **wrklnk** on the 5250 console.

# В

# **Introduction to IBM Director**

IBM Director is an integrated, easy-to-use suite of tools that provide customers with flexible systems management capabilities to help realize maximum systems availability and lower IT costs.

This appendix provides an overview of the IBM Director for managing System p servers. It helps you to understand the specifics of IBM Director on System p platform and to decide if IBM Director is the best way to manage your environment.

## **Overview of IBM Director**

IBM Director is an integrated suite of tools that provides you with a system management solution for heterogeneous environments, including IBM System p environment. IBM Director works with the Hardware Management Console (HMC) to provide a comprehensive system management solution. With IBM Director, IT administrators can view and track the hardware configuration of remote systems in detail and monitor the usage and performance of critical components, such as processors, disks and memory.

IBM Director is provided at no additional charge for use on IBM systems.

Extensions to IBM Director are available for customers who want additional capabilities from a consistent, single point of management. IBM Director also complements and integrates with other popular systems management products using its upward integration modules.

For more information about IBM Director, refer to:

► IBM Director information on the Web:

http://www-03.ibm.com/servers/eserver/xseries/systems\_management/ ibm director/

- ▶ IBM Director on System p5, REDP-4219
- ► Implementing IBM Director 5.20, SG24-6188
IBM Director is designed to manage complex environments that contain a large number of servers. Figure 14-40 shows a sample environment that can be managed using IBM Director.



Figure 14-40 IBM Director environment

#### **IBM Director components**

IBM Director product consists of four components:

#### ► IBM Director Core Services

Systems that have IBM Director Core Services installed on them are referred to as Level-1. Level-1 control provides hardware specific functionality for IBM Director to communicate with and administer the managed system. IBM Director provides support for installing IBM Director Core Services on System p and System i servers and LPARs. You would not install it on an LPAR running the VIO Server.

#### ► IBM Director Agent

Systems that have IBM Director Agent installed on them are referred to as Level-2 managed systems. Level-2 provides enhanced functionality with which IBM Director can communicate with and administer the managed system. System p or System i systems and LPARs can have IBM Director Agents installed on them.

#### IBM Director Console

This is the graphical user interface for IBM Director Server from which the system administrator can perform tasks in IBM Director. This is automatically installed with the Director Server on System p, running AIX or Linux. The IBM Director console provides the same GUI, independently of the machine type and operating system.

#### IBM Director Service

This is the main component of IBM Director that contains the management repository and data, the server engine and the application logic. It provides all the management functions of IBM Director.

IBM Director can also manage systems on which no component of IBM Director is installed. Such managed systems are referred to as Level-0 managed systems. These systems must at minimum support either the Secure Shell (SSH) or Distributed Component Object Model (DCOM) protocol.

#### **IBM Director capabilities**

IBM Director provides a comprehensive suite of system management capabilities for managing System p and System i servers when the system management capabilities are enhanced with access to an HMC that is connected to the System p and System i servers. Management capabilities can vary depending on the operating system hosting the management server, the operating system of the managed system, and the agent level installed on it.

This section provides a list of the tasks available for a System p management server and the features available from a managed System p server.

#### **IBM Director Server Tasks**

**Note:** IBM Director management server tasks that are available are the same whether they are running on AIX or Linux on POWER.

When running in a System p server, almost all of the IBM Director Server tasks are available. The following list includes both core features and extensions:

 Base Director tasks available on System p server: Discovery, Associations, Group Management, System Status, Inventory, Event Log Viewer, Event Action Plan, Resource Monitor, Process Management, Remote Control, Remote Session, File Transfer, CIM Browser, SNMP Browser, Scheduler, Update Assistant, Microsoft Cluster Browser, Discovery preferences, Console preferences, Server preferences, User administration, Encryption administration, Message Browser, command line interface.

- ► Platform tasks available on System p server: Hardware/System Status. Hardware Control, Asset ID<sup>™</sup>, Configure SNMP Agent, Network Configuration, System Accounts.
- BladeCenter® tasks available on System p server: BladeCenter Configuration Wizard, BladeCenter Management C Module Launch, Switch Management Launch.
- ► IBM system x specific functions
  - Available on System p platform: Management Processor Assistant Launch, Configure Alert Standard Format.
  - Not Available on System p platform: ServeRAID<sup>™</sup> Manager.
- Other platform specific tasks available on System p platform: HMC Support, z/VM® Center Management.
- Advanced Server Tasks
  - Available on System p platform: Rack Manager, Software Distribution.
  - Not available on System p platform: Capacity Manager, System Availability, Remote Deployment Manager, Virtual Machine Manager.

#### **IBM Director Agent features**

Depending on the agent level, a System p managed system provides different features for management.

#### Agentless managed systems

A managed System p server on which no IBM Director component is installed is named as an agentless system or Level-0. An agentless managed system provides the following basic features:

- Discovery
- Remote session (requires ssh)
- Power control
- Promotion to Level-1 or Level-2 through Update Assistant

#### Agent Level-1 managed system

Managed systems that have IBM Director Core Services (but not IBM Director Agent) installed on them are referred to as Level-1. It provides hardware specific

functionality for IBM Director to communicate with and administer the managed system.

The IBM Director Core Services package installs on Linux:

- ► A Service Location Protocol (SLP) service agent.
- ► An Secure Sockets Layer (SSL) enabled CIMOM.
- An optional ssh server.
- ► Platform specific instrumentation.

IBM Director Core Services provide a subset of IBM Director Agent functionality. Level-1 Agent provides management entirely through standard protocols. You can perform the following tasks on a Level-1 managed system:

- ► All Level-0 functions.
- ► Collecting inventory.
- Promotion to Level-2 management by distributing the IBM Director Agent package.
- Managing events using event action plans, event subscription, and the event log.
- Monitoring hardware status.
- Running command line programs.
- ► Distributing system update packages through Software Distribution.

#### Agent Level-2 managed system

A managed system on which the IBM Director Agent is installed is referred to as Agent Level-2 managed system. It provides enhanced management functionalities, which vary depending on the operating system on which it is installed.

#### IBM Director extensions for System p

IBM Director extension are plug in modules which extend the capabilities of IBM Director:

- Install time extensions provided on the base IBM Director CD, installed along with IBM Director Server.
- Free extensions that available for download at no charge.
- ► Fee based extensions, product that require a license.

#### Install time extensions

Depending on the platform on which you install IBM Director Server, the installation package comes with different install time extensions, which are automatically installed with the server software.

When installing IBM Director Server on System p (AIX 5L or Linux), the installation package contains:

- Cluster System Management (CSM) hardware control utilities
- ► Flexible Service Provider
- Collection Services extensions
- ► IBM Director Agent
- ► ASMLIB
- ► System x<sup>TM</sup> extension
- BladeCenter extension
- ► IBM Director HMC common code extension
- ► IBM Director HMC console extension

# С

# Moving existing System i LPAR profiles to HMC

This appendix discusses how to migrate IBM System i LPAR profiles from a System i that does not have an HMC to a System i which is running logical partitions and is managed by an HMC. The HMC or IVM is required for any system i that is running logical partitions. The HMC or IVM creates and manages all LPAR configuration profiles.

#### Saving LPAR profiles using System i Navigator

This section discusses how to save System i LPAR profiles from a system that does not have a HMC by using System i Navigator. Follow these steps:

- 1. Load i5/OS V5R3 on all the logical partitions of the current system.
- 2. Do a complete system save of the current system.
- 3. Export the LPAR configuration:
  - a. Start an System i Navigator session and select the system that is partitioned as shown in Figure C-1.



Figure C-1 Starting System i Navigator

b. Click Configuration and Service as shown in Figure C-2.



Figure C-2 System i Navigator Panel

c. Select **Logical Partitions**, then right-click and select **Configure Partition** as shown in Figure C-3.



Figure C-3 System i Navigator Panel - Logical Partition

d. A list of partition configurations displays as shown in Figure C-4.



Figure C-4 System i Navigator Panel - Physical System

e. Right-click **Physical System** and select **Recovery**. Then select **Save All Configuration Data** as shown in Figure C-5.



Figure C-5 System i Navigator Panel

f. Enter a file name as shown in Figure C-6. The file should have been created prior to this step. You can browse for the file name as well. Click OK. The file is saved to the media of your choice. We recommend CD or diskette. The HMC uses either media.



Figure C-6 System i Navigator Save Configuration Data Panel

#### Importing LPAR profiles to HMC

This section describes how to import System i LPAR profiles that you have already saved before by using System i Navigator to an HMC using restricted shell. Using the restricted shell to finish this task requires the administrator to be logged onto the HMC locally. Follow these steps:

- 1. Complete the setup of the HMC.
- 2. Import or migrate the LPAR configurations to the HMC.

During the migration of the LPAR configurations, partition P0/Primary is reassigned the next available partition number, Pn+1. The Primary partition, as you know it today, no longer exists. The HMC is now used to manage the partitions.

To start the import process, a command is executed using the command line from an restricted shell terminal session at the HMC.

- 3. Perform the following steps to migrate the configuration data to the HMC:
  - a. Log on to the HMC with the default system administrator user ID *hscroot* with its password.
  - b. In the HMC workplace window, click **HMC Management** as shown in Figure C-7.

🖉 https://9.3.5.230 - localhost: Hardware Management Console Workplace (V7R310.0) - Microsoft Internet Expl 🖃 🗖 🔯		
Hardware Management	Console	hscroot   Help   Logoff
🔁 Welcom e	Welcome (HMC Version)	
⊞ Îi System s Managem ent	Use the Hardware Management Console (HMC) to manage this HMC as well as servers, logical partitions, managed systems, and other resources. Click on a link in the navigation pane at the left.	
System Plans	🗐 Systems Management	Manage servers, logical partitions, managed systems, and frames; set up, configure, view current status, troubleshoot, and apply solutions.
Xo Service Management	System Plans	Import, deploy, and manage system plans on the HMC.
💭 Updates	📕 HMC Management	Perform management tasks to set up, configure, and customize operations associated with this HMC.
	ង់ Service Management	Perform service tasks to create, customize and manage services associated with this HMC.
	🕅 Updates	Perform and manage updates on your system.
	Status Bar	View details of status and messages.
	Additional Resources	
	鬝 Guided Setup Wizard	Provides a step-by-step process to configure your HMC.
	HMC Operations Guide (View as HTML)	Provides an online version of Operations Guide for the Hardware Management Console and Managed Systems for system administrators and system operators using the HMC.
Status: Open Serviceable Events	66° HMC Readme	Provides hints and errata information about the HMC.
	Online Information	Additional related online information.
Applet com.ibm.hwmca.fw.servlet.taskcont	roller.applet.TaskControllerApplet started	🔒 🧶 Internet

Figure C-7 HMC Welcome Screen

Iocalhost: Hardware Management Console Workplace (V7R310.0) - Hardware Management Console			
E Welcom e			
	HMC Management (HMC Version)		
🗄 🏥 Systems Management	Operations		
System Plans	View HMC Events		
HMC Management	Shut Down or Restart		
¥8	Schedule Operations		
80 Service Management	Format Media		
	Back up HMC Data		
	Restore HMC Data		
	Save Upgrade Data		
	Change Network Settings		
	Change Network Settings		
	View Network Torology		
	Vew Network Topology		
	Tip of the Day		
	View Licenses		
	Change User Interface Settings		
	Change Date and Time		
	Launch Guided Setup Wizard		
	Administration		
	Change User Password		
	Change User Profiles and Access		
	Manage Task and Resource Roles		
	Manage Users and Tasks		
	Manage Certificates		
(	Remote Command Execution		
	Remote Virtual Terminal		
	Remote Operation		
Status: Open Serviceable Eve🏠	Change Language and Locale		
	Create Welcome Text		
	Manage Data Replication		

c. Then, Select Remote Virtual Terminal as shown in Figure C-8.

Figure C-8 HMC Management

d. A restricted shell terminal displays as shown in Figure C-9. You can enter the commands to start the migration process. Load your diskette or CD that contains your configuration data into your HMC drive. Then, enter the following command:

migrcfg -t 1 -m [system-name] -f [filename]



Figure C-9 Restricted Shell Terminal - Command

4. After the LPAR configurations are migrated as shown in Figure C-10, correct any resource reallocations resulting from P0/Primary being reassigned. Allocate new hardware resources as required. Validate the new Pn+1 partition (former primary) against the configuration and resource allocation documentation gathered in early steps.



Figure C-10 Example of i5 System

5. After all allocations have been made and partition profiles verified, the partitions can be activated. In both of the scenarios listed earlier, all partitions moved over intact.

As with any new install, migration, or upgrade, getting a backup of the new information is critical. Refer to 11.1, "Critical Console Data backup" on page 304.

# **Related publications**

We consider the publications that we list in this section particularly suitable for a more detailed discussion of the topics that we cover in this book.

#### **IBM Redbooks**

For information about ordering these publications, see "How to get IBM Redbooks publications" on page 507. Note that some of the documents that we reference here might be available in softcopy only.

- ► LPAR Simplification Tools Handbook, SG24-7231
- ► A Practical Guide for Resource Monitoring and Control (RMC), SG24-6615
- Advanced POWER Virtualization on IBM System p5: Introduction and Configuration, SG24-7940
- ► IBM System p Advanced POWER Virtualization Best Practices, REDP-4194
- Advanced POWER Virtualization on IBM System p5: Introduction and Configuration, SG24-7940
- ▶ IBM Director on System p5, REDP-4219
- ► Implementing IBM Director 5.20, SG24-6188

#### **Other publications**

This publication is also relevant as a further information source:

 Operations Guide for the Hardware Management Console and Managed Systems, SA76-0085

#### **Online resources**

These Web sites are also relevant as further information sources:

► Hardware Information Center

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp

HMC Support Web Site

http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html

Host Channel Adapter

http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?top ic=/iphae/iphaeinfinibandproducts.htm

man pages for the CLI

http://www14.software.ibm.com/webapp/set2/sas/f/hmc/power6/related/h
mc\_man\_7310.pdf

IBM Corporate site

http://www.ibm.com

Fix Level Recommendation Tool (FLRT)

https://www14.software.ibm.com/webapp/set2/flrt/home

Firmware downloads

http://www14.software.ibm.com/webapp/set2/firmware/gjsn

► IBM Electronic Support

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

- Contract requirements for On/Off CoD http://www-912.ibm.com/supporthome.nsf/document/28640809
- CoD Web site http://www-03.ibm.com/systems/p/cod/
- ► CoD activation codes

http://www-03.ibm.com/systems/p/cod/activation.html

► CoD requesting Trial activation

https://www-912.ibm.com/tcod\_reg.nsf/TrialCod?OpenForm

► IBM Director Home Page

http://www-03.ibm.com/servers/eserver/xseries/systems\_management/ibm
\_director/

#### How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

#### **Help from IBM**

IBM Support and downloads

ibm.com/support

**IBM Global Services** 

ibm.com/services

## Index

#### **Symbols**

/opt/hsc/data/sysplan 134

#### **Numerics**

7042-C06 4 7042-CR4 4 7310-C03 78 7310-C04 78 7310-C06 4 7310-CR2 70 7310-CR3 70 7310-CR4 4, 70

#### A

Activate 39 Additional HMC Users 86 Address Resolution Protocol (ARP) 211 Administrator mailing address 108 Advanced POWER Virtualization 262 Advanced System Management Interface, see ASMI Agreement for Service Programs 111 AIX 229 Allow an existing Internet connection for service 355 Allow Incoming 202 Allow local modem call answering 360 Allow pass-through systems for service 357 ambiguity 151 ASMI accessing with ASCII terminal 426 Activate Capacity on Demand 469 Autopower Restart 430 Change Default Language 471 Change Password 470 CoD Command 469 CoD Order Information 467 CoD Recovery 469 Configure I/O Enclosures 443 connecting with HMC 424 connection through Web browser 425 default IP addresses for service processors 425

Error/Event Logs 433 Factory Configuration Reset 436 Firmware Update Policy 447 Floating Point Unit Computation Test 449 Hardware deconfiguration 450 Hardware Management Consoles 448 I/O Adapter Enlarged Capacity 447 Immediate Power Off 431 login 426 Login Profile 470 Network Access 464 Network Configuration 462 Network Services menu 461 On Demand Utilities 466 PCI Error Injection Policy 447 Performance Setup 465 Power Control Network Trace 439 Power/Restart Control 429 Previous Boot Progress Indicator 439 Program Vital Product Data 456 Progress Indicator History 440 Real-time Progress Indicator 441 Reset Service Processor 436 Retrieve Login Audits 471 Service Processor Dump 435 System Configuration menu 442 System Dump 433 System Information 438 System Memory Page Setup 466 System Name 443 System Reboot 431 System Service Aids 432 Time of Day 446 Update Installed Languages 472 User Access Policy 472 Viewing Information about CoD Resources 470 Virtual Ethernet Switches 448 Vital Product Data 438 ASMI CoD interface 419 Automatic allocation 93 Available and installed I/O 27 Available and installed memory 27 Available and installed processors 27 Available Memory 25

Available Processing Units 24-25

#### В

Back up 53 Back Up Critical Console Data example 475 using NFS 475 Backup HMC Data 305 Barrier Synchronization Register (BSR) 13, 272 boot mode 245 BPA 217 BPC 217 connection status 57 replacing 304 Built-in self-test 451 Bulk Power Assembly (BPA) 46 status 48

#### С

C2T-to-KVM 72 Cabling 70 cage number 46 Call Home 340 Call home 337 Call Home Dump 347 Call-home 432 Call-home policy 432 Capacity BackUp (CBU) 384 Capacity on Demand, see CoD Capacity Upgrade on Demand 375 Central Electronic Complex 151 Certificate importing 184 restoring 184 Certificate Authority 180 Certificate Management 177 Change Network Settings 54 Change Password 31 Change the system name 442 Change the time of day 442 Change User Interface Settings 58 Change User Password 61, 185 CLI 171 chcod Utility Capacity on Demand changes 292 chhmc new options 297 chhwres

examples 299 HEA changes 274 shared pool usage of dedicated processor changes 283 chsvcevent new options 297 chsyscfg barrier synchronization register changes 286 examples 299 HEA changes 275 i5/OS changes 296 Partition availability priority changes 280 partition processor compatibility mode changes 291 shared pool usage of dedicated processor changes 282 chsysstate i5/OS changes 296 common usage examples 298 cpsysplan 171 defsysplanres system planning changes 288 deploysysplan (deploy system plan on a managed server) 171 dump system dump changes 289 lscod 376 Utility Capacity on Demand changes 292 Isdump system dump changes 288 Ishwres barrier synchronization register changes 287 examples 299 HEA changes 272 shared pool usage of dedicated processor changes 284 Islic new options 298 Islparutil shared pool usage of dedicated processor changes 284 Utility Capacity on Demand changes 294 lssyscfg 217, 298 barrier synchronization register changes 285 HEA changes 277 i5/OS changes 295

new options 297 Partition availability priority changes 278 partition processor compatibility mode changes 289 shared pool usage of dedicated processor changes 281 lssysconn 298 Issysplan (display list of system plans) 171 Issysplanres system planning changes 288 mksyscfg barrier synchronization register changes 286 examples 300 HEA changes 276 i5/OS changes 296 Partition availability priority changes 279 partition processor compatibility mode changes 290 shared pool usage of dedicated processor changes 281 mksysplan 171 new options 297 rmsyscfg examples 300 rmsysconn example 300 rmsysplan system planning changes 288 rmsysplan (delete a system plan) 171 rsthwres HEA changes 275 CLI commands updated with version 2 171 Cloning HMC Configurations 253 Close Event 341 close serviceable events 297 Cluster Systems Management (CSM) 312 CoD 39 activation codes 387 benefits 374 enhancements 14 entering enablement codes 395 Gathering Processor Information 391 managing On/Off CoD 406 managing Reserve CoD 402 managing Trial CoD 413 managing Utility CoD 396 permanent types requesting trial activation 390

server attributes 26 temporary types 377 Viewing Utility CoD usage 402 Web site 385 CoD Memory Capable 25 CoD Processor Capable 25 Command level interface 171 Concurrent install and activate 328 Concurrent install with deferred disruptive activate 328 Configurable Memory 25 Configurable Processing Units 25 Configure Connectivity to Your Service Provider 109 Configure Customizable Data Replication 66, 68 Configure DNS 103 Configure Domain Suffix 104 Configure HMC Firewall 99 Configure HMC Gateway 102 Configure HMC Network Settings 94 connected minutes 370 connection logical partition 196 managed system 196 remote users 196 service and support 196 connection monitoring 243 Connection status 57 Connections 34 disconnect Another HMC 35 reset or remove 35 Contact Address 107 Contact Information 108 Copy Dump to Media 347 Copy Dump to Remote System 347 Corrective Service 304 Create Event 333 Create Logical Partition 31 Create System Plan 141 create virtual adapter 240 Critical Console data 304 Critical Console Date (CCD) backup 304 CSM Highly Available Management Server (CSM-HA) 312 Custom groups 10 Customer Groups 22 Customizable Data Replication 64 Customize User Controls 190 Customized Data Replication 10

#### D

Data Replication 63 Date and Time 79, 83 change 59 Deconfigure on functional failure 450 Deconfigure on predictive failure 450 Deconfigure on system bus failure 450 dedicated capacity shared pool usage 220, 223 dedicated processor idle cycles 13 dedicated processor partition 236 dedicated processor sharing 224 Default Gateway 205 default password 19, 84 Delay the repair 339 Delete 42 Delete Dump 347 Deploy 152, 154, 165-166 Deploy System Plan 155 Deployment 153, 155, 161, 165, 167 Deployment examples 152 Desired memory 238 Desired processing units 233 Desired virtual processors 235 DHCP Client 201 DHCP Server 200 DHCP server 93, 130 DIAG DEFAULT 245 DIAG\_STORED 245 Diagnostic dial-out 453 Dial prefix values 114 Dial-up Number 117 DIMM 453 directory path for a sysplan 134 disconnected minutes 370 disconnected sessions 20 Discovered Console Information 68 Display the processing unit identifier 442 Disruptive install with activate 328 DLPAR 235 Memory 44 Physical Adapters 45 Processor 44 DNS server IP address 103 Domain 101 Domain suffix 104 Dump Retry 41 **DVD-RAM** formatting 53

Dynamic Logical Partitioning (DLPAR) 44

#### Ε

Electronic Service Agent 79, 123 Emergency power off 431 Enable Service Agent Connection Manager 371 Enabling hardware inventory collection from active partitions 142 Enclosure serial number 443, 458 Enforce strict password 187–188 Event log 433 Exception Trial CoD 378 Export System Plan 140

#### F

Factory-shipped configuration settings 432 Fast power off 29 FC 0962 5 Firewall 98 Firewall Settings 202 RMC 145 firmware managed systems 326 permanent side 328 Temporary side 328 Firmware components 433 firmware downloads 329 Firmware Update Policy 447 Firmware update policy 442 first power on 79 Fix Level Recommendation Tool (FLRT) 312 Format Media 53, 305, 344 Frames 22 change password 47 initialize 46 rebuild information 47 reset connections 49 System Management 45 FRU 338 FSP 217 connection status 57 replacing 304 ftp.software.ibm.com 319

#### G

General Parallel File System (GPFS) 312 GUI differences 9 Task bar 21 Guided Setup wizard 59, 79 checklist 80 launching 81

#### Η

HACMP/XD 384 hardware inventory enabling detailed retrieval 143 hardware inventory collection enabling 142 Hardware Management Console 133, 177 Hardware Management Console name 196 hardware validation during system plan deployment 151 High Availability Cluster Multi-processing (HACMP) 312 HMC 151 backup information 53 concepts 2 firewall settings 98 hardware validation - important note 151 identification 196 interface 3 predefined roles 4 rack mounted 4 viewing hardware details with a system plan 134 HMC code applying updates 320 downloading updates 316 updating from IBM FTP server 318 upgrading 320 HMC firmware maintenance 310 HMC Management 50 HMC Security management 178 HMC service data managing 344 HMC software version determining 311 HMC users 79 HMC Version 51 hmcsuperadmin 187 Host Channel Adapter 37 Host Ethernet Adapter 12, 220, 272 configuration 36

Host Name 101 hscroot 84 https //hmc\_hostname 178

#### I

I/O Units 46 i5/OS 272, 476 IBM Director 485-486 Agent Level-1 489 Agent Level-2 490 Agentless managed systems 489 capabilities 488 components 487 extensions 490 server tasks 488 IBM Director Agent features 489 IBM Electronic Service Agent Web site 123 IBM Electronic Services profile 363 IBM HACMP V5 384 IBM Systems Director 1 Identify LED 29 Import System Plan 138 Importing a system plan to the HMC 137 Importing LPAR Profiles 499 Inbound Connectivity 352 incident 370 Indicators by location code 461 InfiniBand 37 Initialize resetting all configuration data 249 initialize a frame 46 Initiate System Dump 346 initiating deployment using the HMC graphical interface 153 Install Corrective Service 319 Internet Secure Sockets Layer (SSL) 109 Internet Virtual Private Network (VPN 109 inventory scout 143 invscout 143 IOA 134 IOP 134 IP ranges 93

#### L

LAN adapter 89 configuration 198 Language 62 language 80 Launch Remote Hardware Management Console 60 LED Status 29 LED status 27 LHEA 12 Licensed Internal Code (LIC) 57 Linux 229 Local Area Network (LAN) adapters 198 Local Bridge 38 Local NIC 38 Locale 62 locale 80 Location code 443 Lock HMC Screen 59 log on 19 logical HEA 12 logical partitions creating 228 LPAR profiles moving 493 lssyscfg 57

#### Μ

Machine check 451 Machine type 443 Manage Attention LED 41 Manage Certificates 61, 178, 182 Manage Connection Monitoring 370 Manage Custom Groups 31, 43, 47 Manage customer information 361 Manage Data Replication 67 Manage Dumps 345 Manage eService Registration 363, 366 Manage Events 334 Manage inbound connectivity 359 manage partition data 247 Manage Problem Data 340 Manage Profiles 42 Manage Remote Connections 342 Manage remote connections 342 Manage Remote Support Reguests 343 Manage Serviceable Event Notification 368 Manage Systems Call-Home 352 Manage Tasks 61 Manage User Profiles 61 Manage User Profiles and Access 185 Manage Users 61 Managed Resource Roles 190–191

managed resources 22 managed system power off options 28 power on options 28 Managed System Dump 272 Managed Systems connecting to HMC 130 Master-to-subordinate replication 65, 67 Maximum memory 238 Maximum processing units 233 Maximum virtual processors 235 Memory deconfiguration 453 Minimum memory 238 Minimum processing units 233 Minimum virtual processors 234 mksysplan 146 Mobile CoD 15, 375 Model number 443 Modem Configuration 114 Modem configuration 353

#### Ν

network configuration 196 network interfaces viewing addresses 209 network routing information 204 network settings 88 Network Time Protocol (NTP) 59 Network Topology view 216 New Certificate 181 Node Status 57 node status 217 Nonroutable IP address ranges 93 Normal power off 29 Notification of Problem Events 124, 126

#### 0

Object Manager 178 Obtain an IP address automatically 201 Offload to Media 340 On/Off CoD 374, 378 Contract requirements 378 enablement codes 382 reporting requirements 381 On/Off CoD Memory State 25 On/Off CoD Processor State 25 Open 5250 Console 60 Open Restricted Shell Terminal 60 OPEN\_FIRMWARE 245 Outbound Connectivity 351

#### Ρ

parallel programming 13 partition automatic starting 243 Partition auto start 28, 132 Partition Availability Priority 13, 225, 272 Partition availability priority 220 partition availability priority 33 Partition communication 144 Partition Data Backup 250 manage 34 Partition Processor Compatibility Modes 272 Partition standby 28, 132 partition validation 152 partition validation during deployment 152 Partitions 22 Pass-Through System 120, 122, 356 password 19, 79, 84 change 27 changing 185 minimum length 19 PCI error injection policies 442 Peer-to-Peer Replication 65 Pending Authentication 131 performance management 349 Permanent Memory 25 Permanent Processors 25 Permanent side 328 Physical I/O 239 Ping Current Node 56 Ping Saved Node 56 Post Guided Setup tasks 130 Power control network identifier 443 POWER Hypervisor 260, 265 Power On/Off I/O Unit 47 POWER4 servers Service Agent focal point 371 POWER6 modes 11 POWER5 compatible 11 POWER6 Enhanced 11 POWER6 modes 11 Power-on self-test 451

Previous boot indicator 438 Private Network 91 private network 93, 200 Private or open network 80 processing units 232 Processor deconfiguration 451 processor enclosures (CEC) 151 profile data Backup priority 248 Delete 251 Full restore 248 Managed system priority 249 restoring 248 Profile name 230 Progress Code 10 Progress indicator history 438

#### R

Rack address 443 Rack-mounted 78 RAS enhancements 13 Rebuild 27. 30 recommended minimum fix levels 315 Recovery CD 304 ordering 316 Redbooks Web site 507 Contact us xv redundancy 8 redundant error path 243 redundant error path reporting 244 Redundant HMC configuration 254 Redundant HMC configurations 253 Redundant HMC considerations 256 Redundant Remote HMC 256 Reference Code 25, 336 Reference Code History 11 Remote Bridge 38 Remote Command Execution 62 remote connections securing 178 Remote Hardware Management Console 60 Remote NIC 38 Remote Operation 62 Remote Restore of Critical Data 54 remote support requests 342 Remote Virtual Terminal 62 Remove System Plan 150

Removing system plan on the HM 150 Repair actions 339 Request Service 334 Reserve Capacity 374 Reserve Capacity CoD 383 Reserve CoD Processor State 25 Reset the service processor 432 Reset your system 432 Resource Management and Control (RMC) firewall settings 146 Resource Monitoring and Control 142 Resource roles 61 ResourceLink 337, 339 Restart 40, 52 Dump 41 HMC 52 Operating System 41 Operating System Immediate 41 Restore Critical Console Data 309 Restore HMC Data 54, 309 Restricted shell 171 RIO cables 38 RIO Topology 38 RMC 142 role hmcoperator 193 hmcpe 193 hmcservicerep 193 hmcsuperadmin 193 hmcviewer 193 Viewer 188 root password 85 routed daemon 205 routing table viewing 210 Run-time diagnostics 451

#### S

Save Current Configuration 43 Save Upgrade Data 54, 322 Saved Topology 56 Schedule Operations 27, 42, 52, 307 Scheduled Operations 30 Selected deployment wizard action 163 Selected FRU 338 Self-signed certificate 180 Sequence Number 458 Serial number 443 Server processor 130 Server Security 178 Servers 22 Service Agent registration 80 Service data managing 344 Service events 333 Service Focal Point (SFP) 243 Service Indicators 458 service processor 79, 130 Service processor dump 432 Service Processor Status 34 Service processor's serial port 432 Service Provider 109 Serviceable event information 344 Session Preservation 19 Shared Ethernet Adapter 261 Shared Ethernet adapter 267 Shared Pool Usage of Dedicated Processor Capacity 272 Shared processors 231 Shut Down 40, 52 Delaved 40 Immediate 40 Operating System 40 Operating System Immediate 40 Signed by a Certificate Authority 180 SMS 245 SMTP 80, 113 **SPCN 439** SPCN power control network trace 438 ssh 62 SSL 178 configure 118 SSL Proxy 119 SSL proxy 355 Standard Trial CoD 378 startup 18 step 167 steps 164-165 Support Requests canceling 343 sysplan 10, 133-134 System Brand 456 System dump 432 System enclosure 457 System i Navigator 494 System Keyword 457 System Management Services 245

System p CoD Web site 385 system plan 134, 151 creating 141 deployment 150 exporting 139 failed deployment examples 157 functions 136 hardware validation 151 importing 137 partition errors examples 159 partition validation 151 removing 150 successful validation 160 validation 156 viewing 146 System Plan Viewer 163 System Planning 272 System Planning Tool 152 System Planning Tool (SPT) 10, 134 System Plans 31 HMC menu 136 System plans 134 CLI commands 171 System profile 28, 132 manage 33 System Reference Code (SRC) 10 Systems Call-Home 351

#### Т

Task Roles 190 TCP/IP sockets 212 Test LED 30 Test Network Connectivity 55, 206 Tip of the Day 57 Transmission Control Protocol (TCP) connections 213 Transmit Service Data to IBM 351 Transmit service information 349 Trial CoD 378 Trial CoD Processor State 25 two LAN adapters 89

#### U

Uncapped 234 uncapped weight 234 Unit address 443 Upgrade HMC Software 323 User adding 186 User Administration 177 User Datagram Protocol (UDP) statistics 214 User Management 184 Using the HMC graphical user interface 135 Utility Capacity 374 Utility Capacity on Demand (CoD) 272 Utility CoD 15, 383 Utility CoD Processor State 25 Utilization Data 27, 30

#### V

V6 to V7 upgrade 324 Validation 151, 157, 159-160 validation of hardware 151 View Guided Setup Wizard Log 129 View HMC Events 51 View Network Topology 55 View RIO Topology 49 View Shared Processor Utilization 401 View System Attention LED 29 View System Plan 142, 146 Viewing a system plan on the HMC 146 **VIOS 175** Virtual adapter creating 240 Virtual Ethernet 265 Virtual I/O 259 Virtual I/O Adapters 37 Virtual I/O Server 261 Virtual LAN(VLAN) 266 Virtual Private Network (VPN) 356 virtual processors 232, 234 Virtual SCSI 262 virtual SCSI adapter 262 adding 264 Vital product data 438 VLAN 38 VPD 344 VPD data collection 351 VPN 120

#### W

WebSM 9, 133, 179 Weight 234 Welcome Text 63 Work pane customizing 26 workload management groups 33



(1.0" spine) 0.875"<->1.498" 460 <-> 788 pages

# Hardware Management Console V7 Handbook



#### Discusses both POWER6 and POWER5 technologies

Documents the improved Remote Client Access

#### Describes the improved user interface

The IBM Hardware Management Console provides systems administrators a tool for planning, deploying, and managing IBM System p and IBM System i servers. This IBM Redbooks publication is designed for system administrators to use as a desk-side reference when managing partition-capable System i and System p servers using the HMC.

The major functions that the HMC provides are server hardware management and virtualization (partition) management.

In this book, we discuss how to:

- Configure the HMC
- Manage software levels on the HMC
- Use service functions on the HMC
- Update firmware of managed systems
- Move profiles from System i servers that previously did not connect to a HMC
- Use System Planning Tool deployments

In addition, we explain how to use the new HMC graphical user interface and the new HMC commands that are available with the HMC software Version 7, Release 3.

#### 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

SG24-7491-00

ISBN 0738486507