Hardware Management Console for pSeries Installation and Operations Guide

SA38-0590-07

Hardware Management Console for pSeries Installation and Operations Guide

SA38-0590-07

Eighth Edition (November 2003)

Before using this information and the product it supports, read the information in Appendix B, “Notices,” on page 197 and product warranties included with your system.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Information Development, Department H6DS-905-6C006, 11501 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

Contents

Safety Notices

A *caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury. *Caution* notices appear on the following pages:

- xii
- 9

For a translation of the safety notices contained in this book, see the *System Unit Safety Information*, order number SA23-2652.

Laser Safety Information

CAUTION:
This product may contain a CD-ROM, DVD-ROM, or laser module on a PCI card, which are class 1 laser products.
C30

Laser Compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with the IEC 825 (first edition 1984) as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
All mentioned laser modules are designed so that there is never any human access to laser radiation above a class 1 level during normal operation, user maintenance, or prescribed service conditions. Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. Only trained service personnel should perform the inspection or repair of optical fiber cable assemblies and receptacles.
C25, C26

Data Integrity and Verification

IBM computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the IBM support websites for updated information and fixes applicable to the system and related software.

About This Book

This book provides information to operators and system administrators about how to install and use an IBM Hardware Management Console for pSeries (HMC) to manage a system. This book includes information about the HMC software. It also discusses the issues associated with the planning and implementing of partitioning.

The following table describes the HMC code levels and the *Hardware Management Console Installation and Operations Guide* version that supports each code level.

HMC Release	**Hardware Management Console Installation and Operations Guide Form Number**
HMC Release 1 Version 1.0, 1.1 (First PTF), 1.2 (Second PTF)	SA38-0590-00
HMC Release 2 Version 1.0, 1.1 (First PTF), 1.2 (Second PTF)	SA38-0590-01
HMC Release 3 Version 1.0, 1.1 (First PTF), 1.2 (Second PTF)	SA38-0590-02
HMC Release 3 Version 2.0, 2.1 (First PTF), 2.2 (Second PTF)	SA38-0590-03 and later

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
Italics	Identifies parameters whose actual names or values are to be supplied by the user.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Accessing Information

Documentation for the IBM @server pSeries is available online. Visit the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base.

- To access the pSeries publications, click **Hardware documentation**.
- To view information about the accessibility features of @server pSeries hardware and the AIX operating system, click **AIX and pSeries accessibility**.

References to AIX Operating System

This document may contain references to the AIX operating system. If you are using another operating system, consult the appropriate documentation for that operating system.

This document may describe hardware features and functions. While the hardware supports them, the realization of these features and functions depends upon support from the operating system. AIX provides this support. If you are using another operating system, consult the appropriate documentation for that operating system regarding support for those features and functions.

Related Publications

The following publications contain related information:

- The documentation shipped with your managed system contains detailed planning, installation, and option information.
- The managed system's user's guide, which contains user information for the managed system connected to your HMC.
- The *AIX 5L Version 5.2 AIX Installation in a Partitioned Environment* guide, order number SC23-4382, contains information about installing, managing, and maintaining the AIX 5L operating system in a partitioned environment.
- The *Site and Hardware Planning Information*, order number SA38-0508, contains information to help you plan the installation of your machine.
- The @server *pSeries Electronic Service Agent for eServer pSeries User's Guide*, order number LCD4-1060, provides detailed information about the Service Agent application.
- The *Hardware Management Console for pSeries Maintenance Guide*, provides information about servicing your HMC, and includes diagnostic and error information.
- The *PCI Adapter Placement Reference*, order number SA38-0538, provides information about where to place an adapter in your managed system.
- The @server *pSeries Planning for Partitioned-System Operations* , order number SA38-0626, describes planning considerations for dynamic logical partitioning and Capacity Upgrade on Demand on products that can be partitioned.

Trademarks

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

- AIX
- AIX 5L
- @server
- IBM
- pSeries

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows NT, Windows 2000, and Windows XP are all registered trademarks of the Microsoft Corporation in the United States and other countries.

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

Chapter 1. Reference Materials

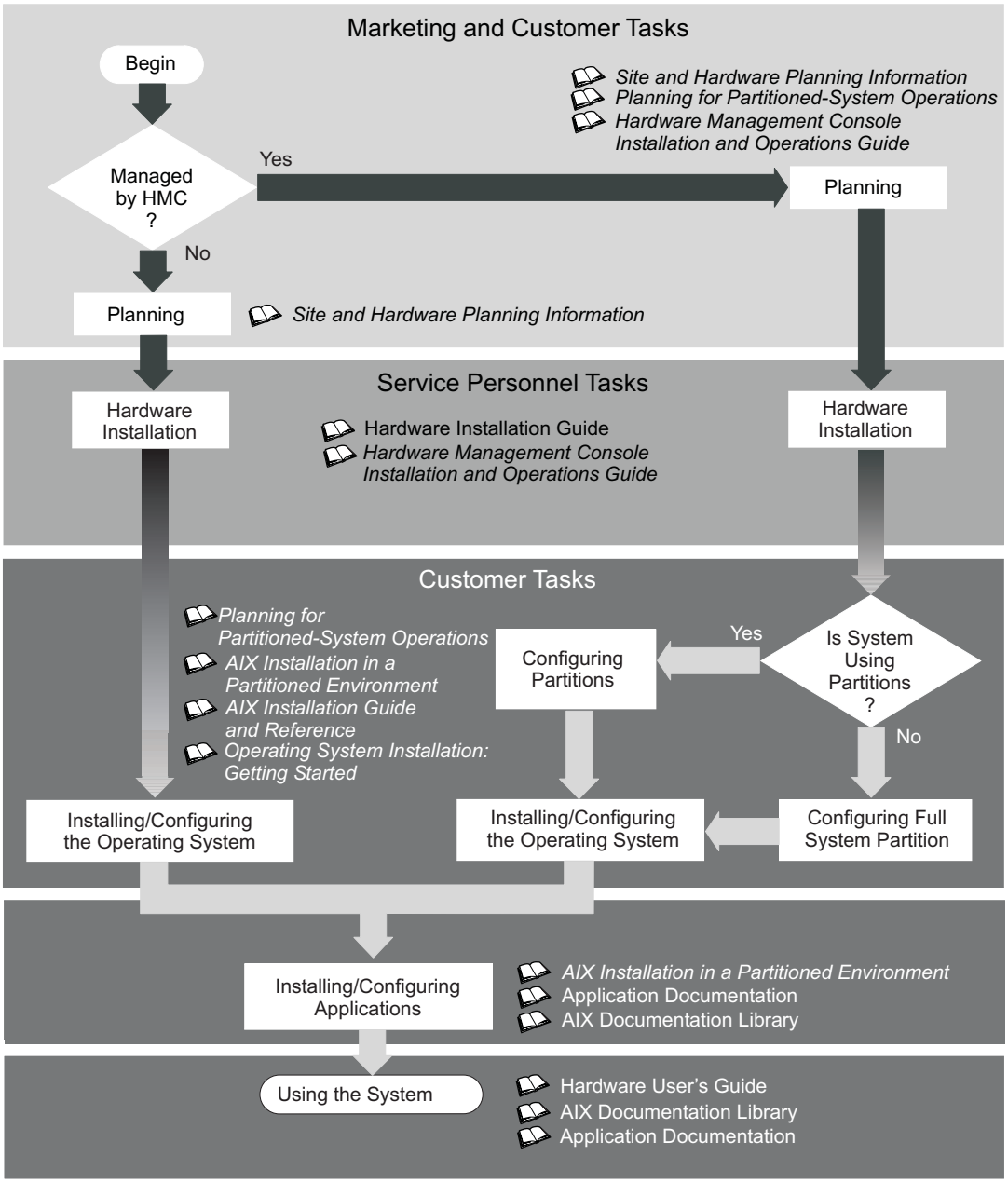
Note: This document may contain references to the AIX operating system. If you are using another operating system, consult the appropriate documentation for that operating system.

This document may describe hardware features and functions. While the hardware supports them, the implementation of these features and functions depends on support from the operating system. AIX provides this support. If you are using another operating system, consult the appropriate documentation for that operating system regarding support for those features and functions.

This chapter helps you get started with installing and configuring the @server pSeries environment. The following information is included in the chapter:

- @server pSeries Roadmap
- Documentation Overview - Brief description of the printed and softcopy documentation shipped including targeted audience

The @server pSeries Roadmap helps you locate marketing, service, and customer task information. The roadmap guides you through the tasks and the publications that document those tasks.



The publications listed in this section are available online. To access the online books, visit our IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base.

Documentation Overview

This section provides descriptions and target audience information for the @server pSeries and AIX 5L documentation libraries. Some of the documentation may only be available in printed form or in softcopy form. Based on the documentation content, the books are divided into the following categories: **Planning**, **Installing and Configuring**, and **Using the System**.

Table 1. Planning

Documentation Title	Description	Audience	Type
Site and Hardware Planning Information	Contains information to help plan for site preparation tasks, such as floor-planning, electrical needs, air conditioning, and other site-planning considerations.	Marketing, system administrators	softcopy
Planning for Partitioned-System Operations	Describes planning considerations for partitioned systems, including information on dynamic partitioning and Capacity Upgrade on Demand.	System administrators	printed and softcopy
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy

Table 2. Installing and Configuring

Documentation Title	Description	Audience	Type
Hardware Installation Guide	Provides information on how to install system hardware, cable the system, and verify operations.	System installer	printed and softcopy
Planning for Partitioned-System Operations	Describes planning considerations for partitioned systems, including information on dynamic partitioning and Capacity Upgrade on Demand.	System administrators	printed and softcopy
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy
AIX Installation in a Partitioned Environment	Provides information on how to install the AIX operating system in an LPAR environment.	System administrators	printed and softcopy
AIX Operating System Installation: Getting Started	Provides information on how to install and configure the AIX operating system on a standalone system using a CD-ROM device.	System administrators	printed and softcopy
AIX 5L Installation Guide and Reference	Provides information on installing the AIX 5L operating system on standalone systems, as well as on client systems using the Network Installation Management (NIM) interface.	System administrators	printed and softcopy
PCI Adapter Placement Reference	Outlines system-specific PCI adapter slot placement and adapter support configurations.	System administrators, service personnel	softcopy
AIX 5L Release Notes	Provides late-breaking information for a specific AIX release.	System administrators	printed and softcopy
AIX 5L Documentation CD	AIX documentation library (system management guides, user guides, application programmer guides, commands and files references, AIX man pages, and so on).	System administrators	softcopy

Table 3. Using the System

Documentation Title	Description	Audience	Type
Hardware Management Console for pSeries Installation and Operations Guide	Provides information on how to install, configure, and use a Hardware Management Console (HMC). Logical partition (LPAR) tasks, such as configuring and managing partitions on multiple host servers, are included.	System administrators	printed and softcopy
Hardware User's Guide	Provides using, problem determination, and service processor information.	System administrators	printed and softcopy
Diagnostic Information for Multiple Bus Systems	Combines operating instructions for hardware diagnostic programs with common MAPs and SRNs (Service Request Numbers).	Service personnel	printed and softcopy
PCI Adapter Placement Reference	Outlines system-specific PCI adapter slot placement and adapter support configurations.	System administrators, service personnel	printed
Hardware Management Console for pSeries Maintenance Guide	Contains MAPs, removal and replacement, error code, and parts information to help diagnose and repair the system.	Service personnel	printed and softcopy
Adapters, Devices, and Cable Information for Multiple Bus Systems	Provides information about adapters, devices, and cables that are attached to or used within the system.	System administrators	printed and softcopy
System Unit Safety Information	Contains the English version of safety notices, as well as translations of those safety notices into other languages.	System administrators, service personnel	printed and softcopy
AIX 5L Documentation CD	AIX documentation library (system management guides, user guides, application programmer guides, commands and files references, AIX man pages, and so on).	System administrators	softcopy

Chapter 2. Introducing the Hardware Management Console

The HMC uses its connection to one or more systems (referred to in this book as *managed systems*) to perform various functions, including the following:

- Creating and maintaining a multiple-partitioned environment
- Displaying a virtual operating system session terminal for each partition
- Displaying virtual operator panel values for each partition
- Detecting, reporting, and storing changes in hardware conditions
- Powering managed systems on and off
- Acting as a service focal point for service representatives to determine an appropriate service strategy and enable the Service Agent Call-Home capability
- Activating additional resources on demand

Managed System Operations

Partitioning provides users with the ability to configure a single computer into several independent systems. Each of these systems, called *partitions*, is capable of running applications in its own independent environment. This independent environment contains its own operating system, its own set of system processors, its own set of system memory, and its own I/O adapters.

The HMC allows you to perform many hardware management tasks for your managed system, including configuring logical partitions. You can choose to operate your managed system as a single server, or you can choose to run multiple partitions.

You can use the following types of partitioning: logical partitioning and the Full System Partition.

Partitioning

Logical partitioning has no limitations to the number of hardware resources that are contained in a partition. A partition could have any number of installed processors assigned to it, limited only by the total number of installed processors. Similarly, a partition could have any amount of memory, limited only by the total amount of memory installed. I/O adapters are physically installed in one of many I/O drawers in the system. However, with logical partitioning, any I/O adapter in any I/O drawer can be assigned to any partition.

Some systems have the ability to create affinity partitions. An *affinity partition* is a special type of logical partition, in that it has a close physical proximity to each of its resources. Hardware resources for affinity partitioning, with the exception of I/O, are defined by the HMC. When creating an affinity partition, the HMC automatically determines which system resources are to be grouped together and allows you to choose which type of grouping you want. The HMC then creates a profile for each affinity partition and a system profile that contains the affinity partitions for the managed system.

The operating system running in a partition is completely independent of any other operating system running in another partition. Operating system levels in each partition do not need to be the same, nor do the application levels.

By using partitions, for example, a company can test its program on one partition while developing the same program on another, all at the same time, all by using the same system. This ″same system″ partitioning method is more cost-effective, potentially eliminating the need for a separate test system.

For more information about partitions and their capabilities, see Chapter 4, “Partitioning,” on page 19.

Service Focal Point

Service representatives use the Service Focal Point application to start and end their service calls and provide them with event and diagnostic information. The HMC can also automatically notify service representatives of hardware failures by using a feature called *Service Agent*. You can configure the HMC to use Service Agent's call-home feature to send event information to your service representative.

The HMC must have a LAN connection to each partition (including the Full System Partition, if used) to collect partition errors. The HMC must also be connected to a modem and analog telephone line for the automatic notification process to function correctly.

The Service Focal Point application must be configured so that the proper information is sent. Also, whenever you make any changes to a system configuration, follow the guidelines in this book to ensure that changes are compatible with Service Focal Point. For more information about Service Focal Point, see Chapter 21, "Service Focal Point," on page 131.

Chapter 3. Installing and Configuring the HMC

This chapter contains information about installing the HMC and configuring the service software.

Note: The HMC parallel and audio ports are not supported and the diskette drive is not supported for use.

Installing the Hardware Management Console

To install your HMC, use the following procedure:

Step 1. Position the HMC and Monitor

CAUTION:
Follow handling precautions provided with the unit.

Position the HMC and monitor at or near their desired location, using the following guidelines:

- Use caution when lifting or moving the HMC.
- Use caution when lifting or moving the monitor.
- Leave enough space around the HMC to safely and easily complete the setup procedures.
- Be sure to maintain at least 51 mm (2 inches) of space on the sides of the system unit and 152 mm (6 inches) at the rear of the system unit to allow the system unit to cool properly. The front of the system requires a minimum of 76 mm (3 inches) of space. Blocking the air vents can cause overheating, which might result in a malfunction or permanent damage to the system unit.
- Place the HMC in a location where all necessary power outlets and network connections can safely be reached.
- Place the monitor in a stable and sturdy location.

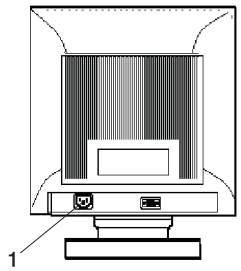
Step 2. Connect the Cables

Use the following steps to connect the cables to your HMC. Look for the small icons on the back of your HMC, which show where to attach the cables for the keyboard, mouse, and monitor.

Note: HMC is a closed management appliance, and as such, the HMC supports only the USB mouse and keyboard that is shipped with the HMC. No other USB devices are supported on the HMC via the extra USB ports. There is no specific requirement that the user must use a specific USB port for the keyboard and mouse. The HMC is shipped with all of the USB ports active. You cannot selectively disable these USB ports. Only 2 USB connectors are supported for a keyboard and mouse, which are mutually exclusive with a PS/2 keyboard and mouse.

1. Attach the monitor cable to the monitor connector, and tighten the screws.
2. If a label for the monitor was shipped with your system, attach the label to the bottom-right corner of the monitor.
3. Attach the power cord to the monitor (item 1 in the following illustration). If the HMC has a voltage switch, ensure that it is in the correct position for the supply voltage.

Attention: *Do not* plug the power cords into the electrical outlet at this point.



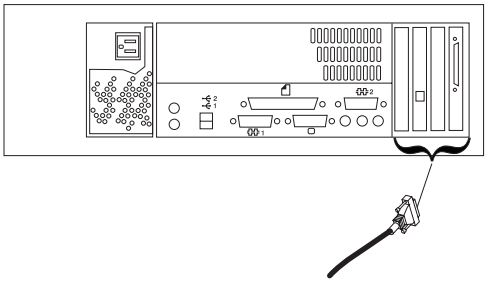
4. Connect the mouse and keyboard to their connectors.
5. Connect the HMC serial cable to the serial port on your managed system.

   Note: Serial port 2 is reserved for use with the modem.
   For two HMCs, connect the redundant HMC into the second serial port on your managed system. The part numbers for the HMC serial cables are as follows:

Part Number and Description	Position
Part Number 11P3955 6-m cable	9 Position to 9 Position
Part Number 11P3956 15-m cable	9 Position to 9 Position
Part Number 31L7196 15-m cable	9 Position to 25 Position

Step 3. Connect the 8-Port Adapter Cables

If you are using any optional 8-port adapters, connect the cables to the appropriate connectors in slots 1 through 4, as shown in the following illustration.



Step 4. Connect the External Modem

The external modem is used in conjunction with the HMC's Service Agent and Call Home features. To properly service your machine, it is important that you configure the Service Agent feature correctly the first time. For more information about configuring the modem and the Service Agent feature, see Chapter 20, "Service Agent," on page 123.

Note:

To connect the external HMC modem, do the following:

1. Connect the modem cable to the external HMC modem.
2. Connect the other end of the modem cable to serial port 2.
3. Connect the phone cable line port of the external modem.
4. Connect the other end of the phone cable to the analog jack on your wall.

Check the microswitch settings on the modem. The settings should be as follows:

Switch	Position	Function
1	Up	Force Data Terminal Ready (DTR)
2	Up	Hardware Flow Control (&E4)
3	Down	Result Codes Enabled
4	Down	Modem Emulation Disabled
5	*Down	Auto Answer Disabled
6	Up	Maximum Throughput Enabled
7	Up	Ready to Send (RTS) Normal Functions
8	Down	Enable Command Mode
9	Down	Remote Digital Loopback Test Enabled
10	Up	Dial-Up Line Enabled
11	Down	Asynchronous Terminal (AT) Responses Enabled (Extended Responses Enabled)
12	*Down	Asynchronous Operation
13	UP	28.8 KB Line Speed
14	Up	
15	Up	Carrier Detect (CD) and Data Set Ready (DSR) Normal Functions
16	Up	2-Wire Leased Line Enabled
Note: * Only switches 5 and 12 are changed from the factory default settings.		

Connecting the service modem the 7315-CR2

The Service Agent application defaults to using the second serial port on an HMC, the /dev/ttyS1 port. The 7315-CR2 does not have this serial port. To attach the modem to the 7315-CR2 serial port, you must reconfigure the Service Agent application to use the /dev/ttyS0 port.

To change the port on the HMC, do the following:

1. In the Navigation area, select **Service Applications**.
2. In the Navigation area, select **Service Agent**.
3. In the Contents area, select **Register and Customize Service Agent** and log in to the Service Agent application.
4. In the Service Agent application, expand the **Network** tab.
5. Expand the tab that corresponds to your HMC's network host name.
6. Select **Dialer**.
7. Scroll down on the right pane to TTY# and change the entry to `ttyS0`.
8. Save the entry and reboot the HMC.

To assign the modem to an 8 port adapter port, after the adapter has been properly configured, do the following:

1. In the Navigation area, select HMC Maintenance.
2. In the Navigation area, select System Configuration.
3. In the Contents area, select Configure Serial Adapter.
4. Select Configure RS422 ports on an 8-port Serial Adapter.

5. Select an adapter.
6. A list of the ports on the fan out box and the /dev/tty entries for that port displays. An example of the listing is `0 ttyD000 rs232`. Leave the port setting as `rs232`.
7. Plug the modem into port 0 of the 8-port fanout box.
8. Use the directions in the previous section to change the TTY# entry to ttyD000 (from example)

Assigning the Modem to an 8-Port Adapter Port

To assign the modem to an 8 port adapter port, after the adapter has been properly configured, do the following:

1. In the Navigation area, select **HMC Maintenance**.
2. In the Navigation area, select **System Configuration**.
3. In the Contents area, select **Configure Serial Adapter**.
4. Select **Configure RS422 ports on an 8-port Serial Adapter**.
5. Select an adapter.
6. A list of the ports on the fan out box and the /dev/tty entries for that port displays. An example of the listing is `0 ttyD000 rs232`. Leave the port setting as `rs232`.
7. Plug the modem into port 0 of the 8-port fanout box.
8. Use the directions in the previous section to change the TTY# entry to `ttyD000`.

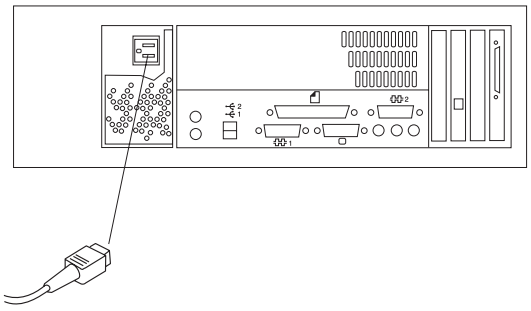
Step 5. Connect the LAN Cable

The LAN cable is recommended because each active partition reports errors to the HMC's Service Focal Point application through the LAN network. The HMC must be attached to the system's LAN, and each partition should have a LAN adapter assigned as a resource.

Connect the LAN to the adapters assigned to each partition and to the LAN connection on the HMC system hardware.

Step 6. Plug in the HMC Power Cords

1. Plug in the power cord, as shown in the following illustration.



2. Plug the power cords for the monitor, HMC, and modem into electrical outlets.

Configuring Your HMC

To configure your HMC, use the steps in this section .

Step 1. Configure the Keyboard and Mouse

If your HMC has PS/2-style mouse and keyboard, use the hardware discovery utility to configure the mouse and keyboard. You must configure the keyboard and mouse the first time you boot the HMC after it has been installed. The hardware discovery utility (Kudzu) opens automatically when you boot the HMC for the first time. Press Enter when the Kudzu screen appears to configure the keyboard and mouse.

If the HMC has a USB mouse and keyboard, the configuration is done automatically.

Step 2. Change the Keyboard Settings

During the system boot, you are prompted to change the HMC keyboard settings. If you do not take any action, this prompt times out in 30 seconds and defaults to an English-language keyboard setting. If you only want to use an non-English keyboard setting, you can select the language you want and disable this prompt for future sessions.

Step 3. Log in to the HMC

The HMC is shipped with a predefined user ID and password. Both the user ID and password are case-sensitive and must be typed exactly as shown. This default user ID and password are as follows:

- ID: hscroot
- Password: abc123

When the console is powered on for the first time, use this user ID to log in. For more information about user management and roles, see Chapter 14, “User Management,” on page 67. This hscroot user ID is a member of the System Administrator role.

After you power on your HMC, the HMC login window displays, which prompts you to enter your user ID and password.

Step 4. Change the Predefined hscroot Password

To restrict access, change the predefined hscroot password immediately. To change the predefined hscroot password, do the following:

1. In the Navigation area (the area on the left side of the screen), click the **User** icon.
2. In the Contents area (the area on the right side of the screen), right-click the **hscroot** icon.
3. Select **Change Password**.
4. Type the new password in the first field.
5. Confirm the new password by typing it again in the **Retype new password** field.

Step 5. Change the Predefined Root-User Password

The HMC is shipped with the following predefined root-user password: passw0rd

The root-user ID and password cannot be used to log in to the console. However, the root-user ID and password are needed to perform some maintenance procedures.

To control access to the HMC, do the following:

1. In the Navigation area (the area on the left side of the screen), click the **User** icon.
2. In the Contents area (the area on the right side of the screen), right-click the **root** icon.
3. Select **Change Password**.
4. Type the new password in the first field.

5. Confirm the new password by typing it again in the **Retype new password** field.

Step 6. Create HMC Users

After you have logged in and changed both passwords, you are ready to create additional HMC users. The additional users can be assigned different roles to control their access to different HMC tasks. For more information about user management and roles, see Chapter 14, “User Management,” on page 67.

Step 7. Set Up Your HMC Software for Service and Dynamic Logical Partitioning

To configure your managed system for service and dynamic logical partitioning (DLPAR), do the following

1. Ensure that the required planning information in *pSeries Planning for Partitioned-System Operations*, order number SA38-0626, has been completed.
2. Log in to the HMC.
3. Configure the HMC’s date and time. For more information about setting the HMC’s date and time, see “Setting and Viewing the Console Date and Time” on page 39.
4. Configure the network settings on your HMC. For more information about setting up the network, see “Customizing Network Settings” on page 40. You will use the information you provided in *pSeries Planning for Partitioned-System Operations*, order number SA38-0626.
5. Reboot the HMC. For more information about rebooting the HMC, see “Shutting Down, Rebooting and Logging Off the HMC” on page 29.
6. Create at least one partition. For more information about creating partitions, see “Creating Logical Partitions” on page 93.
7. Install an operating system on the partition. For more information about installing an operating system on a partition, see the documentation provided with your operating system.
8. Set up and configure the Service Focal Point application. For more information about setting up and configuring Service Focal Point, see “Service Focal Point Settings” on page 132.
9. Verify that Service Focal Point is operating properly by generating a test error. For more information about testing Service Focal Point’s error reporting, see “Testing Error Reporting” on page 131.
10. Configure the Inventory Scout application. For more information about configuring Inventory Scout, see “Configuring the Inventory Scout Services Profile” on page 59.
11. Configure the Service Agent application. For more information about configuring Service Agent, see “Configuring and Using Service Agent” on page 124.

Step 8. Set Up Service Authority

If you powered on with the Full System Partition, you do not have to take additional steps to prepare for firmware upgrades.

Firmware upgrades are done at the system level, not on a per-partition basis. A firmware upgrade can be performed from a partition that is running AIX or from the service processor menus.

When partitions are being created, it is recommended that one partition be given service authority. The partition designated as having service authority is used to perform system firmware upgrades and set other system policy parameters. Using a partition with Service Authority allows you to perform upgrades without powering off the managed system. All other partitions must be shut down before the firmware upgrade is initiated.

The partition that has service authority must also have access to the firmware upgrade image. If the firmware upgrade image is going to be read from diskettes, the diskette drive must be assigned to the partition that has service authority. If you are downloading the firmware upgrade from the network, download it to the partition that has service authority.

For more information about setting service authority on a partition, read “Setting Service Authority” on page 110.

Upgrading the HMC

Upgrading the HMC Software

This section describes how to upgrade the HMC software to the latest release level.

If you upgrade the HMC software and do not follow these steps, the HMC’s configuration settings must be set when the new software is installed. Before performing any upgrade task, save the current state of the HMC software to DVD by performing the Backup Critical Console Data task. For more information about this task, see “Scheduling Backups” on page 44.

Software upgrades on the HMC can be performed in the following ways:

- Between releases, you can perform the Install Corrective Service task to update the HMC software. For more information about performing this task, see “Installing Corrective Service for the HMC” on page 120.
- To upgrade, you must perform an upgrade procedure, which involves a series of steps that ensures that configuration settings, such as network configuration are saved and restored after the upgrade.

Prepare for the HMC Software Upgrade

To prepare your HMC for the upgrade, verify your software version, record configuration information, and back up console information.

Verify Your Current HMC Software Level: To determine your current HMC software version, do the following:

1. Log in to the HMC as hscroot or as a user with System Administrator role. For more information about user tasks and roles, see Chapter 14, “User Management,” on page 67.
2. Click **Help —> About Hardware Management Console**.

   If you have an HMC release earlier than Release 3, continue with the following preparation steps.

Record Current HMC Configuration Information: Before you upgrade to the new version, record HMC configuration information. To record HMC configuration information, do the following:

1. In the Navigation area, click the **HMC Maintenance** folder.
2. In the Navigation area, click**System Configuration**.
3. In the Contents area, click **Scheduled Operations**. The Scheduled Operations window opens.
4. Select **Sort —> By Object**.
5. Select each object. Record the following details:
   - Object Name
   - Schedule Date
   - Operation Time (displayed in 24-hour format)
   - Repetitive. If repetitive is **YES**, do the following:
     a. Select **View —> Schedule Details**.
     b. Record the interval information.
     c. Close the Scheduled Operations window.
6. Repeat the previous step for each scheduled operation.
7. Close the Scheduled Operations window.
8. In the Navigation area, click the **Server and Partition** folder.
9. In the Contents area, double-click **Server Management**.
10. In the Contents area, right-click the managed system and select **Profile Data** –> **Backup**.

11. Type a backup file name and record this information.
12. Click **OK**.
13. Repeat steps 11-13 for each managed system.
14. In the Navigation area, click the **Software Maintenance** icon.
15. In the Navigation area, click the **System Configuration** icon.
16. In the Contents area, click **Enable/Disable Remote Command Execution**.
17. Record the settings of the following option:
    - Enable remote command execution using the **ssh** facility

    For more information about using **ssh** facilities, see the documentation provided with your operating system.

Back Up Critical Console Information: To back up critical console information, do the following:

1. If you previously backed up the HMC during the HMC software installation, remove the old label from the DVD.
2. To ensure that the DVD is not write-protected, examine the switch in the front lower-left corner. The switch should be in the lower position.
3. Insert the DVD into the HMC's DVD-RAM drive.
4. In the Contents area, click **Backup Critical Console Data**.
5. Click **Continue** and wait for the HMC to complete the task.
6. Click **OK**.
7. Remove the DVD from the drive, and write the date, time, and code level on the DVD.

Upgrade the HMC Software

To upgrade your HMC software, do the following:

1. Log in to your HMC as **hscroot**.
2. In the Navigation area, double-click the **Software Maintenance** folder.
3. In the Contents area, click **HMC**.
4. In the Contents area, click **Save Upgrade Data**.
5. Click **Hard Drive**.
6. Click **Continue**.
7. Click **Continue** again to start the task. Wait for the task to complete. If the Save Upgrade Data task fails, contact software support before proceeding. *Do not* continue the upgrade process if the Save Upgrade Data task fails.
8. Click **OK**.
9. Insert the *HMC Recovery CD* into the DVD-RAM drive.
10. Select **Console** menu option, then select **Exit**.
11. Click **Exit now**.
12. The **Exit Hardware Management Console** window opens. Click **Reboot Console**.
13. Select the Upgrade option by pressing F1.
14. Press F1 again to confirm.
15. When the upgrade is complete, the DVD ejects from the drive. Remove the Recovery CD from the drive and close the DVD-RAM drive. Press Enter to reboot the HMC.

    Note: If there is a modem installed, ensure that it is powered on.
16. When the HMC reboots, if the Kudzu screen appears, immediately press Enter to start the Hardware Discovery Utility.

17. For each Hardware Removed window (if any), click **Remove Configuration**. This task logically removes hardware devices from the system configuration.
18. For each Hardware Added window, click **Configure**. This task configures the devices. Most devices, such as modems, require no additional settings. Added devices such as an Ethernet adapter will prompt you to migrate to an existing network. If this occurs, click **Migrate Existing Network**.
19. The **Keyboard Mapping Section** window opens. There is a timer on the keyboard mapping selection screen. Select an applicable keyboard option for your locale.
20. When the HMC boot has completed, configure the new software version. For more information about configuring the HMC, see Chapter 8, "System Configuration," on page 39. If you recorded the **ssh** or scheduled operation facilities, reset them now.

Checking Your HMC Software Version

You can use the HMC interface to check your current HMC software version.

To check, do the following:

1. Log in to the HMC as **hscroot** or as a user with System Administrator role.
2. At the top of HMC interface, select **Help**.
3. Select **About Hardware Management Console**. A window opens that displays HMC software-level information.

For more information about updating the HMC code, see "Upgrading the HMC Software" on page 15.

Chapter 4. Partitioning

This chapter provides an overview of partitions and how a partitioned system is managed.

Partitioning your system is similar to partitioning a hard drive. When you partition a hard drive, you divide a single physical hard drive so that the operating system recognizes it as a number of separate logical hard drives. You have the option of dividing the system's resources by using the HMC to partition your system. On each of these divisions, called *partitions*, you can install an operating system and use each partition as you would a separate physical system.

Types of Partitions

The HMC allows you to use two types of partitions: logical partitions, and the Full System Partition.

Logical Partitions

Logical partitions are user-defined system resource divisions. Users determine the number of processors, memory, and I/O that a logical partition can have when active.

Some systems are equipped to use affinity partitions. An *affinity partition* is a special type of logical partition. Affinity partitions are divisions of system-defined resources that have a close physical proximity to each other. When you decide to create an affinity partition, the system determines the number of processors and memory that a partition can have, but the user determines the I/O requirements for each of these partitions.

Full System Partition

A special partition called the *Full System Partition* assigns all of your managed system's resources to one large partition. The Full System Partition is similar to the traditional, non-partition method of operating a system. Because all resources are assigned to this partition, no other partitions can be started when the Full System Partition is running. Likewise, the Full System Partition cannot be started while other partitions are running.

The HMC allows you to easily switch from the Full System Partition to logical partitions. The actual setup of the operating system in a partition may require some careful planning to ensure no conflicts exist between the two environments.

Benefits of Partitioning

Partitioning provides greater flexibility when deploying multiple workloads on servers, providing better management, improved availability, and more efficient use of resources.

- **Consolidate Servers**: A server with sufficient processing capacity that is capable of being partitioned can address the need for server consolidation by logically subdividing the server into a number of separate, smaller systems. In this way, application-isolation needs can be met in a consolidated environment, with the additional benefits of reduced floor space, a single point of management, and easier redistribution of resources as workloads change.
- **Merge Production and Test Environments**: Partitioning enables separate partitions to be allocated for production and test systems, eliminating the need to purchase additional hardware and software. When testing has been completed, the resources allocated to the test partition can be returned to the production partition or elsewhere as required. As new projects are developed, they can be built and tested on the same hardware on which they will eventually be deployed.
- **Consolidate Multiple Versions of the Same Operating System**: A single system can have different versions of the operating system installed to accommodate multiple application requirements. Furthermore, a partition can be created to test applications under new versions of the operating system *prior* to upgrading the production environments. Instead of having a separate server for this function, a

minimum set of resources can be temporarily used to create a new partition where the tests are performed. When the partition is no longer needed, its resources can be incorporated into the other partitions.

- **Consolidate Applications Requiring Different Time Zone Settings**: Partitioning enables multiple regional workloads to be consolidated onto a single server. The different workloads can run in different partitions, with different operating systems, as well as with different time and date settings. For example, workloads for operations based in San Francisco and New York can run in different partitions on a single server. The evening batch workload, maintenance, or upgrade for the New York operation does not affect those of the San Francisco operation.

Managing a Partitioned System

Using the HMC to manage your partitioned system, different managed-object types exist within the user interface. You can perform management functions by selecting the appropriate object type and then selecting an appropriate task. The main types of objects are managed systems, partitions, and profiles.

Managed Systems

Managed systems are the systems that are physically attached to and managed by the HMC. The HMC can perform tasks that affect the entire managed system, such as powering the system on and off. You can also create partitions and profiles within each managed system. These partitions and profiles define the way that you configure and operate your partitioned system.

Partitions

Within your managed system, you can assign resources to create partitions. Each partition runs a specific instance of an operating system. The HMC can perform tasks on individual partitions. These tasks are similar to those you can perform on traditional, nonpartitioned servers. For example, you can use the HMC to start the operating system and access the operating system console.

Because the HMC provides a *virtual terminal* for each partition, a terminal window can be opened for each console. This virtual terminal can be used for software installation, system diagnostics, and system outputs. The managed system firmware and device drivers provide the redirection of the data to the virtual terminal. For more information about the virtual terminal window, see Chapter 18, “Virtual Terminal Window,” on page 115.

Profiles

A profile defines a configuration setup for a managed system or partition. The HMC allows you to create multiple profiles for each managed system or partition. You can then use the profiles you created to start a managed system or partition in a particular configuration.

You can create the following types of profiles:

Partition Profiles

A partition does not actually own any resources until it is activated; resource specifications are stored within partition profiles. The same partition can operate using different resources at different times, depending on the profile you activate.

When you activate a partition, you enable the system to create a partition using the set of resources in a profile created for that partition. For example, a logical partition profile might indicate to the managed system that its partition requires 3 processors, 2 gigabytes of memory, and I/O slots 6, 11, and 12 when activated.

You can have more than one profile for a partition. However, you can only activate a partition with one profile at a time. Additionally, affinity partitions and logical partitions cannot be active at the same time.

Partition profiles are not affected by changes you make using the Dynamic Logical Partitioning feature. If you want permanent changes, you must then reconfigure partition profiles manually. For example, if your partition profile specifies that you require two processors and you use Dynamic Logical Partitioning to add a processor to that partition, you must change the partition profile if you want the additional processor to be added to the partition the next time you use the profile.

System Profiles

Using the HMC, you can create and activate often-used collections of predefined partition profiles. A collection of predefined partition profiles is called a *system profile*. The system profile is an ordered list of partitions and the profile that is to be activated for each partition. The first profile in the list is activated first, followed by the second profile in the list, followed by the third, and so on.

The system profile helps you change the managed systems from one complete set of partitions configurations to another. For example, a company might want to switch from using 12 partitions to using only four, every day. To do this, the system administrator deactivates the 12 partitions and activates a different system profile, one specifying four partitions.

When you create a group of affinity partitions, the HMC automatically creates a system profile that includes all of the affinity partitions that you created.

Chapter 5. Preparing for Partitioning

This chapter helps you prepare for a multiple-partitioned environment, including information about requirements, host name considerations, and managed system operating states.

Partitioning Requirements

This section contains information about the requirements you must have in order to create partitions.

Before creating partitions, do the following:

- Record the required subnet mask, any gateway information, and address of your DNS server (if used).
- Check that you have a suitable LAN (hub or switch and cables) to connect to each HMC and each network adapter used by partitions.
- Record the TCP/IP names and addresses to be resolved by a DNS server, or to be entered into the **/etc/hosts** file in each partition, and on the HMC.
- Locate the HMC in a suitable position so that the serial cable can be physically connected to the managed system.
- Verify that an analog telephone port is close to the HMC location to connect the modem.

Before you start using partitioning, you must determine the following:

- Your current resources for each partition
- The operating system host name for each partition
- The partition you want to use for service actions

Assignable Resources for Logical Partitioning

For logical partitions, you must assign resources by creating partition profiles. Use the following guidelines for assigning resources in logical partition profiles.

Assigning Processors

Each processor installed and configured on your system can be individually assigned to a logical partition. You must assign at least one processor to each logical partition.

Assigning Memory

The HMC can assign memory to a logical partition in increments of 256 MB, with a minimum of 256 MB per partition. One GB is equal to 1024 MB. This section describes the HMC's various logical-partition memory considerations.

When using dynamic logical partitioning, you must allocate at least 512 MB of memory to each partition you want to activate.

While models that support greater than 256GB memory sizes have the potential to define greater than 256GB logical partition sizes, AIX 5.1 logical partitions have a maximum logical partition memory size of 256GB. AIX 5.1 partitions defined to have greater than 256GB will fail to activate with an insufficient real mode memory failure. AIX 5.2 and Linux partitions can be greater than 256GB in size.

Logical Partition Memory Usage: The system requires some memory overhead when it creates logical partitions. Use the following table to help you determine how much memory overhead the system needs for partitioning. You can also use this table to determine the maximum number of partitions you can create.

Total Memory (in GB)	Approx. Memory Overhead (in GB)	Approx. Usable Partition Memory (in GB)	Maximum Number of Partitions: AIX or Linux, any version Pre-10/2002 firmware ≤16 GB and >16 GB (see Notes 1 and 2)	Maximum Number of Partitions: AIX 5.1 Post-10/2002 Firmware ≤16 GB and >16 GB (see Notes 1 and 3)	Maximum Number of Partitions: AIX 5.2 (+) or Linux Post-10/2002 firmware All partition sizes (see Notes 1, 4, and 5)	Maximum Number of Partitions: AIX 5.1 Post-5/2003 Firmware <=16GB and >16GB (see Notes 1,3, and 6)	Maximum Number of Partitions: AIX 5.2 (+) or Linux Post-5/2003 firmware All partition sizes (see Notes 1,4,5, and 6)
2	.75 to 1	1 to 1.25	0 and 0	5 and 0	5	5 and 0	5
4	.75 to 1	3 to 3.25	2 and 0	13 and 0	13	13 and 0	13
8	.75 to 1	7 to 7.25	6 and 0	16 and 0	16	29 and 0	29
16	.75 to 1	15 to 15.25	14 and 0	16 and 0	16	32 and 0	32
24	1 to 1.25	22.75 to 23	16 and 0	16 and 0	16	32 and 0	32
32	1 to 1.5	30.5 to 31	16 and 0	16 and 0	16	32 and 0	32
48	1.5 to 2	46 to 46.5	16 and 1	16 and 1	16	32 and 1	32
64	1.5 to 2.25	61.75 to 62.5	16 and 2	16 and 2	16	32 and 2	32
96	2 to 3.5	92.75 to 94	16 and 4	16 and 4	16	32 and 4	32
128	2.5 to 4	124 to 125.5	16 and 6	16 and 6	16	32 and 6	32
192	3.5 to 5.75	186.25 to 188.5	16 and 10	16 and 10	16	32 and 10	32
256	4.5 to 7.5	248.5 to 251.5	16 and 14	16 and 14	16	32 and 14	32
320	5.5 to 9.25	310.75 to 314.5	N/A	N/A	N/A	32 and 18	32
384	6.5 to 11	373 to 377.5	N/A	N/A	N/A	32 and 22	32
448	7.5 to 12.75	435.25 to 440.5	N/A	N/A	N/A	32 and 26	32
512	8.5 to 14.5	497.5 to 503.5	N/A	N/A	N/A	32 and 30	32

Notes:

1. All partition maximums are subject to availability of sufficient processor, memory, and I/O resources to support that number of partitions. For example, a system with only 8 processors can only support a maximum of 8 partitions
2. These rules apply to systems running partitions with any version of AIX or Linux, if the firmware and HMC release levels are earlier than the 10/2002 release level.
3. These rules apply to systems running partitions with AIX version 5.1, if the firmware and HMC release levels are at the 10/2002 release level or later. The HMC partition profile option for ″Small Real Mode Address Region″ option should not be selected for AIX 5.1 partitions. These numbers reflect the maximum when running only AIX 5.1 partitions, but AIX 5.1 and 5.2 partitions can be mixed, and may allow for additional partitions to be run (up to the maximum of 32).
4. These rules apply to systems running partitions with AIX version 5.2 (or later) or Linux, if the firmware and HMC release levels are at the 10/2002 release level or later. The HMC partition profile option for ″Small Real Mode Address Region″ should be selected for these partitions.

5. AIX 5.2, when run with the **Small Real Mode Address Region** profile option, requires that the maximum memory setting is no greater than 64 times the minimum memory setting. For example, if the minimum memory setting is 256MB, then the maximum memory setting should not be greater than 16GB. If you violate this condition, AIX does not start.
6. If you want to activate more than 16 partitions, you must have a p690 with the new service processor Feature Code.

Real Mode Address Region (RMO) Memory Considerations: When assigning memory to a partition, consider the following memory options:

Small Real Mode Address Region: When you create a partition profile and select the memory sizes, you can select Small Real Mode Address Region, allows you to:

- Use managed system memory efficiently
- Avoid some of the memory-allocation constraints associated with large partitions

To use the Small Real Mode Address Region option, you must have either Linux or AIX 5.2 and later installed in the partition. If you select the **Small Real Mode** check box and have the required operating system on your partition, the large real mode memory boundary rules do not apply.

AIX 5.1 might not boot in a partition with the Small Real Mode Address Region option selected, because AIX 5.1 requires a Real Mode Address Region that scales with the size of the overall partition. If you meet these operating system requirements and check the **Small Real Mode Address Region** box, then the following memory allocation restrictions do not apply.

Large Real Mode Address Region: If you do not select the Small Real Mode Address Region option, when you assign your minimum, desired, and maximum memory amounts in the partition profile, all three memory values are limited to a specific range. Each range is associated with a scalable Real Mode Address Region of a particular size (256 MB, 1 GB, and 16 GB). The Real Mode Address Region size is determined by the maximum partition memory size that you specify. These memory ranges are defined as follows:

Maximum Memory Size (in GB)	Real Mode Address Region size (in GB)	Partition Memory Range (in GB)
Up to 4	.25	.25 to 4
4.25 to 16	1	1 to 16
16.25 to 256	16	16 to 256

Because large Real Mode Address Regions have more limits when placed in memory, use the following guidelines when you plan to create partitions that do not use the Small Real Mode Address Region option:

- Start all the partitions that are greater than 16 GB in size *before* starting all the partitions that are less than or equal to 16 GB in size. If the last partition that you activate is greater than 16 GB, it might not start.
- If all of your partitions are greater than 16 GB in size, start the largest partition last.

I/O Devices

I/O is assignable to a given partition on a PCI adapter-slot basis.

Because each partition requires its own separate boot device, the system must have at least one boot device and associated adapter per running partition.

Each partition should have at least one network adapter, although this is not mandatory. In addition to providing a network connection, the connection is also needed to provide the capability for HMC service functions. For more information, see “Customizing Network Settings” on page 40.

For more information about a specific device and its capabilities, see the documentation provided with that device. For a list of supported adapters and a detailed discussion about adapter placement, see the *PCI Adapter Placement Reference*, order number SA38-0538.

Assignable Resources for Affinity Partitioning

The HMC pre-allocates processors and memory to affinity partitions. You can choose to create either 4-processor affinity partitions or 8-processor affinity partitions. If you have 32 processors on your system, choosing a 4-processor group allows you to create up to eight affinity partitions. Likewise, an 8-processor group allows you to create up to four affinity partitions. You cannot define 4-processor groups and 8-processor groups at the same time.

I/O Devices

The user allocates I/O to each affinity partition. I/O is assignable to a given partition on a PCI adapter-slot basis. You can also dynamically reassign I/O between affinity partitions.

Because each partition requires its own separate boot device, the system must have at least one boot device and associated adapter per partition.

Each partition should have one network adapter, although this is not mandatory. In addition to providing a network connection, the connection is also needed to provide the capability for HMC service functions. For more information, see “Customizing Network Settings” on page 40.

For more information about a specific device and its capabilities, see the documentation provided with that device. For a list of supported adapters and a detailed discussion about adapter placement, refer to the *PCI Adapter Placement Reference*, order number SA38-0538.

Assigning a Host Name to Your Partition

Each partition, including the Full System Partition, must have a unique host name that can be resolved. Host names cannot be reused between the Full System Partition and the logical partitions. To change the host name of the partition manually, you may need to update the Network Settings on the HMC. You will need to update the settings if a short partition name is used or if a DNS server is not used. For more information about changing the host name manually, see “Changing a Partition Host Name Manually” on page 258. To determine if any additional changes are needed, see “Customizing Network Settings” on page 40.

Operating States

The HMC Contents area displays an operating state for the managed system.

Operating States for Managed Systems

The following operating states apply to the managed system:

State	Description
Initializing	The managed system is powered on and is initializing.
Ready	The managed system is powered on and operating normally.
No Power	The managed system is powered off.
Error	The managed system’s operating system or hardware is experiencing errors. For recovery information, see “Managed System Operating States” on page 253.

State	Description
Incomplete	The HMC cannot gather complete partition, profile, or resource information from the managed system. For recovery information, see “Managed System Operating States” on page 253.
No Connection	The HMC cannot contact the managed system. For recovery information, see “Managed System Operating States” on page 253.
Recovery	The partition and profile data stored in the managed system must be refreshed. For recovery information, see “Managed System Operating States” on page 253.
Version Mismatch	Your managed system’s service processor level is later than your HMC’s code level. For recovery information, see “Managed System Operating States” on page 253.
CUoD CTA	You must accept the CUoD (Capacity Upgrade on Demand) license. For recovery information, see “Managed System Operating States” on page 253.

Operating States for Partitions

The following operating states apply to the logical partition you have created.

State	Description
Ready	The partition is not active but is ready to be activated.
Starting	The partition is activated and is undergoing booting routines.
Running	The partition has finished its booting routines. The operating system might be performing its booting routines or is in its normal running state.
Error	This partition failed to activate due to a hardware or operating system error. For recovery information, see Appendix E, “Error Messages and Recovery Information,” on page 203.
Not Available	This partition is not available for use. Reasons can include: • The managed system is powered off. • The Full System Partition is not available when the managed system is powered on with the Partition Standby power-on option. • Logical partitions are not available when the managed system is powered on with the Full System Partition power-on option. • Affinity partitions are not available when the managed system is powered on and non-affinity partitions are activated first. • Non-affinity partitions are not available when the managed system is powered on and affinity partitions are powered on first. For recovery information, see Appendix E, “Error Messages and Recovery Information,” on page 203.
Open Firmware	The partition was activated by a profile that specified an OPEN_FIRMWARE boot mode.

Chapter 6. User Environment

This chapter discusses the user environment and Hardware Management Console (HMC) applications.

Using the Login Window

The HMC provides a predefined user ID called hscroot. The hscroot password is abc123. This hscroot user ID is a member of the System Administrator role. When the console is powered on for the first time, use this user ID to log in. After you are logged in, you can create additional users.

After you power on your HMC, the HMC login window displays, and prompts you to enter your user ID and password.

Service representatives may request that you create a special user ID that has the Service Representative role, enabling them to log in to perform service functions. For more information about creating users and assigning roles, see Chapter 14, “User Management,” on page 67.

Shutting Down, Rebooting and Logging Off the HMC

This task allows you to shut down, reboot and log off the HMC interface.

To log off the HMC interface, do the following:

1. In the main menu, click **Console —> Exit**. At this point, you can choose to save the state of the console for the next session by clicking the box next to the option.
2. Click **Exit Now**.
3. When you exit from your HMC session, you can choose to shut down, reboot, or log off your session. The following is a description of each option:

   Shutdown Console
   Powers off the HMC

   Reboot Console
   Shuts down the HMC and then reboots it to the login prompt

   Logout
   Returns the user to the login prompt without shutting down the HMC

HMC System Management Environment

The HMC system management environment allows you to manage your managed systems. The HMC interface is based on the AIX Web-based System Manager.

When you log in to the HMC, the HMC management window opens, and the management environment is already selected. This window is divided into the Navigation area and the Contents area.

The panel on the left (the Navigation area) displays a hierarchy of icons that represent collections of systems, individual systems, managed resources, and tasks. Each Navigation area folder identifies a collection of related applications. Each icon in these folders identifies an application. At the highest point, or *root* of the tree, is the Management Environment. The Management Environment contains one or more host system applications that are managed by the console. Each system application contains its own collection of applications that contain managed objects, tasks, and actions for a related set of system entities or resources.

The panel on the right (the Contents Area) displays results based on the item you select in the Navigation area. When you click on an application in the Navigation area, the Contents area displays the tasks you can perform using that application.

Each HMC contains the following set of application groups:

- System Manager Security
- Server and Partition
- Software Maintenance
- HMC Management
- HMC Maintenance
- Service Applications

Each HMC contains the following set of application icons:

- System Manager Security
- Server Management
- Switch Management
- System Configuration
- Users
- Frame
- HMC
- Inventory Scout Services
- Service Agent
- Service Focal Point
- Problem Determination

Using Multiple HMCs

You can use one HMC to view and manage other HMCs by adding the additional HMCs to the Navigation area.

You can also connect two HMCs to the same managed system. In this configuration, either HMC can perform tasks on that managed system. For more information about using multiple HMCs, see Chapter 12, “Using Two HMCs Connected to One Managed System,” on page 63.

Using One HMC to Manage Multiple Managed Systems

You can use one HMC to view and manage more than one managed system.

For more information about using one HMC to manage multiple managed systems, see Chapter 13, “Using One HMC to Connect to More Than One Managed System,” on page 65.

Using Multiple Managed Systems Connected to One HMC

You can connect more than one managed system to an HMC. When a managed system is connected to an HMC, it displays in the Navigation area. You can also use your HMC to manage a frame of managed systems. A frame contains multiple managed systems and I/O drawers.

Security Enhancements

Starting with HMC Release 3 Version 2.4, the HMC has been enhanced to keep track of failed login attempts in two ways. Failed logins at the local console or from a remote client are kept in the Console Event log. The Console Event log is accessible by clicking **View Console Events** on the HMC or by using the **lssvcevents** command. If you use the **lssvcevents** command, you must specify `console` as the type of event to display.

Failed logins via ssh are kept in the **/var/hsc/log/secure** file. This file is kept under logrotate control and is accessible to all HMC users with the System Administration role.

HMC Application Overview

This section provides an overview of each application’s functions. For detailed information, see the chapter that discusses each application.

Switch Network Interface

Switch Network Interface (SNI) is an AIX component that provides support for the eServer pSeries High Performance Switch (HPS). For additional overview, configuration, and reference information, see the *eServer Cluster 1600 pSeries High Performance Switch Planning, Installation, and Service*, order number GA22-7951.

System Manager Security

System Manager Security provides for the secure operation of the HMC in client-server mode. System Manager Security is based on Public Key Encryption, the Secure Socket Layer (SSL) protocol, and the Pluggable Authentication Module (PAM) authentication policy method. In the System Manager Security operation, the managed machines are servers and the managed users are clients.

Servers and clients communicate over the SSL protocol, which provides server authentication, data encryption, and data integrity. The client manages the server using an account on that system and authenticates to the System Manager server by sending the user ID and password. To ensure security during configuration, users of the System Manager Security application must be logged in to the HMC locally.

For more information about using this application, see Chapter 10, “System Manager Security,” on page 53.

Server and Partition Application Group

The Server and Partition application folder contains the Server Management application.

Server Management

The Server Management application manages all partition-related activities. Use the Server Management application to create, maintain, activate, and delete partitions. You can also use this application to power managed systems on and off.

For more information about using this application, see Chapter 17, “Server Management Tasks,” on page 93.

Switch Management

Switch Network Manager (SNM) manages networks consisting of High Performance Switches and 2-Link or 4-Link Switch Network Interfaces.

For more information about using this application, see the *Switch Network Interface for eServer pSeries High Performance Switch Administration Guide and Reference*, order number SC23-4869-00.

Software Maintenance Application Group

The Software Maintenance folder contains the Software Maintenance applications.

Frame

The Frame software maintenance application allows you to receive and install corrective service for a frame.

For more information about using this application, see Chapter 19, “Software Maintenance for the HMC and the Frame,” on page 119.

HMC

The HMC software maintenance application allows you to save and back up important HMC-related information and format removable media. You can also install corrective service on the HMC.

For more information about using this application, see Chapter 19, “Software Maintenance for the HMC and the Frame,” on page 119.

HMC Management Application Group

The HMC Management folder contains the Users application.

Users

The Users application controls user access to the HMC. You can assign one role to each user you create. Different roles allow the user to perform different tasks in the HMC environment.

For more information about using this application, see Chapter 14, “User Management,” on page 67.

HMC Maintenance Application Group

The HMC Maintenance application folder contains applications related to setting up and maintaining the HMC environment.

System Configuration

The System Configuration application allows you to do the following:

- Set the console’s date and time
- Enter and check HMC network information
- View console events
- Schedule routine backups
- Enable and disable remote commands
- Configure serial adapters
- Enable remote virtual terminal connections
- Change the HMC interface language

For more information about using this application, see Chapter 8, “System Configuration,” on page 39.

Service Applications Group

The service applications folder contains applications used to service both the HMC and managed system.

Problem Determination

Service representatives have access authority to use this application to view and diagnose HMC problems. This application is available to service representatives *only*.

Inventory Scout Services

Inventory Scout Services is a tool that surveys the managed system for hardware and software information. This tool also provides a customized report indicating the latest microcode level. Inventory Scout Services helps users to keep track of software updates and patches on managed systems.

For more information about using this application, see Chapter 11, “Inventory Scout Services,” on page 59.

Service Agent

The Service Agent application accepts hardware errors from the Service Focal Point. Service Agent reports serviceable events, assuming they meet certain criteria for criticality, for service without requiring customer intervention.

Service Agent enables the following:

- Automatic problem reporting; service calls can be placed without customer intervention
- Automatic sending of extended vital product data to IBM
- Automatic customer notification
- Network environment support with minimum number of telephone lines for modems

For more information about using this application, see Chapter 20, “Service Agent,” on page 123.

Service Focal Point

Service representatives and system administrators use Service Focal Point to view operating system error logs.

For more information about using this application, see Chapter 21, “Service Focal Point,” on page 131.

HMC Management Window

The HMC menu bar on the HMC management window displays all of the operations performed on the console and managed objects. The menus are organized as follows:

Console Menu

The Console Menu contains choices that control the console. It allows you to do the following tasks:

- Add and remove host systems from the management environment, including other HMCs
- Save console preferences
- Specify whether to automatically attempt to log in to a host with a stored password
- View the console session log
- Exit the console

Object Menu

The name of the Object Menu changes to indicate the type of resource managed by the current application you have selected. For example, when you select the **Partition Management** application, the Object Menu title becomes Partitions. The Object Menu contains general choices and actions for an application that do not require you to select specific object actions. Typically, actions for creating new resource objects are located in the Object Menu. When a new application is selected, the contents of the Object Menu are updated.

Selected Menu

The Selected Menu contains those actions for an application that require you to select which managed objects an action is to apply to, such as **Open**, **Properties**, **Copy**, **Delete**, or **Start**. When you select a new managed object, the contents of the Selected Menu are updated.

View Menu

The View Menu contains choices for navigating, such as **Back**, **Forward**, and **Up One Level**. It also includes choices for customizing the console in the **Show** submenu. For example, you can select to show or hide the tool bar and status bar. The View Menu includes options that control how objects are

presented. For example, if the application provides a choice of views, such as *Large Icon*, *Small Icon*, *Details*, and *Tree*, these choices are listed here. If the application only supports a single view, no view choices are listed. When an application is displaying an icon or *Details* view, the View Menu includes choices for sorting and filtering the container.

Window Menu

The Window Menu contains actions for managing sub-windows in the console workspace. **New Window** creates a new console sub-window in the workspace. Other choices control how all console sub-windows are presented.

Help Menu

The Help Menu lists user-assistance choices. You can view help contents and search for help on a particular topic.

Documentation Browser

The icon on the lower left of the window opens a documentation browser. Use it to view HMC documentation.

HMC Keyboard Control

The HMC can be used with or without a pointing device, such as a mouse. If you do not use a pointing device, you can use the keyboard to move among controls and menus.

Using Mnemonics and Shortcuts

You can access menu functions using the following keyboard methods:

- **Mnemonics**: Mnemonics are underscored letters in menu choices and control text. To access a visible menu choice or control, press the Alt key followed by the mnemonic. When using mnemonics, it is not necessary to use the space bar or Enter key to select an item.
- **Shortcuts**: Shortcuts (also known as *accelerators*) are keyboard combinations that directly access frequently used controls. Shortcuts also use a combination of keys to access functions; in this case, the Ctrl key followed by a character. Unlike mnemonics, menu shortcuts do not require that a menu choice be visible to be directly accessed.

Navigating the Console with the Keyboard

Use the following keys or key combinations to navigate the HMC:

Keys or Key Combinations	Actions
Arrow Keys	Moves focus between: • Objects in the Navigation Area. Right and left arrows expand and contract nodes; up and down arrows move vertically through items. • Objects in the Contents Area • Icons in tool bar • Items in menus
Ctrl + Arrow Key	Move location focus to another object in the contents area without selecting it. By using Ctrl+Arrow keys and the space bar, you can select multiple objects that are not contiguous.
Escape	Closes an open menu without activating a choice.
F1	Opens browser-based help to contents section.

Keys or Key Combinations	Actions
F8	Moves focus to the splitter bar between the Navigation Area and Contents Area of the console. Moves the splitter bar using Home, End, and the Arrow keys.
F10	Moves focus to and from the Menu bar.
Shift + Arrow Key	Extends a contiguous selection.
Spacebar, Enter	Selects the object that has focus.
Tab, Shift + Tab	Moves focus between areas of the console.

Navigating Window Fields with the Keyboard

Use the following keys or key combinations to navigate HMC window fields:

Keys or Key Combinations	Actions
Alt+F6	Moves focus into or out of a dialog box
Arrow keys	• Opens drop-down lists • Moves between options in lists • Moves between tabs in tabbed dialogs when a tab has focus
Ctrl + Tab, Ctrl + Shift + Tab	Moves focus between controls
Enter	Activates the command button that has focus
Escape	Cancels the dialog box
F1	Opens the context help window
Space Bar	• Selects the option that has focus • Activates the command button which has the location cursor on

Accessing Help with the Keyboard

Use the following keys or key combinations to navigate the HMC help system:

Keys or Key Combinations	Actions
F1	• Opens browser-based help to the Contents Area • In dialog boxes, opens context help window
F9	Shows keys help.
Alt + F6	In context help mode, moves focus between context help window and parent dialog.

Chapter 7. Evaluation Assurance Level 4+

A Common Criteria (CC) Evaluated System is a system that has undergone an evaluation process according to the Common Criteria. The CC is an ISO standard (ISO 15408) for the security assurance evaluation of IT products. The system configuration that meets these requirements is described in this section.

System administrators can choose to install the managed system firmware that has been evaluated according to the Evaluation Assurance Level 4+ (EAL4+). The evaluation at EAL4+ guarantees that important security aspects of the LPAR functionality have undergone a security assessment. Please refer to the Security Target of the CC evaluation for the defined security functions that were subject of the evaluation.

For more information about the managed system firmware compliance, see your managed system's firmware release notes.

Note: Managed system firmware that has been evaluated at Evaluation Assurance Level 4+ (EAL4+) is available on pSeries models p630, p650, and p690. However, only a particular managed system firmware version has been evaluated and is therefore the subject of this chapter. Please refer to the firmware release notes for verification whether the installed managed system firmware version is the evaluated version.

The whole-system firmware has been evaluated. However, only the functional subset handling the security aspects of the firmware functionality was subject to the security assessment.

The evaluated configuration allows the operation of logical partitions given that the guidelines and restrictions described in this section are strictly followed.

The evaluation of the managed system firmware did not make any claims or restrictions on operating systems running in the partitioned environment. For more information about installing AIX 5L Version 5.2 with the 5200-01 Recommended Maintenance package with the CAPP and EAL4+ function on a partition, see the AIX 5L Version 5.2 Security Guide.

Organizational Environment for a EAL4+ System

The following organizational requirements must be met for a EAL4+ system:

- The administrator must be well trained.
- The administrator must be considered trusted and must follow the instructions given in this guide.

Operational Environment for a EAL4+ System

The following operational requirements and procedures must be met for a EAL4+ system:

- The HMC, managed system, and attached I/O devices must be located in a physically controlled environment.
- Only authorized personnel can access the operational environment and the HMC, managed system, and attached I/O devices.
- The HMC must only be used for the following tasks:
  - Initial configuration of the partitions. No partitions can be active during the configuration process.
  - Restarting of ″hanging″ partitions
- Once the partitions have been configured and started, the HMC must be physically disconnected from the managed system.
- The system's ″call home″ feature must be disabled.

- Remote modem access to the system's service processor must be disabled.
- Remote and network access to the HMC must be disabled.
- If AIX runs in an LPAR-enabled environment, the administrator should check with the AIX documentation for requirements on the EAL4+ operation of logical partitions.
- The host's hardware must be checked regularly using appropriate diagnostic tools, to ensure that it continues to function correctly.
- The installation of the system firmware must performed correctly and according to the installation instructions by the responsible personnel.
- The service authority feature must be disabled on logical partitions.
- The command line tools must not be used in the evaluated configuration, since they apply to dynamic configuration only.
- Systems in an LPAR environment cannot share a PCI Host Bridge (PHB). For more information about your managed system's PHBs, see the *PCI Adapter Placement Reference*, order number SA38-0538.

Chapter 8. System Configuration

This chapter discusses the System Configuration application, which allows you to do the following:

- Set the console's date and time
- Enter and check HMC network information
- View console events
- Schedule routine backups
- Enable and disable remote commands
- Configure serial adapters
- Enable remote virtual terminal connections
- Change the HMC interface language

Setting and Viewing the Console Date and Time

Any user role can view the console date and time. To update the console date and time, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator
- Service Representative
- Operator
- Viewer

The battery-operated clock keeps the date and time for the HMC. You might need to set the console date and time under the following circumstances:

- If the battery is replaced in the HMC
- If your system is physically moved to a different time zone

To customize your console date and time, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Console Date / Time**.
4. To change the month, click on the month shown in the **Date** field. Similarly, click the day or year shown in the **Date** field to change those values.
5. Click on the hour, minute or second shown in the **Time** field to change the values. To update this input field to the currently set time, press the **Refresh** button.
6. From the list, select the region and city closest to your location, and click **OK**.

If you click **OK** and the new time setting does not display in the lower right of the HMC interface, log off and then log back in again. For more information about logging off the HMC, see "Shutting Down, Rebooting and Logging Off the HMC" on page 29.

Viewing Console Events

To see a log of recent HMC activity, you can view console events. Each event has an associated time stamp. The following is a sample of the events recorded:

- When a partition was activated
- When a system was powered on
- When a partition was shut down
- Results of a scheduled operation

To view console events, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative
- Viewer

To view console events, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, select **View Console Events**.

Customizing Network Settings

While the HMC conducts most of its management function through the direct serial connections to the managed systems, connecting the HMC to your network provides you with additional remote management capabilities. It also significantly enhances service and maintenance for partitioned systems.

Enabling the HMC network connection allows you to take advantage of the following HMC capabilities:

- **Remote Management**: You can access the HMC user interface remotely from a Web-based System Manager graphical user interface client. Both the Web-based System Manager client and server are provided with the AIX base operating system can be installed in any AIX operating system. The client is also available in a standalone version that can be installed on a number of platforms. To manage a system remotely, you can start the client on a remote system, enter the HMC host name or IP address, and provide a valid HMC user ID and password. After you complete these steps, the HMC user interface options display in the user interface, just as they would on the HMC itself.

  The HMC also provides you with some basic command-line functions for managing systems and partitions. With a network connection, you can connect to the HMC and run these command functions remotely, either manually or as part of an automated script. For more information about the high-level command line, see Chapter 22, “Using the Command Line,” on page 137.
- **Service Functions**: To configure your network to allow network connections between the HMC and the partitions in the managed systems, plan to include network adapters in each partition. While you need only a single network adapter in a partition to handle both management functions and general-purpose networking, you can also use separate adapters if you want to keep these functions separate, or you can put them on separate networks.

  If the network connections are available:

  – The partitions automatically forward hardware service events to the HMC for collection in the Service Focal Point and for automatic dispatch of service through Service Agent (if enabled). Without these connections, service events are reported and logged only within the individual partitions that observe them, which can delay reporting and fixing the problem.

  – You can use the Inventory Scout application to collect hardware and microcode information from the partitions to the HMC, to build a complete picture of the hardware inventory in a partitioned system. The Inventory Scout application then sends this hardware configuration information to IBM to assist in accurate hardware-upgrade planning. Inventory Scout also enables you to check for available updates to the versions of system firmware and adapter microcode that are currently installed in your systems and partitions.

Using Network Adapters to Communicate with Partitions

After a partition has been started, it uses the network adapter to communicate with the HMC. Both the HMC and the partition must be configured so that they can use the network adapters to communicate with each other. The AIX partition must be configured to identify the HMC (or HMCs) on the network. It is recommended that the network be configured using a Domain Name Service (DNS) server and each

partition be identified using a fully qualified host name. This identification ensures uniqueness of all the partitions and the HMC in the network. Fully qualified host names cannot be more than 100 bytes in length.

The HMC and partitions can also be configured using a short host name, in which the domain name is not defined. This is typically done in a private or test network. If the HMC is defined using a short host name, you must perform extra network configuration steps to ensure that the partitions and the HMC communicate correctly. For information about modifying the HMC host name on the partitions, see the *AIX 5L Version 5.2 AIX Installation in a Partitioned Environment* guide, order number SC23-4382.

On the HMC, to communicate with a partition that is not identified on the network by a fully qualified host name or if DNS is not being used, the host name of the partition must be entered in the network settings of the HMC. If you use short host names rather than fully qualified host names, make sure that the host names are unique and that the mappings to IP addresses are specified correctly. The HMC provides an interface for updating the **/etc/hosts** file. For instructions on adding partitions to the HMC **/etc/hosts** file, see "Setting Host Names" on page 42.

The HMC can communicate to partitions that use DNS, fully qualified host names, and short host names. The following examples illustrate possible situations:

- If the partition is specified using a fully qualified host name (for example: `host123.mydomain.mycompany.com`), the HMC must enable the use of a DNS server or must specify the fully qualified host name in the local **/etc/hosts** file. For instructions on adding partition names to the HMC **etc/hosts** file, see "Setting Host Names" on page 42.
- If the partition is specified using a short host name (for example: `host123`), the HMC must specify the short host name in the local **/etc/hosts** file and ensure that the short host name is located before the fully qualified host name, if the fully qualified host name is also specified in the **/etc/hosts** file. For instructions on adding partition names to the HMC **/etc/hosts** file, see "Setting Host Names" on page 42.

Note: Changes made to your HMC's network settings do not take effect until you reboot the HMC.

To customize network settings, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator
- Service Representative

Setting the IP Address

To customize your HMC's IP address, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **IP Address** tab.
5. Type TCP/IP and gateway information as appropriate. For information about your network and how it is configured, see your network administrator.
6. When you are finished customizing the network, click **OK**.

   Note: Changes made to your HMC's network settings do not take effect until you reboot the HMC.

Setting Domain Names

To enable your HMC and managed system for service, you must change the default domain names and enter your own.

To set a domain name, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **Name Services** tab.
5. The system displays the default domain name as `localdomain`. Replace this name with your network information as appropriate.

   Note: Do *not* assign the `localhost.localdomain` with an IP address other than the loopback `127.0.0.1`.

   For information about your network and how it is configured, see your network administrator.
6. Click **OK**.

Setting Host Names

The **/etc/hosts file** on your HMC's hard drive stores all host name information. Regardless of whether or not you are using DNS, you must add the HMC host name using the following procedure. If you are *not* using DNS, you must also add all host names (for each LPAR and HMC) to this file using the following procedure.

In addition, you must also update the local **/etc/hosts** files in each LPAR. For more information about updating files, see the documentation provided with your operating system.

To set a host name in the **/etc/hosts** file, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **Host** tab.
5. Enter your host name information as appropriate.
6. Click **OK**.

If you change the local host name, you must reboot the HMC for changes to take effect. For more information about rebooting the HMC, see "Shutting Down, Rebooting and Logging Off the HMC" on page 29.

For more information about setting host names, see the *AIX 5L Version 5.2 AIX Installation in a Partitioned Environment* guide, order number SC23-4382.

Adding and Changing IP Addresses and Host Names

If you need to completely reinstall your partition (which includes setting a new host name) or if you switch host names between partitions, you must perform the steps listed in "Changing a Partition Host Name Manually" on page 258 for each affected partition.

To add or change a host name in the **/etc/hosts** file, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **Hosts** tab.
5. Click **New** or **Change**.

6. The Host Entries window opens. In the first field, type the IP address you want to add or change.
7. In the second field, type the host name or names you want to associate with the IP address you typed in the first field. If you enter multiple host names, list the primary host name first and separate the names by spaces. Enter multiple host names when you want to identify a machine by both its fully qualified host name and its short host name. For example, if your domain is `mycompany.com`, then for `some` IP address, you might enter `myname.mycompany.com` *somename*.
8. Click **OK**. The **/etc/hosts** file is updated with your new information.

Setting Routing Information

You can add, change, or delete routing information.

To set routing information, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **Routing** tab.
5. Select **New**, **Change**, or **Delete**.
6. Type the gateway information in the fields as appropriate. For information about your network and how it is configured, see your network administrator.
7. Click **OK**.

Setting Device Attributes

You can use your HMC to select speed and duplex modes for your Ethernet adapters.

To set device attributes, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Customize Network Settings**. The Customize Network Settings window displays.
4. Click the **Device Attributes** tab.
5. Select the speed and duplex mode for your adapter. For more information about your adapter's speed and mode, see the documentation that was provided with your adapter.
6. Click **OK**.

Testing Network Connectivity

This option enables you to verify that you are properly connected to the network.

To test network connectivity, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator
- Service Representative

To test network connectivity, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Test Network Connectivity**.
4. Type the host name or IP address of the system to which you are attempting to connect.

5. Click **OK**.

To test the connectivity of a partition to your HMC (for example, using the **ping** command), see the documentation provided with your partition's operating system.

Scheduling Backups

This option enables you to schedule the time and dates for backing up critical console information. When you schedule a backup operation, the information is saved on a formatted DVD-RAM disk on your HMC. Each time this data is saved, old data is replaced with the more recent data. If you do not want older information overwritten, insert a new DVD-RAM disk in the HMC's drive each time you perform a backup.

For more information about critical console data, see "Backing up Critical Console Data" on page 119.

To schedule a backup of console data, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator

Scheduling a Backup Operation

You can schedule a backup to DVD to occur once, or you can set up a repeated schedule. You must provide the time and date that you want the operation to occur. If the operation is scheduled to repeat, you must select how you want this backup to repeat (daily, weekly, or monthly).

Note: Only the most-recent backup image is stored at any time on the DVD.

To schedule a backup operation, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Scheduled Operations**.
4. In the menu, click **Options**.
5. Select **New**.
6. In the appropriate fields, enter the time and date that you want this backup to occur.
7. If you want this scheduled operation to repeat, click the **Repeat** tab and enter the intervals at which you want the backup to repeat. You can schedule backup operations to repeat at monthly, weekly, daily, or hourly intervals. If you select Daily intervals, you can select the individual day of the week you want the backup to occur. If you want to repeat a scheduled operation daily or hourly, you can also specify the days of the week on which you want this operation to occur.
8. When you are finished setting the backup time and date, click **OK**.

After you have defined a scheduled backup operation, a description of the operation displays in the Scheduled Operations window.

Reviewing an Existing Scheduled Operation

You can use the HMC to review an existing scheduled operation that you have created.

To review an existing operation, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator

To review an operation you have already created, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.

3. In the Contents area, click **Scheduled Operations** from the menu to display a list of scheduled operations.

You can view the duration of the backup tasks you scheduled and customize the way you view those tasks.

To modify your view, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator

To view the time range of a scheduled backup, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Scheduled Operations** from the menu to display a list of scheduled operations.
4. Select the operation you want to view.
5. From the menu, select **View**.
6. Select **New Time Range**. The Change Time Range window opens.
7. After viewing the time range information you want to view, click **OK**.

Enabling and Disabling Remote Commands

This option provides the ability to run commands remotely through the **ssh** command.

To install **ssh** software on your PC, type the following Web address:

`http://HMC System Name/remote_client_security.html`

This page provides links to download the PC and Linux security package installed on the HMC. By default, the security package is installed and configured; however, the HMC system administrator can uninstall the Remote Client Security package. If the HMC administrator uninstalls the Remote Client Security Package, an error message displays stating that the Security package needs to be installed. The U.S. strong encryption is also installed by default, and can also be uninstalled by the HMC system administrator. For more information about the Remote Client, see Chapter 9, “Installing and Using the Remote Client,” on page 49. For more information about configuring your HMC for security, see Chapter 10, “System Manager Security,” on page 53.

On an AIX system, the software to install the security package is located on the Expansion Pack. The security installation image operates for both the AIX Client and the remote client; there are no separate installation images. To download the images to the remote client, the AIX system must also have IHS (IBM HTTP Server) installed and configured. Type the following Web address:

`http://HMC System Name/remote_client_security.html`

This page provides links to download the PC and Linux Security package installed on the system (U.S. or Export).

To enable or disable remote commands, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator
- Service Representative

To enable or disable remote commands, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.

2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Enable / Disable Remote Command Execution**.
4. Select the appropriate check box.
5. Click **OK**.

Configuring a Serial Adapter

You can use your HMC to configure adapters that are installed in your HMC. When performing this task, all serial adapters in the system must be configured at the same time. When adding an additional adapter, the original adapter must also be reconfigured. If you do not reconfigure the original adapter, its original definition will be lost.

To configure serial adapters, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Configure Serial Adapter**.
4. The Working window opens. Type 1 to select Configure Serial Adapter(s)
5. The configuration utility guides you through a series of questions.

   For an 8-port adapter, you must provide the following questions with the following answers:

   a. Question: How many boards would you like to install? Answer: Type the total number of 8-Port and/or 128-Port async adapters in the system.
   b. Question: Board #1. What type of board is this? (L for list) Answer: Board type 15
   c. Question: Do you want to set Altpin on this board? (y or n) Answer: No

   If two 8-port adapters are installed in the system, the HMC asks the following questions:

   a. Question: Board #2. What type of board is this? (L for list) Answer: Board type 15
   b. Question: Do you want to set Altpin on this board? (y or n) Answer: No

   For a 128-port adapter, you must provide the following questions with the following answers:

   a. Question: How many boards would you like to install? Answer: The total number of 8-Port and/or 128-Port async adapters that are installed in the HMC PC.
   b. Question: Board #1. What type of board is this? (L for list) Answer: Board type 16 (IBM 128-Port async PCI)
   c. Question: How many ports does this digiBoard have? Possible values:

      1) 8
      2) 16
      3) 24
      4) 32
      5) 40
      6) 48
      7) 56
      8) 64
      9) 72
      10) 80
      11) 88
      12) 96
      13) 104
      14) 112
      15) 120

16) 128

Board #1 How many ports? (1-16) Answer: Count the total number of Enhanced RANs you are attaching to the 128-Port async adapter and multiply by 2. Type the selection number 4), for 32 in this example, at the prompt.

d. Question: Do you want to set Altpin on this board? (y or n) Answer: No

If two 128-Port async adapters are installed in the system, the utility repeats the previous sequence of questions for each. The configuration utility guides you through a series of questions.

Note: The term C/CON is synonymous with Enhanced RAN or RAN.

a. Question: How many C/X cards do you have? Answer: Type the total number of 128-Port async adapters installed in the HMC PC.
b. Question: How many C/CONs (RANs) are connected to card 1 line 1? Answer: Type the total number of RANs on line 1. For this example, two concentrators (RANs) are connected to line 1.
c. Question: What type of wiring scheme are you going to use for card 1, line 1? Answer: A
d. Enter the type of communication mode to use on line 1. (Type L for a list) Answer: 14
e. Question: How many ports does this C/CON (RAN) support? (conc #1) Answer: 16
f. Question: How many C/CONs (RANs) are connected to card 1, line 2? Answer: Type the number of RANs connected to line 2.

Reboot your HMC to load the adapter device driver.

Configuring RS422 Ports on an 8-Port Adapter

This task allows you to switch a port from RS232 to RS422. Use this task for ports that are connected to a frame's power supply.

Note: Managed systems should continue to use the default RS232 port type.

To configure RS422 ports on an 8-Port adapter connected to the HMC, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Configure Serial Adapter**.
4. The Working window opens. Select **Configure RS422 ports on an 8-port Adapter**.
5. From the menu, select the 8-port adapter you want to configure.
6. From the menu, select the port change.

Enabling Remote Virtual Terminal Connections

Remote virtual terminal connections are disabled by default. To enable remote virtual terminal connections, you must be a member of the System Administrator role.

To enable remote virtual terminal connections, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Enable/Disable Remote Virtual Terminal Connections**. The Enable Remote Virtual Terminal window displays.
4. Select the **Enable remote virtual terminal connections** check box.
5. Click **OK**.

Changing the HMC Interface Language

You can change the language of your HMC interface by:

- Powering on the HMC

OR

- Using the Change Current Locale application

When you power on the HMC, the HMC automatically prompts you to change the locale. The locale is the language in which you want your HMC to display. If you do not respond, the HMC continues to power on with the most recently used locale.

Any user role can change the HMC's interface language.

To change your HMC's interface language when you power on the HMC, do the following:

1. Power on the HMC.
2. When you are prompted to change the locale, type the number **2** to select Change Locale. The Locale Selection window opens.
3. From the list, select the locale you want to display.
4. Click **OK**.

When the HMC completes the power-on process, it displays the language you selected.

To change your HMC's interface language by using the System Configuration application, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Change Current Locale**.
4. In the window, select the locale.
5. Click **OK**.
6. Log off the HMC interface and then log back in. For more information about logging off and logging in, see "Shutting Down, Rebooting and Logging Off the HMC" on page 29.

Chapter 9. Installing and Using the Remote Client

You can access your HMC remotely by installing and configuring the remote client on your PC. This chapter discusses how to install the remote client and Remote Client Security.

Note: Remote management does *not* allow you to do the following:

- Configure System Manager Security for certificate authority or view Overview and Status information
- Determine the level of HMC code
- Reboot the HMC interface

By default, the HMC uses a connect port of 9090 to handle the initial login communication. After successfully logging in, the initial 9090 port is closed, and a secondary port is opened in the range 30000 - 30009 for the rest of the communication. Therefore, up to 5 remote clients can be logged in simultaneously.

Installation Requirements to Support Remote Client and Remote Client Security

To use a PC to run the remote client, your computer must have the following:

- Either Microsoft Windows (supported versions include Windows NT, Windows 2000, or Windows XP) or the Linux operating system (supported versions include Red Hat 7.2 or Red Hat 7.3)
- 150 MB of free disk space on the default drive for temporary use during the installation procedure
- 150 MB of free disk space on the drive that you plan to use to install the remote client
- Minimum PC processor speed of 800 MHz
- Minimum of 256 MB of memory (512 MB of memory is recommended)

Installing and Uninstalling the Remote Client

This section describes how to install and uninstall the remote client.

Installing the Remote Client on a System Installed with Microsoft Windows

To install the remote client on a system installed with Microsoft Windows, do the following:

1. Uninstall any previous version of Web-based System Manager Remote Client. For more information, see “Uninstalling the Remote Client from a System Installed with Microsoft Windows” on page 50.
2. Type the following address in your machine’s Web browser:

   `hostname/remote_client.html`

   where *hostname* is the name of the HMC.
3. To download the **setup.exe** file to your machine, click the **Windows** link that displays on the Web page.
4. Run the **setup.exe** file to begin the installation process.
5. When the **Remote Client Installer** window displays, click **Next** to continue.
6. To install using the default location, click **Next**. Otherwise, type the desired location and click **Next**.
7. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. Click **Next** to start the installation. If any of the information shown is incorrect, click **Back** to make corrections.

8. A status window displays a message indicating the installation completed successfully or error messages if errors occurred during the installation. Click **Finish** to close the window.

Uninstalling the Remote Client from a System Installed with Microsoft Windows

To uninstall the remote client from a system installed with Microsoft Windows, do the following:

1. From the taskbar, select **Start --> Settings --> Control window**.
2. In the **Control window**, double-click the **Add/Remove Programs** icon.
3. From the list of programs on the **Install/Uninstall** tab, select **Web-Based System Manager Remote Client**.
4. Click **Add/Remove** to start the Uninstall wizard.

   Note: Earlier versions of remote client may display as **Web-based System Manager PC Client.**
5. Click **Next** in the initial window.
6. To uninstall remote client, click **Next** in the Confirmation window.
7. A status window displays a message indicating that the installation completed successfully or error messages if errors occurred during the installation. Click **Finish** to close the window.

Installing the Remote Client on a System Installed with Linux

To install the remote client on a system installed with Linux, do the following:

1. Uninstall any previous version of Linux Client on your machine. For more information, see “Uninstalling the Remote Client from a System Installed with Linux.”
2. Type the following address in your machine’s Web browser:

   hostname/remote_client.html

   where *hostname* is the name of the HMC.
3. To download the **wsmlinuxclient.exe** file to your machine, click the **Linux** link that displays on the Web page.
4. Run the **wsmlinuxclient.exe** file to begin the installation process. If the file does not run, modify the permissions on the file so that you have execute permissions. To modify the permissions, type the following at the command prompt:

   ```
   chmod 755 wsmlinuxclient.exe
   ```
5. When the Remote Client Installer window displays, click **Next** to continue.
6. To install using the default location, click **Next**. Otherwise, type the desired location and click **Next**.
7. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. Click **Next** to start the installation. If any of the information shown is incorrect, click **Back** to make corrections.
8. A status window displays a message indicating the installation completed successfully, or error messages if errors occurred during the installation. Click **Finish** to close the window.

   Note: If changes do not take effect immediately, either log off your current session and log in again, or source your **. /etc/profile** file.

Uninstalling the Remote Client from a System Installed with Linux

To uninstall the remote client from a system installed with Linux, run the following command:

installdir/_uninst/uninstall

where *installdir* is the name of the directory where the remote client is located.

Installing the Remote Client Security Package

This section describes how to install the remote client Security.

Installing Remote Client Security on a System Installed with Microsoft Windows

To install remote client Security on the system installed with Microsoft Windows, do the following:

1. Type the following Web address in your machine's Web browser:

   hostname/remote_client_security.html

   where *hostname* is the name of the HMC.
2. To download the **setupsec.exe** file to your machine, click the **Windows** link on the Web page.
3. To begin the installation process, run the **setupsec.exe** file.
4. When the Remote Client Security Installer window displays, click **Next** to continue.
5. To install using the default location, click **Next**. Otherwise, type the desired location and click **Next**.

   Note: Be sure that the location you select in this step is the same location that you selected in "Installing the Remote Client on a System Installed with Microsoft Windows" on page 49.
6. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. Click **Next** to start the installation. If any of the information shown is incorrect, click **Back** to make corrections.
7. A status window displays a message indicating the installation completed successfully, or error messages if an error occurred during the installation. Click **Finish** to close the window.

Uninstalling Remote Client Security from a System Installed with Microsoft Windows

To uninstall the remote client from a system installed with Microsoft Windows, do the following:

1. From the taskbar, select **Start --> Settings --> Control window**.
2. In the **Control window**, double-click the **Add/Remove Programs** icon.
3. From the list of programs on the **Install/Uninstall** tab, select **Remote Client Security** .
4. To start the Uninstall wizard, click **Add/Remove**.

   Note: Earlier versions of remote client Security may display as **Web-based System Manager PC Client Security.**
5. Click **Next** in the initial window.
6. To uninstall remote client Security, click **Next** in the Confirmation window.
7. A status window displays a message indicating the installation completed successfully, or error messages if errors occurred during the installation. Click **Finish** to close the window.

Installing the Remote Client Security on a System Installed with Linux

To install the remote client Security on a system installed with Linux, do the following:

1. Uninstall any previous version of remote client Security on your machine. For more information, see "Uninstalling Remote Client Security from a system installed with Linux" on page 52.
2. Type the following address in your machine's Web browser:

   hostname/remote_client_security.html

   where *hostname* is the name of the HMC.
3. To download the **setupsecl.exe** file to your machine, click the **Linux** link that displays on the Web page.

4. Run the **setupsecl.exe** file to begin the installation process. If the file will not run, modify the permissions on the file so that you have execute permissions. To modify permissions, type the following at the command prompt:

   ```
   chmod 755 setupsecl.exe
   ```

5. When the Remote Client Security Installer window displays, click **Next** to continue.
6. To install using the default location, click **Next**. Otherwise, type the desired location and click **Next**.

   Note: Be sure the location you select in this step is the same location that you selected in “Installing the Remote Client on a System Installed with Linux” on page 50.

7. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. Click **Next** to start the installation. If any of the information shown is incorrect, click **Back** to make corrections.
8. A status window displays a message indicating the installation completed successfully, or error messages if errors occurred during the installation. Click **Finish** to close the window.

   Note: If changes do not take effect immediately, either log out of your current session and log in again, or source your **. /etc/profile** file.

Uninstalling Remote Client Security from a system installed with Linux

To uninstall the remote client from a system installed with Linux, run the following command:

```
installdir/_uninstssl/uninstallssl
```

where *installdir* is the name of the directory in which your remote client resides.

Configuring Remote Client Security by Copying the Public Key File

To establish secure connections in Remote Client mode, copy the Certificate Authority’s **SM.pubkr** public key file to the **codebase** directory in the location where you installed Remote Client.

For more information about copying this key file, see “Distribute the Certificate Authority’s Public Key to Your Clients” on page 55.

Chapter 10. System Manager Security

This chapter describes configuration tasks associated with System Manager Security.

System Manager Security ensures that the HMC can operate securely in the client-server mode. 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. Each HMC System Manager server has its own private key and a certificate of its public key signed by a Certificate Authority (CA) that is trusted by the System Manager clients. The private key and the server certificate are stored in the server's private key ring file. Each client must have a public key ring file that contains the certificate of the trusted CA.

Define one HMC as a Certificate Authority. You will use this HMC to generate keys and certificates for your HMC servers and client systems. The servers are the HMCs you want to manage remotely. A unique key must be generated and installed on each server. You can generate the keys for all your servers in one action on the CA and then copy them to diskette, install them at the servers, and configure the servers for secure operation.

The client systems are the systems from which you want to do remote management. Client systems can be HMCs, AIX, or PC clients. Each client system must have a copy of the CA's public key ring file in its System Manager codebase directory. You can copy the CA public key ring file to the diskette on the CA and copy it from the diskette to each client.

Note: To configure an AIX client correctly, you must install a security fileset. For more information, see your AIX documentation.

To use the System Manager Security application, you must be a member of the System Administrator role. To ensure security during configuration, users of this application must be logged in to the HMC locally.

Configuring HMC System Manager Servers and Clients for Secure Operation

The following steps are required to configure HMC System Manager servers and clients for secure operation.

Configure One HMC as a Certificate Authority

Note: You cannot perform this function using the remote client.

Define one HMC as a Certificate Authority (CA) to generate keys and certificates for your HMC servers and clients.

A Certificate Authority verifies the identities of the HMC servers to ensure secure communications between clients and servers. To define a system as a Certificate Authority, you must be logged in as the hscroot user at the machine being defined as the internal Certificate Authority. This procedure defines a system as an internal Certificate Authority for HMC security and creates a public key ring file for the Certificate Authority that you can distribute to all of the clients that access the HMC servers.

To configure a system as a Certificate Authority, do the following:

1. In the Navigation area, click **System Manager Security** .
2. In the Contents area, click **Certificate Authority**.
3. In the System Manager Security: Certificate Authority window, click **Configure This System as a Certificate Authority**. You can also select **Configure...** from the Certificate Authority menu.

4. Use the wizard windows to complete the task.

Generate Private Key Ring Files for the HMCs That You Want to Manage Remotely

After you define the internal Certificate Authority, you can use the CA to create the private key ring files for the HMCs that you want to manage remotely.

Each HMC server must have its private key and a certificate of its public key signed by a Certificate Authority that is trusted by the HMC clients. The private key and the server certificate are stored in the server's private key ring file.

To create private key ring files for your servers, do the following:

1. In the Navigation area, click **System Manager Security**.
2. In the Contents area, click **Certificate Authority**.
3. In the System Manager Security: Certificate Authority window, click **Generate Servers' Private Key Ring Files**. You can also select **Generate Keys...** from the Certificate Authority menu.
4. In the Password window, type the certificate authority private key file password. This password was created when the system was configured as the Certificate Authority.
5. Click **OK**.
6. In the Generate Server's Private Key Ring Files window, use the help to guide you through completing the task. To view help in the windows, click **Help** to open the Help window, then move the cursor over the item for which you want to display help.
7. Click **OK** when you are finished.

Install the Private Key Ring Files and Configure Your HMC Servers as Secure System Manager Servers

After you generate the private key ring files for your HMC servers, you can copy them to a diskette and install them on the servers.

Copying Server Private Key Ring Files to Diskette

This procedure copies the servers' private key ring files to a **tar** diskette so that you can install them on your servers.

To copy the servers' private key ring files to a diskette, do the following:

1. In the Navigation area, click **System Manager Security**.
2. In the Contents area, click **Certificate Authority**.
3. In the System Manager Security: Certificate Authority window, click **Copy Servers' Private Key Ring Files to Diskette**. You can also select **Copy Servers' Keys...** from the Certificate Authority menu.
4. When the Copy Server's Private Key to Diskette dialog displays, insert a diskette. To view help in the dialog, click **Help** to open the Help window, then move the cursor over the item for which you want to display help.
5. Click **OK** to copy the servers' private key ring files.

Installing the Private Key Ring File on Each Server

This procedure installs a server's private key ring file from a **tar** diskette.

Install the private key ring files from the **tar** diskette onto each server. Repeat the following steps for each server for which you generated a private key ring file.

To install a server's private key ring file, do the following:

1. In the Navigation area, click **System Manager Security**.

2. In the Contents area, click **Server Security**.
3. In the System Manager Security: Server Security window, click **Install the private key ring for this server**. You can also select **Install Key...** from the Server Security menu.
4. In the Install Private Key Ring File window, select **tar diskette** as the source for the server private key ring files. Insert the diskette containing the server's key into the diskette drive.
5. Click **OK**.

Use the help to guide you through completing the task. To view help in the dialog, click **Help** to open the Help window, then move the cursor over the item for which you want to display help.

Configuring a System as an HMC Secure Server

Configure the system as a secure server. Repeat the following steps for each server on which you installed a private key ring file.

To configure a server as a secure server, do the following:

1. In the Navigation area, click **System Manager Security**.
2. In the Contents area, click **Server Security**.
3. In the System Manager Security: Server Security window, click **Configure this system as a secure HMC server**. You can also select **Configure...** from the Server Security menu.
4. Use the wizard windows to complete the task.

Distribute the Certificate Authority's Public Key to Your Clients

Each client must have a copy of the Certificate Authority's public key ring file (**SM.pubkr**) installed in its System Manager codebase directory. The remote client and remote client security must be installed on your client systems before you distribute the CA's public key. For more information about installing the remote client and remote client security, see Chapter 9, "Installing and Using the Remote Client," on page 49.

The public key ring file can be copied from the CA to a **tar** diskette or as a PC DOS file, then copied from the diskette onto each client.

Copying the Certificate Authority's Public Key Ring File to Diskette

Note: To copy the certificate authority's public key ring file to diskette, have a DOS-formatted diskette available for use.

To copy the Certificate Authority's public key ring file to diskette, do the following on the CA system:

1. In the Navigation area, click **System Manager Security**.
2. In the Contents area, click **Certificate Authority**.
3. In the System Manager Security: Certificate Authority window, click **Copy this Certificate Authority's Public Key Ring File to Diskette**. You can also select **Copy out CA Public Key...** from the Certificate Authority menu.
4. When the Copy CA Public Key to Diskette window opens, insert a diskette.
5. Select the type of client to which you want the public key ring file to be copied. Selecting **HMC or AIX client** writes the file to a **tar** diskette. Selecting **Remote Client** writes the file to diskette in DOS file format. Use the help to guide you through completing the task. To view help in the dialog, click **Help** to open the Help window, then move the cursor over the item for which you want to display help.
6. Click **OK** to copy the public key ring file.

Copying a Certificate Authority's Public Key Ring File from Diskette to an HMC Client

All clients must have a copy of the Certificate Authority's public key ring file (**SM.pubkr**) installed in its System Manager codebase directory.

To copy a Certificate Authority's public key ring file from diskette to an HMC client, do the following on each HMC that you want to use as a client for remotely managing HMCs:

1. In the Navigation area, click **System Manager Security**.
2. In the Contents area, click **Certificate Authority**.
3. In the System Manager Security: Certificate Authority window, click **Copy another Certificate Authorities Public Key Ring File from diskette**. You can also select **Copy in CA Public Key...** from the Certificate Authority menu.
4. When the Copy CA Public Key from Diskette window opens, insert the tar diskette that contains the copied Certificate Authority's public key ring file.

   To view help in the dialog, click **Help** to open the Help window, then move the cursor over the item for which you want to display help.
5. Click **OK** to copy the public key ring file.

To copy a Certificate Authority's public key ring file from a tar diskette to an AIX client, use the **tar** command to extract the **SM.pubkr** file to the **/usr/websm/codebase** directory.

To copy a Certificate Authority's public key ring file from diskette to a Remote Client, use a DOS **copy** command to copy the **SM.pubkr** file into the codebase directory in the location where you installed Remote Client.

Viewing Configuration Properties

After the security configuration has been completed, you can view the properties of the Certificate Authority (CA) and of any server.

To view CA properties, do the following:

1. In the Navigation area, select your local host.
2. Underneath the local host, click the **System Manager Security** icon.
3. Click **Certificate Authority**.
4. Select **Properties**.
5. Type the password.

Note: This window provides read-only information for the CA.

To view a server's properties, do the following on the server:

1. In the Navigation area, select your local host.
2. Underneath the local host, click the **System Manager Security** icon.
3. Click **Server Security**.
4. Select **View properties for this server** from the task list.

Note: This window provides read-only information for the server.

Configure HMC Object Manager Security

Before performing this task, you must install the server private key ring file on the HMC. You can configure Object Manager Security to switch between plain sockets and SSL protocols.

To configure HMC Object Manager Security, do the following:

1. In the Navigation area, select your local host.
2. Underneath the local host, click the **System Manager Security** icon.
3. Click **Object Manager Security**.

4. Select **Configure Object Manager Security**.
5. Select a socket mode.
6. Click **OK**.

Chapter 11. Inventory Scout Services

This chapter provides information about Inventory Scout Services, a tool that surveys managed systems for hardware and software information. Inventory Scout provides an automatic configuration mechanism and eliminates the need for you to manually reconfigure Inventory Scout Services. Depending on the levels of your HMC and partition software, you might be required to manually configure partitions that you create in order to perform Inventory Scout tasks. Depending on your HMC level, you may also have to reconfigure Inventory Scout Services whenever you change partition information.

You can use the HMC to perform the following Inventory Scout Services tasks:

- Inventory Scout Services Profile Configuration
- Conduct Microcode Survey
- Collect VPD Information
- Restart Inventory Scout Daemon

Configuring the Inventory Scout Services Profile

To set up Inventory Scout Services for each managed system and partition, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To configure Inventory Scout Services, activate all of the partitions in the managed system.

To configure a partition for Inventory Scout Services, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Inventory Scout Services** icon.
3. In the Contents area, click **Inventory Scout Profile Configuration**. The Inventory Scout Configuration Assistant window opens.
4. Select the managed system you want to configure and click **Next**.
5. A list of partitions, along with each partition's configuration status, displays. Systems that have status of *automatically configured* do not require configuration. Partitions listed as *not configured* must be manually configured. For more information about manually configuring Inventory Scout Services, see "Manually Configuring Inventory Scout Services."

Manually Configuring Inventory Scout Services

This wizard helps you set up Inventory Scout Services for each system managed by the HMC, and for each logical partition running an instance of AIX. All partitions must be either auto configured or manually configured in order to conduct microcode surveys or collect VPD.

Notes:

1. The default listening port for Inventory Scout Services is 808.
2. If a system has been powered on using the Full System Partition power-on option, configure the Full System Partition to use Inventory Scout Services.
3. You must also do the following for each partition:
   - Set up a password for the Inventory Scout Services user ID.
   - Set up the operating system to automatically start the Inventory Scout Services daemon whenever the partition is rebooted.

For more information about configuring your operating system, see the documentation provided with your operating system.

To manually configure Inventory Scout Services for each managed system and partition, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Inventory Scout Services** icon.
3. In the Contents area, click **Inventory Scout Profile Configuration**. The Inventory Scout Configuration Assistant window opens.
4. From the list, select a managed system for which you want to configure Inventory Scout Services.
5. Click **Next**.
6. The partitions are displayed, along with their configuration status. From the list, select the partition you want to configure.
7. Click **Next**. The next window identifies the selected partition.
8. Type the following:
   - Partition password (for the AIX partition, this password is the invscout password. It must first be set by the AIX administrator on each partition - for example, by using the **passwd invscout** command.)
   - Inventory Scout listening port (default is 808).
   - IP address of the AIX partition

   Note: If the IP address is not detected by the HMC, Service Focal Point is not configured properly. For more information about configuring Service Focal Point, see “Service Focal Point Settings” on page 132.
9. To configure additional partitions, you can click either the **Next** or **Previous** buttons.

   OR

   Click **Done** to complete the partition configuration and return to the previous window.

Collecting Vital Product Data Information

Use this option to collect the Vital Product Data (VPD) for the specified managed system into a file.

Note: To ensure that the survey data is accurate, VPD collection requires that all partitions be active.

To collect the managed system’s VPD, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To collect the managed system’s VPD, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Inventory Scout Services** icon.
3. In the Contents area, click **Collect VPD information**.
4. From the list, select the name of the managed system for which you want to collect the VPD.
5. Click **Next**.
6. The wizard requests confirmation about the managed system, and then prompts you to insert a blank, DOS-formatted diskette into the HMC diskette drive.
7. Click **Finish**. The file containing the VPD is then copied to the diskette in the specified drive.

Restarting Inventory Scout Services

To survey the HMC VPD and microcode remotely, you can restart the Inventory Scout Services daemon. If the daemon stops running, or if you need to stop and then restart the daemon, use this task to start the daemon. If the daemon is already running, this task stops the daemon, and then restarts it.

To restart the Inventory Scout daemon, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative
- Operator

To restart the Inventory Scout daemon, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Inventory Scout Services** icon.
3. In the Contents area, click **Restart Inventory Scout Daemon**.
4. Click **Restart**.

Chapter 12. Using Two HMCs Connected to One Managed System

This chapter describes how to perform operations on two HMCs connected to one managed system.

Each system that supports a Hardware Management Console has two serial port connections, so that you may optionally attach a second HMC to the same system. The benefits of using two HMCs are as follows:

- Ensures that access to the HMC management function capabilities are not interrupted
- Ensures access if the network is down

Working with Two HMCs

In configurations with two HMCs, 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.

To avoid basic conflicts, mechanisms in the communication interface between HMCs and the managed systems allow an HMC to temporarily take exclusive control of the interface, effectively locking out the other HMC. Usually this locking is done only for the duration of time it takes to complete an operation, after which the interface is available for further commands. HMCs are also 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 select 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 selects to activate a partition, and a short time later, a user on the other HMC selects to power off the system, the system will power off. Effectively, any sequence of commands that you can do from a single HMC is also permitted when your environment contains redundant HMCs. For this reason, it is important to carefully consider how you want 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, is 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 may be necessary to manually release the lock. For more information about this task, see “Releasing an HMC Lock on the Managed System” on page 261.

Other Considerations for Redundant HMCs

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 the 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, enable Service Agent on only one HMC.

Perform HMC software maintenance separately on each HMC, at separate times, so that there is no interruption in accessing HMC function. This situation allows one HMC to run at the new fix level, while the other HMC can continue to run at the previous fix level. Make sure that both HMCs are moved to the same fix level as soon as possible.

Chapter 13. Using One HMC to Connect to More Than One Managed System

This chapter describes how to use one HMC to connect to more than one managed system.

Connecting One HMC to More Than One Managed System

Configuring a Serial Adapter

You can use your HMC to configure adapters that are installed in your HMC. When performing this task, all serial adapters in the system must be configured at the same time. When adding an additional adapter, the original adapter must also be reconfigured. If you do not reconfigure the original adapter, its original definition will be lost.

To configure serial adapters, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Configure Serial Adapter**.
4. The Working window opens. Type 1 to select Configure Serial Adapter(s)
5. The configuration utility guides you through a series of questions.

   For an 8-port adapter, you must provide the following questions with the following answers:

   a. Question: How many boards would you like to install? Answer: Type the total number of 8-Port and/or 128-Port async adapters in the system.
   b. Question: Board #1. What type of board is this? (L for list) Answer: Board type 15
   c. Question: Do you want to set Altpin on this board? (y or n) Answer: No

   If two 8-port adapters are installed in the system, the HMC asks the following questions:

   a. Question: Board #2. What type of board is this? (L for list) Answer: Board type 15
   b. Question: Do you want to set Altpin on this board? (y or n) Answer: No

   For a 128-port adapter, you must provide the following questions with the following answers:

   a. Question: How many boards would you like to install? Answer: The total number of 8-Port and/or 128-Port async adapters that are installed in the HMC PC.
   b. Question: Board #1. What type of board is this? (L for list) Answer: Board type 16 (IBM 128-Port async PCI)
   c. Question: How many ports does this digiBoard have? Possible values:

      1) 8
      2) 16
      3) 24
      4) 32
      5) 40
      6) 48
      7) 56
      8) 64
      9) 72
      10) 80
      11) 88
      12) 96

13) 104

14) 112

15) 120

16) 128

Board #1 How many ports? (1-16) Answer: Count the total number of Enhanced RANs you are attaching to the 128-Port async adapter and multiply by 2. Type the selection number 4), for 32 in this example, at the prompt.

d. Question: Do you want to set Altpin on this board? (y or n) Answer: No

If two 128-Port async adapters are installed in the system, the utility repeats the previous sequence of questions for each. The configuration utility guides you through a series of questions.

Note: The term C/CON is synonymous with Enhanced RAN or RAN.

a. Question: How many C/X cards do you have? Answer: Type the total number of 128-Port async adapters installed in the HMC PC.
b. Question: How many C/CONs (RANs) are connected to card 1 line 1? Answer: Type the total number of RANs on line 1. For this example, two concentrators (RANs) are connected to line 1.
c. Question: What type of wiring scheme are you going to use for card 1, line 1? Answer: A
d. Enter the type of communication mode to use on line 1. (Type L for a list) Answer: 14
e. Question: How many ports does this C/CON (RAN) support? (conc #1) Answer: 16
f. Question: How many C/CONs (RANs) are connected to card 1, line 2? Answer: Type the number of RANs connected to line 2.

Reboot your HMC to load the adapter device driver.

Configuring RS422 Ports on an 8-Port Adapter

This task allows you to switch a port from RS232 to RS422. Use this task for ports that are connected to a frame's power supply.

Note: Managed systems should continue to use the default RS232 port type.

To configure RS422 ports on an 8-Port adapter connected to the HMC, do the following:

1. In the Navigation area, click the **HMC Maintenance** icon.
2. In the Contents area, double-click the **System Configuration** icon.
3. In the Contents area, click **Configure Serial Adapter**.
4. The Working window opens. Select **Configure RS422 ports on an 8-port Adapter**.
5. From the menu, select the 8-port adapter you want to configure.
6. From the menu, select the port change.

Working with More Than One Managed System

After the serial adapters and cables are connected to the managed systems and you have configured the serial adapters using your HMC, each managed system appears automatically in the Navigation area of the HMC interface. You can then manage each system as you would any other system on the HMC.

Chapter 14. User Management

This chapter discusses how an HMC system administrator can manage users and assign roles. To use the User Management application, first determine who will use the HMC. Next, you can assign a role to that user to assign appropriate access. For example, you can create general users and assign operator roles to these users so that they can perform basic HMC tasks.

Note: You must create a user named hscpe so that your software support representative has access to perform fixes on the HMC code. This user name is reserved for your support representative and is considered a ″hidden″ role. Do not assign the hscpe user name to one of your users. For more information about creating users and assigning roles, see “Creating a User” on page 72.

Overview of Roles

Each HMC user can be a member of one of six different roles. Each of these roles allows the user to access different parts of the HMC. The user roles specified by the HMC are as follows:

- System Administrator
- Advanced Operator
- Service Representative
- Operator
- User Administrator
- Viewer

Each role is described as follows:

System Administrator
The System Administrator acts as the root user, or manager of the HMC system. The System Administrator has unrestricted authority to access and modify most of the HMC system.

Advanced Operator
An Advanced Operator can perform some partition or system configuration and has access to some user-management functions.

Service Representative
A Service Representative is an employee who is at your location to install or repair the system.

Operator
An Operator is responsible for daily system operation.

User Administrator
A User Administrator can perform user-management tasks, but cannot perform any other HMC functions.

Viewer
A Viewer can view HMC information, but cannot change any configuration information.

Roles and Tasks

The following table lists all roles and the tasks available to each:

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
Problem Determination						
Problem Determination tasks are available only to product support engineers.						

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
Software Maintenance: HMC						
Back up Critical Console Data	X	X	X	X		
Format Media	X	X	X	X		
Install Corrective Service	X		X			
Save Upgrade Data	X	X	X			
Software Maintenance: Frame						
Receive Corrective Service	X	X	X	X		
Install Corrective Service	X		X			
System Configuration						
Customize Console Date and Time	X	X	X	X		
Customize HMC Network Settings	X	X	X			
Schedule Operations	X	X				
View Console Events	X	X	X			X
Test Network Connectivity	X	X	X			
Change Current Locale	X	X	X	X		
Configure Serial Adapter	X	X	X			
Enable/Disable Remote Virtual Terminal	X	X				
Enable/Disable Remote Command Execution	X	X	X			
User Management Tasks						
Create Users	X				X	
Modify Users	X				X	
View User Information	X				X	X
Delete Users	X				X	
Change User Password	X				X	
Managed System Tasks						

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
Open Terminal Session	X	X	X	X		
Close Terminal Session	X	X	X	X		
Release Lock on Managed System	X	X	X			
Power On Managed System	X	X	X	X		
Power Off Managed System	X	X	X			
Delete Managed System	X					
View Managed System Properties	X	X	X	X	X	X
Modify Managed System Policies	X	X				
Rebuild HMC Software Connection	X	X	X	X	X	
Back up Profile Data	X	X	X			
Restore Profile Data	X	X	X			
Remove Profile Data	X	X	X			
Initialize Profile Data	X					
Refresh Frame	X	X	X	X	X	X
Initialize Frame	X		X			
View Frame Properties	X	X	X	X	X	X
Deactivate Service Processor	X		X			
Reset Service Processor	X		X			
Deactivate Frame's I/O Drawers	X		X			
System Profile Tasks						
Create System Profile	X	X				
Modify System Profile	X	X				

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
View System Profile	X	X	X	X	X	X
Activate System Profile	X	X	X	X		
Delete System Profile	X					
Copy System Profile	X	X				
Validate System Profile	X	X	X	X		
Partition Tasks						
Create Partition	X	X				
Setup Affinity Partition	X	X				
View Partition	X	X	X	X	X	X
Modify Partition	X	X				
Update Affinity Partition	X	X				
Activate Partition	X	X	X	X		
Delete Partition	X					
DLPAR Adapters (all tasks)	X					
DLPAR Processors (all tasks)	X					
DLPAR Memory (all tasks)	X					
Remove Affinity Partition	X	X				
Reset Operating System	X	X	X			
Shut Down Operating System	X	X	X			
Open Terminal Session	X	X	X	X		
Close Terminal Session	X	X	X	X		
Partition Profile Tasks						
Create Partition Profile	X	X				
View Partition Profile	X	X	X	X	X	X
Copy Partition Profile	X	X	X			
Delete Partition Profile	X					

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
Activate Partition Profile	X	X	X	X		
Modify Partition Profile	X	X				
Change Default Profile	X	X				
Service Focal Point Tasks						
Setting Service Focal Point	X		X			
Use Hardware Services Functions	X		X			
Select Serviceable Events	X		X			
View Service Focal Point Setting	X	X	X	X		X
View Hardware Services Functions	X	X	X	X		X
View Serviceable Events	X	X	X	X		X
Inventory Scout Services Tasks						
Configure Profile	X	X	X			
Conduct Microcode Survey	X	X	X			
Collect VPD Information	X	X	X			
Restart Inventory Scout Daemon	X	X	X	X		
Service Agent Tasks						
Register and Customize Service Agent	X	X	X	X		
Stop Service Agent	X	X	X	X		
Change Modes	X	X	X	X		
Start Processes	X	X	X	X		
Stop Processes	X	X	X	X		
Enable E-mail Notification	X	X	X	X		
Configure HealthCheck Interval	X	X	X	X		

Task	Sys. Admin	Adv. Operator	Serv. Rep	Operator	User Admin	Viewer
Enable Performance Management Data Collection	X	X	X	X		
Capacity on Demand Tasks						
Accept CUoD License	X	X	X	X		
Permanently Activate CUoD Resources	X					
View Processor Capacity Settings	X					
Use Processor Activate Immediate	X					
Disable Activate Immediate for Processors	X					
View Memory Capacity Settings	X					
Use Memory Activate Immediate	X					
Disable Activate Immediate for Memory	X					

User Management Tasks

You can perform the following tasks using the Users application:

Creating a User

This process allows you to create a user.

To create users, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To create a user, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, click the **Users** icon.
3. Select **Users** from the menu.
4. Select **New**.
5. Select **User** from the cascade menu.
6. In the **Login Name** field, type the login name.
7. (optional) In the **Full Name** field, type the full name.
8. To select a role for your new user, click an item in the role list.
9. Click **OK**. The Change User Password window opens.

10. In the first field of the Change User Password window, type the user's password.
11. Type the same password again in the **Retype new password** field.
12. Click **OK**.

The new user displays in the Contents area.

Note: It is strongly recommended that you create a user named `hscpe` for software fixes and updates from your software support representative. Support representatives may need to log in to your HMC using this user name when they are analyzing a problem.

Editing User Information

To edit user information, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To edit user information, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **Users** icon.
3. In the Contents area, right-click the appropriate User icon.
4. Select **Properties**.
5. Edit the user's base information (Login name, Full name, and User role).
6. Click **OK**. The Change User Password window opens.
7. Type the user's password in each field.
8. Click **OK**.

Viewing User Definitions

Sometimes it is useful to review a user's definitions to make sure you have correctly configured the user's access. For more information about roles and access, see "Roles and Tasks" on page 67.

To view user definitions, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To view a user's definitions, including the assigned Login name, Full name, and User role, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **Users** icon.
3. In the Contents area, right-click the appropriate User icon.
4. Select **Properties**.

At this point, you can also edit any user information.

Deleting a User

To delete a user, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To delete a user from the system, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **Users** icon.
3. In the Contents area, right-click the appropriate User icon.
4. Select **Delete.**

5. Click **OK** to confirm that you want to delete this user.

The user is removed from the contents area and no longer has access to the HMC management environment. Some reserved users cannot be deleted.

Changing Passwords

To change user passwords, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To change a user's password, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **Users** icon.
3. In the Contents area, right-click the appropriate User icon.
4. Select **Change Password**.
5. Type the new password in the first field.
6. Confirm the new password by typing it again in the **Retype new password** field.
7. Click **OK**.

Chapter 15. Basic System Management Tasks

This chapter describes how to perform system and frame management tasks. This chapter also includes information about system profiles.

You can perform the tasks discussed in this chapter when the managed system is selected in the Contents area. A managed system is shown underneath a frame in the Contents area. A *frame* manages a collection of managed systems.

The HMC communicates with the managed system to perform various system management, service, and partitioning functions. Systems connected to an HMC are recognized automatically by the HMC, and are then shown in the Contents area.

You can connect up to two HMCs to each managed system by using the serial cable that was provided with the HMC. For more information about using two HMCs connected to one managed system, see Chapter 12, “Using Two HMCs Connected to One Managed System,” on page 63. You can also manage multiple systems with one HMC. For more information about using one HMC with multiple managed systems, see Chapter 13, “Using One HMC to Connect to More Than One Managed System,” on page 65.

To view more information about the managed system, expand the **Server and Partition** folder in the Navigation area. Then, click the **Server Management** icon. The Contents area expands to show the frame, which you can then expand to show information about the managed system, including its name, its state, and the operator panel value.

To expand your view of the managed system’s properties, click the plus sign (+) next to the managed system’s name to view its contents.

In the Contents area, you can also select the managed system by right-clicking on the managed system icon to perform the following:

- Power the managed system on or off
- View the managed system’s properties
- Open and close a terminal window
- Create, restore, back up, and remove system profile data
- Rebuild the managed system
- Release the HMC lock on this managed system
- Delete the managed system from the HMC graphical user interface

You can also access these options by clicking on the managed system and then clicking **Selected** on the menu.

Powering On the Managed System

You can use your HMC to power on the managed system.

To power on the managed system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Operator
- Service Representative

To power on the managed system, do the following:

1. In the Navigation area, open the **Server and Partition** folder.

2. Click the **Server Management** icon.
3. In the Contents area, select the managed system.
4. From the menu, click **Selected –> Power On**.

   You are asked to select a power-on mode from the following:

   - Partition Standby
   - Full System Partition
   - System Profile
   - Power On Autostart

   The next section discusses each of these power-on modes.

Note: You must power off your managed system to switch between using the Full System Partition and using either logical or affinity partitions. You must also power off the system between activating logical partitions and affinity partitions.

Partition Standby

The Partition Standby power-on mode allows you to create and activate logical partitions. When the Partition Standby power-on is completed, the operator panel on the managed system displays `LPAR...`, indicating the managed system is ready for you to use the HMC to partition its resources.

Note: The Full System Partition is listed as *Not Available* because the managed system was powered on using the Partition Standby option.

For more information about partitions, see Chapter 4, “Partitioning,” on page 19.

Full System Partition

The Full System Partition power-on mode allows you to use all of the system’s resources on one operating system after the system has been powered on. This is the traditional single-system method of using your system’s resources.

The physical operator panel on your managed system displays progress codes when you boot the system to this mode.

Power-On Options

If you select the Full System Partition power-on mode, you can then select one of the following boot options:

Power On Normal
: This option boots the operating system as previously specified in the SMS settings. Depending on what is specified in the SMS settings, different boot types may result. Refer to the documentation provided with your managed system for a complete description of this power on option.

Power On Diagnostic Default Boot List
: This option is similar to Power On Diagnostic Stored Boot List option, except the system boots using the default boot list that is stored in the system firmware.

Power On Diagnostic Stored Boot List
: This option causes the system to perform a service mode boot using the service mode boot list saved on the managed system. If the system boots AIX from the disk drive and AIX diagnostics are loaded on the disk drive, AIX boots to the diagnostics menu.

  Using this profile to boot the system is the preferred way to run online diagnostics.

Power On SMS
: This option boots to the System Management Services (SMS) menus. The SMS menus include:

  - Password Utilities

- Display Error Log
- Remote Initial Program Load Setup
- SCSI Utilities
- Select Console
- MultiBoot
- Select Language
- OK Prompt

For more information about SMS menus, see the *PCI Adapter Placement Reference*, order number SA38-0538.

Power On Open Firmware OK Prompt
This profile is used only by service representatives to obtain additional debug information. When this selection is enabled, the system boots to the open firmware prompt.

For more information about these power-on options, see the service documentation for your managed system.

For more information about the Full System Partition, see “Full System Partition” on page 19.

System Profile

The System Profile option powers on the system according to a predefined set of profiles.

Note: The profiles are activated in the order in which they are shown in the system profile.
For more information about system profiles, see “Profiles” on page 20.

Power-On Autostart

This option powers on the managed system to partition standby mode and then activates all partitions that have been powered on by the HMC at least once. For example, if you create a partition with four processors, use DLPAR to remove one processor, and then shut down the system, the Power on Autostart option activates this partition with three processors. This is because the three-processor configuration was the last configuration used, and the HMC ignores whatever you have specified in the partition’s profile. Using this option, the partitions boot to AIX, even if some of the partitions had previously been defined to use another power on option.

For more information about partitions, see Chapter 4, “Partitioning,” on page 19.

Powering Off the Managed System

You can also use your HMC to power off the managed system. Before you power off the managed system, ensure that all partitions have been shut down and their states have changed from *Running* to *Ready*.

To shut down a partition, do the following:

1. In the Navigation area, click the **Server and Partition** folder.
2. In the Contents area, click the **Server Management** icon.
3. In the Contents area, click the managed system’s icon to expand the tree.
4. Select the partition that you want to shut down.
5. Select **Operating System —> Shut down**.

To power off the managed system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

- Service Representative

To power off the managed system, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected –> Power Off**.

When you power off the managed system, each partition associated with that managed system also powers off.

Viewing Managed System Properties

You can view your managed system's configuration and capabilities.

Any user can view managed system properties.

To view your managed system's properties, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected**.
3. Click **Properties**.

   If you have powered on your system using the Full System Partition option, the HMC displays the system's name, partition capability, state, serial number, model and type, and policy information. A system that is powered on using the Partition Standby option displays this information, as well as available and assigned processors, memory, I/O drawers and slots, and policy information. The Processor tab displays information that is helpful when performing Dynamic Logical Partitioning processor tasks.

   Use the Processor tab to view the processor status, the processor state, and whether a processor is assigned to a partition. The information in the Processor tab is also helpful when you need to know if processors are disabled and therefore cannot be used by any partition. For more information about recovering resources, see Appendix E, "Error Messages and Recovery Information," on page 203.

Managing Profile Data

You can back up, restore, initialize, and remove profiles that you have created. This section describes each of these options.

Backing Up Profile Data

To back up profile data, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

Note: This is not a concurrent procedure. When the data is restored, the managed system powers on to Partition Standby.

To back up profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected—> Profile Data —> Backup**.
3. Type the name you want to use for this backup file.
4. Click **OK**.

Restoring Profile Data

Selecting this menu item restores profile data to the system from the local file system.

To restore profile data, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To restore profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, choose **Selected—> Profile Data —> Restore**.
3. From the menu, select **Profile Data**.
4. Select the profile information you want to restore from the list of backup files.
5. Select a restore option from the following list, and then click **OK**.

   Full restore from selected backup file
   This option restores all profile data using your backup file *only*. Profile modifications performed after the selected backup file was created will be lost.

   Backup priority - merge current profile and backup
   This option merges the stored backup with recent profile activity. If information conflicts, the stored backup data is restored over the recent profile activity.

   Managed system priority - merge current profile and backup
   This option merges recent profile activity with the stored backup. If information conflicts, the recent profile activity is restored over the stored backup data.

Initializing Profile Data

When you initialize profile data, you return the HMC to its original state. After you perform this task, any profiles that you created are erased.

To initialize profile data, you must be a member of one of the following roles:

- System Administrator

To initialize profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, choose **Selected—> Profile Data —> Initialize**.
3. A warning message window opens. If you are sure you want to initialize profile data, click **Yes**.

Removing Profile Data

To remove stored profile data, you must be a member of one of the following roles:

- System Administrator
- Service Representative
- Advanced Operator

To remove stored profile data, do the following:

1. In the Contents area, select the managed system.
2. From the menu, choose **Selected—> Profile Data —> Remove**.
3. Select the profile data that you want to remove.
4. Click **OK**.

Deleting the Managed System from the Contents Area

If you no longer want to manage a particular system, you can delete it from the Contents area.

Note: Do not disconnect the serial cable from the hardware before you delete the managed system from the Contents area.

To delete the managed system from the Contents area, you must be a member of the System Administrator role.

To delete the managed system from the Contents area, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected**.
3. Select **Delete** from the drop-down menu.
4. Click **Yes** to delete the managed system from the Contents area.
5. Disconnect the serial cable from the managed system.

The managed system's icon is removed from the Contents area, and the connection is broken between the HMC and the managed system.

Rebuilding the Managed System

Rebuilding the managed system acts much like a refresh of the managed system information. Rebuilding the managed system is useful when the system's state indicator in the Contents area is shown as *Recovery*. The Recovery indicator signifies that the partition and profile data stored in the managed system must be refreshed.

This operation is different from performing a refresh of the local HMC panel. In this operation, the HMC reloads information stored on the managed system.

Any user can rebuild the managed system.

To rebuild the managed system, do the following:

1. In the contents area, select the managed system.
2. From the menu, click **Selected**.
3. Click **Rebuild Managed System**.

After you select **Rebuild Managed System**, current system information displays.

Unlocking an HMC Lock on the Managed System

Perform this task only if you have two HMCs connected to your managed system and one of the HMCs is not responding. For more information, see "Releasing an HMC Lock on the Managed System" on page 261.

Resetting the Operating System on a Partition

The HMC enables the operating system on a partition to be reset when errors are encountered in the operating system. The system can undergo either a soft or hard reset, as follows:

Soft Reset

Soft reset actions are determined by your operating system's policy settings. Depending on how you have configured these settings, the operating system might do the following:

- Perform a dump of system information
- Restart automatically

For more information about configuring your operating system's policy settings, see your operating system documentation.

Hard Reset

A hard reset virtually powers off the system.

Attention: Issuing a hard reset forces termination and can corrupt information. Use this option *only* if the operating system is disrupted and cannot send or receive commands.

To reset the operating system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To reset the operating system on a partition, do the following:

1. In the Contents area, select the partition running the operating system you want to reset.
2. In the menu, click **Selected—> Operating System —> Reset**.
3. Select the type of operating system reset.
4. Click **Yes**.

Shutting Down an Operating System

You can use the HMC interface to run an AIX shutdown command on a partition. You can perform this task if the operating system supports this function. To shut down AIX on a partition, do the following:

1. In the Contents area, select the partition running the operating system you want to reset.
2. In the menu, click **Selected**.
3. Select **Operating System**.
4. Select **Shut Down**.
5. Select the type of shutdown you want to perform. For more information about AIX **shutdown** command flags, see your AIX documentation.
6. Click **OK**.

Documentation for the AIX operating system is available from the IBM @server pSeries Information Center at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base. Select **AIX documentation**. The *AIX Documentation* CD contains the base set of publications for the operating system, including system-management and end-user documentation.

Managing a Frame of Managed Systems and Resources Connected to the HMC

A *frame* is a collection of managed systems and resources. Each frame is shown in the Contents area as the root of a resource tree; managed systems are listed underneath each frame.

Any user can refresh a frame.

If a managed system that is part of a frame does not display under the frame in the Contents area, refresh the frame as follows:

1. In the Contents area, select the frame.
2. From the menu, click **Selected –> Refresh**.

The Contents area is updated to show the latest frame information.

If your managed system is a frame that contain multiple managed systems and resources, you can use your HMC to perform the following frame-management tasks:

- Initialize a frame's associated managed systems and resources
- View frame properties, such as machine type, model, and I/O information
- Deactivate and reset the managed system's CSP
- Deactivate I/O drawers

If your managed system is not a frame that contains multiple managed systems and resources, these tasks are not enabled.

Initializing a Frame's Managed Systems and Resources

The frame must be manually powered on before its managed systems and other resources can be powered on.

Perform this task the first time that the frame is plugged into the wall, and whenever resources in a frame have been added, removed, or recabled.

To initialize a frame's managed systems and resources, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To power on the managed resources in the frame, do the following:

1. In the Contents area, select the frame.
2. From the menu, click **Selected –> Initialize**. The **Frame Initialization** window opens.
3. Click **Yes**.

Viewing Frame Properties

The frame properties panel displays all of the managed systems and I/O drawers that exist in the frame.

To view frame properties, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To view frame properties, do the following:

1. In the Contents area, select the frame.
2. In the menu, click **Selected—> Properties**.

Deactivating a Managed System's Processor Subsystem

This option allows you to remove the 350V dc bulk power coming into the DCA(s) in the managed system. This is also known as deactivating the managed system. When the managed system is deactivated, standby power is removed from the processor subsystem. The managed system is usually deactivated by service personnel to perform service or repair actions.

To deactivate a managed system's service processor, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To deactivate a managed system's service processor, do the following:

1. In the Contents area, select the frame.

2. From the menu, click **Selected—> Deactivate—> Service Processor**. The **Deactivate Service Processor** window opens and displays managed systems.
3. Select the managed system whose service processors you want to deactivate.
4. Click **OK**.

Deactivating a System's I/O Drawers

This option allows you to remove the 350V dc bulk power coming into the DCAs in an I/O drawer. This is also known as deactivating the I/O drawer. An I/O drawer is usually deactivated by service personnel to perform service or repair actions.

To deactivate the I/O drawers associated with the frame, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To deactivate the I/O drawers associated with the frame, do the following:

1. In the Contents area, select the frame.
2. In the menu, click **Selected—> Deactivate—> I/O Drawer**. The **Deactivate I/O Drawer** window opens and displays the I/O drawers associated with the frame.
3. Select the I/O drawer that you want to deactivate.
4. Click **OK**.

Resetting a Managed System's Service Processor

This option allows you to reset a service processor on a managed system associated with the frame. The service processor may need to be reset if a hardware error has occurred on the managed system.

Attention: If partitions are running on a managed system whose service processor is reset, the partitions will be halted abruptly when you issue the reset. If possible, shut down the partitions before continuing.

To reset a managed system's service processor, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To reset a managed system's service processor, do the following:

1. In the Contents area, select the frame.
2. From the menu, click **Selected—> Reset—> Service Processor**. The **System Reset** window opens and displays managed systems.
3. Select the managed system that you want to reset.
4. Click **OK**.

Chapter 16. Using Capacity Upgrade on Demand

Capacity Upgrade on Demand (CUoD) adds operational and configuration flexibility. Available for a fee, CUoD allows you to add additional resources as they are needed. Processors and memory can be brought online to meet increasing workload demands. If the system is configured for dynamic LPAR, this can be accomplished without impacting operations.

These features have significant value for those who want to upgrade without disruption, enhance their system RAS (reliability, availability, service ability) characteristics, or simply grow with a finer level of granularity.

The CUoD features available for your system allow the system to be manufactured (or upgraded in your locale) with inactive resources, such as processors and memory. The hardware is delivered with these features built in, ready to be activated when you need them. If your system is ordered with a CUoD feature, you can activate the feature and pay for the increased processing power as your needs grow.

CUoD features enable you to start small, and then increase your processing capacity without disrupting any of your current operations.

CUoD standby features are turned on with an activation code purchased as an upgrade (MES) feature. Orders are entered through the AAS administrative system by the IBM sales representative or IBM Business Partner, just as for any other feature.

In addition to placing an order for the appropriate feature, certain system data must be sent to IBM either through the CUoD Web site or by using the Electronic Service Agent. After IBM verifies that a valid order has been placed and the necessary system data has been provided, the activation code is posted to the CUoD Web site and a printed order confirmation is sent with the activation code. Transmission of the code constitutes shipping of the feature that was ordered.

Note: CUoD is not supported on systems running Linux in the full system partition.

Types of CUoD

After your system with the ordered CUoD features is delivered, you can activate CUoD features in the following ways:

- Permanent Capacity Upgrade on Demand (CUoD) for processors
- Permanent Capacity Upgrade on Demand (CUoD) for memory v
- On/Off Capacity on Demand - for processors
- Trial Capacity on Demand - for processors or memory

Processors on Demand

When you activate processor CUoD, additional processors become activated and usable on your system. Processor CUoD enables you to handle business peaks or add new workloads without having to reboot the server.

Memory on Demand

When you activate memory CUoD features, additional memory becomes activated and usable on your system. Memory CUoD enables you to handle business peaks or add new workloads without having to reboot the server.

Note: The same memory balancing rules apply for Memory CUoD as with traditional memory with the convention that all memory on a CUoD feature should be viewed as activated when applying the rule.

Activation Options

The pSeries processor CUoD features can be activated by one of the following methods:

- Permanent
- On/Off
- Trial

Memory CUoD features can be activated by either of the following methods:

- Permanent
- Trial

Permanent Capacity on Demand

If a resource is activated on a permanent basis, it becomes available for use on your server permanently. Activating processors or memory is done using the HMC interface.

For more information about activating CUoD resources permanently, see “Permanent Activating Process for Capacity Upgrade on Demand” on page 87.

On/Off Capacity on Demand

The On/Off activation allows you to start and stop using processors as your needs change. The user purchases (with feature codes) the amount of usage time they wish and are given an On/Off activation code. When entered, the On/Off activation code loads the systems with the entitled amount of processor usage days. The user then has the ability to activate and de-activate processors as needed. While processors are activated, usage time is charged against the entitled usage days. When processors are de-activated, the charges are stopped. Once the amount of entitled usage is consumed, the user can either purchase additional activation time or discontinue their participation in the On/Off offering.

Processor usage is measured in day increments and is independent of the time of the day used. At initial activation, each processor being used is charged for one day of use. An additional charge of a processor day is made for each 24 hours of continuous usage after the initial charge. Turning the processors on and off is performed using the HMC console interface.

For more information, see “Managing On/Off Capacity on Demand Processors” on page 88.

Trial Capacity on Demand

Trial Capacity on Demand enables CUoD features to be activated one time for a period of 30 consecutive days. If your system was ordered with CUoD features and they have not yet been activated, you can turn the features on for a one-time trial period. With the trial capability, you can gauge how much capacity you might need in the future, if you decide to permanently activate the resources you need. Alternatively, the Trial Capacity on Demand function can be used to immediately activate resources while processing an order for a permanent activation code.

For more information, see “Using the Trial CoD Feature” on page 89.

You can use Capacity Upgrade on Demand on the HMC to do the following:

- Display license agreements
- Display the extra resources preinstalled on your managed system
- Type a resource activation code
- Immediately activate extra resources to try for a limited time
- Disable Trial CoD resource capacity
- Activate extra resources permanently
- Enable CUoD features to be activated one time for a period of 30 consecutive days

- Display CUoD status messages

Permanent Activating Process for Capacity Upgrade on Demand

The CUoD process begins when you determine a potential need for more processing capability in the future and want to have the hardware installed on the server now. If CUoD features are ordered for your server, they are included in the server when it is delivered. When additional processors or amounts of memory become a necessity, and you want to permanently add them to your system's configuration, do the following:

1. Determine the number of standby processors or memory you want to activate.
2. Contact your sales representative or business partner to place an order for a number of CUoD Activation Features.
3. The sales representative places an order to the system or feature coordinator for the specific number of CUoD activation features. The order specifies the number of additional processors and memory you have requested to add.
4. The sales representative is provided with a reminder (through the system or feature configurator) that Vital Product Data (VPD) from the server must be sent to IBM to fulfill the order. To process the order, you must send VPD to IBM. You can send VPD in either of two ways:
   - Electronic Process (Electronic Service Agent)
     a. Ensure TCP/IP is set up and started.
     b. Run the Electronic Service Agent:
        1) In the Navigation area, click the **Service Applications** icon.
        2) In the Contents area, double-click the **Service Agent** icon.
        3) In the Service Applications window, click **Service Agent UI**.
        4) Type the Service Agent password. The default password, which is case sensitive, is:
           `password`
        5) In the Navigation Window, click **SAS-Connections**.
        6) Click **VPD**.
        7) You are presented with several options for transmitting VPD. You can select to send VPD immediately or to send it periodically.

           Note: For more information about using and setting up the Electronic Service Agent, see Chapter 20, "Service Agent," on page 123.
   - Web-based VPD entry:
     Collect the Vital Product Data from the server by following these steps:
     a. Access the internet from any available system and go to the following Web site: http://www.ibm.com/servers/eserver/pseries/cuod/index.html
     b. Record the processor order information. For more information, see "Viewing and Saving Permanent Capacity Upgrade on Demand Order Information" on page 90.
     c. Type the requested data you collected from previous steps.
     d. Retrieve the CUoD activation code from the Web or wait to receive the CUoD activation code by mail. The CUoD activation code will be posted on the Web, usually within one business day of receiving the order on the manufacturing floor if the VPD data has already been sent. To retrieve the CUoD activation code on the Web, do the following:
        1) Go to the following Web site: http://www.ibm.com/servers/eserver/pseries/cuod/index.html
        2) On the Web page, enter the machine type and serial number of the target server.
        3) Print or record the CUoD activation code displayed on the web page.
     e. Type the CUoD activation code. To use the HMC to perform this task, do the following:
        1) In the Contents area, select the managed system.

2) Select **Capacity Upgrade on Demand**.
3) Select **Activate**.
4) Type the activation code supplied to you by your sales representative.
5) Click **OK**. If you entered a valid activation code, the CUoD Activation Success window opens.
6) Click **OK**.

5. Assign the activated resources to a partition. If you are using dynamic logical partitioning, you do not have to reboot the system to use the resources. If you are not using dynamic logical partitioning, you must reboot the managed system before the newly activated resources can be used.

   Before adding resources to a partition running Linux, you must stop Linux partitions and then restart them after you have assigned the resources.

   For more information about assigning resources dynamically, see “Reassigning Partition Resources Dynamically” on page 98.
6. Begin using the new processor or memory capacity.

Managing On/Off Capacity on Demand Processors

On/Off activation allows you to start and stop using processors when you need to start and stop them.

To manage on/off capacity on demand processors, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select **Processor**.
4. Select **Manage On/Off CoD Processors**.
5. The **Manage On/Off CoD Processors** wizard opens. Specify the number of processors to activate or deactivate. The amount specified in the **New number of On/Off CoD processors requested** is the actual amount of new processors that you want to use. A zero in this field indicates that you want to turn off all the On/Off CoD processors. When you are finished, click **Next**.
6. Read the information displayed in the next wizard panel and then click **Finish**. If you have powered on the managed system using the LPAR Standby option, you can immediately begin to assign On/Off processors to partitions. If you have powered on the managed system using the Full System Partition power on option, the processors are not available until the next time you power on the managed system. If you are deactivating processors and have powered on the managed system using the LPAR Standby option, deallocate the processors you want to turn off from the associated partitions.

Accepting the License Agreement

During the first time you power on a CUoD-capable system using an HMC, a license agreement panel displays on the HMC that is attached to the CUoD system. Only users with the System Administrator role can accept the agreement. You must accept the CUoD license agreement in order to power on the system completely. If you choose not to accept the agreement, you must power off the managed system, have a service representative remove all the CUoD hardware, and then power on the machine again. If you do not accept the license agreement and did not have the CUoD hardware removed, the same license agreement window displays at the next power on.

You can view the license agreement at any time.

To view the license agreement, you must be a member of one of the following roles:

- System Administrator
- User Administrator

To view the license agreement, do the following:

1. Select the managed system.
2. Select **Capacity Upgrade on Demand—> License Agreement**.

Displaying Capacity Upgrade on Demand Resources

You can display the following information about your CUoD resources:

- Number of processors and amount of memory installed
- Number of processors and amount of memory permanently in use
- Number of processors and amount of memory not permanently activated
- Number of Trial CoD processors and amount of Trial CoD memory in use
- Number of processors for On/Off Use
- Trial CoD resource capacity condition
- Trial CoD resource capacity days and hours remaining

To display CUoD resource information, do the following:

1. In the Contents area, select the managed system.
2. Click **Capacity Upgrade on Demand**.
3. Select the resource type.
4. Click **Capacity Setting**.

Information about your CUoD resources displays.

Using the Trial CoD Feature

You can temporarily activate CUoD resources using your HMC. When you choose to activate immediately a CUoD resource, you are agreeing to do one of the following within 30 days of clicking **Finish** on the CUoD Trial CoD Capacity window:

- Purchase permanent activations for the same capacity that was immediately activated and enter the generated permanent activation code (mailed to you and available on the Web)
- Stop all work on the immediately activated capacity and return the resource to a state where it can be reclaimed by the system

To activate a CoD resource, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select the resource type.
4. Select **Trial CoD**.
5. The **Trial CoD Capacity** wizard opens. Specify the resource amount you want to activate and click **Next**.
6. Read the information contained on the window.

   Note: The value you specified as **New** in the **Trial CoD processors in use** field cannot be changed after you click **Finish**. If this number is incorrect, click the **Back** button and enter the correct value as appropriate.

   When you have finished reading the information on the window and are ready to confirm your new temporary capacity settings, click **Finish**.
7. Next, you must assign the activated resources to a partition. If you are using dynamic logical partitioning, you do not have to reboot the system to use the resources. If you are not using dynamic logical partitioning, you must reboot the managed system before the newly activated resources can be used.

Before adding resources to a partition running Linux, you must stop Linux partitions and then restart them after you have assigned the resources.

For more information about assigning resources dynamically, see“Reassigning Partition Resources Dynamically” on page 98.

Disabling Trial CoD Resource Capacity

You can disable the resources you immediately activated. To disable temporary resources, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select the resource type.
4. Select **Disable Trial CoD**.
5. A confirmation window opens. Click **Yes** to disable the Trial CoD option for the selected resource.

Viewing and Saving Permanent Capacity Upgrade on Demand Order Information

You can save CUoD ordering information to either an ftp site or a diskette on the HMC.

To save CUoD order information, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select the resource type.
4. Select **Capacity Setting**.
5. Click **Display Order Information**. The following information about your order displays:
   - System type
   - System serial number
   - CUoD capacity card CCIN
   - CUoD capacity card serial number
   - CUoD capacity card unique identifier
   - CUoD resource identifier
   - CUoD resource activated
   - CUoD resource sequence number
   - CUoD resource entry check
6. If you want to save this information, click **Save As**.
7. Select where you want to save the order information, and complete the fields with the appropriate information.

Viewing and Saving On/Off Capacity on Demand Order Information

You can save On/Off Capacity on Demand ordering information to either an ftp site or a diskette on the HMC.

To save CUoD order information, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select **Processors**.
4. Select **Capacity Setting**.
5. Click **Display On/Off Order Information**. The following information about your order displays:

- System type
- System serial number
- Capacity card CCIN
- Capacity card serial number
- Capacity card unique identifier
- Resource identifier
- Activated On/Off CoD processor units
- On/Off CoD sequence number
- On/Off CoD entry check

6. If you want to save this information, click **Save As**.
7. Select where you want to save the order information, and complete the fields with the appropriate information.

Permanently Activating Capacity Upgrade on Demand Resources

You can enter an activation code to permanently activate Capacity Upgrade on Demand resources.

To activate CUoD resources, do the following:

1. In the Contents area, select the managed system.
2. Select **Capacity Upgrade on Demand**.
3. Select **Activate**.
4. Type the activation code supplied to you by your sales representative.
5. Click **OK**. If you entered a valid activation code, The **CUoD Activation Success** window opens.
6. Click **OK**. If you are using dynamic logical partitioning, you do not have to reboot the system to use the resources. If you are not using logical partitioning, you must reboot the managed system before the newly activated resources can be utilized.

   Note: Before adding resources to a partition running Linux, you must stop Linux partitions and then restart them after you have assigned the resources.

Chapter 17. Server Management Tasks

This chapter provides information about the server management tasks you can perform.

To activate more than one partition, you must power on your managed system using the Partition Standby power-on option. For more information about power-on options, see “Powering On the Managed System” on page 75.

Creating Partitions

This section describes how to create logical partitions.

To create partitions, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

Preparing Your System for Partitioning

To prepare your system for partitioning, do the following:

1. Log in to the HMC.
2. In the Navigation area, click the console’s icon to expand the tree.
3. In the Navigation area, double-click the **Server and Partition** folder icon underneath the managed system.
4. In the Navigation area, click the **Server Management** icon to select your preferred partition environment. The Contents area now lists the available managed systems.
5. In the Contents area, select the managed system for which you want to configure partitions.
6. With the managed system selected in the Contents area, choose **Selected** from the menu.

   If your managed system is currently powered on using the Partition option, see “Creating Logical Partitions.”

   If your managed system is currently powered off, continue with the next step.
7. Select **Power On—> Partition Standby**.
8. Click **OK** to power on the managed system. In the Contents area, the managed system’s state changes from *No Power* to *Initializing . . .* and then to *Ready*. When the state reads *Ready* and the virtual Operator Panel Value reads *LPAR . . .* , see “Creating Logical Partitions.” For more information about managed system states, see “Managed System Operating States” on page 253.

Creating Logical Partitions

1. In the Contents area, select the managed system.
2. From the selected menu, select **Create—> Logical Partition**. The Create Logical Partition and Profile wizard opens.
3. In the first window of the Create Logical Partition and Profile wizard, provide a name for the partition profile that you are creating. Use a unique name for each partition that you create. Names can be up to 31 characters long.
4. Click **Next**.
5. Type the name of the profile you are creating for this partition.
6. Click **Next**.
7. Select the desired, minimum, and maximum number of processors you want for this partition profile. The HMC shows you the total number of processors configured for use by the system, and prompts you to enter your *desired*, *minimum*, and *maximum* processor amounts for this partition profile, as follows:

Desired
Desired amounts are used if they are available at the time of activation.

Minimum
Minimum amounts define the smallest number of processors you require for this partition. If these processors are not available at the time you attempt to activate the profile, the partition does not activate.

Maximum
Maximum amounts define the largest number of processors you can assign to this partition. If you attempt to dynamically move an amount of processors to this partition that exceeds this number, an error message displays, and the operation stops.

8. Click **Next**.
9. Select the desired and minimum amount of memory. The HMC shows you the total amount of memory configured for use by the system, and not the amount that is currently available. The HMC prompts you to enter your *desired*, *minimum* and *maximum* memory amounts for this partition profile, as follows:

   Desired
   Desired amounts are used if they are available at the time of activation.

   Minimum
   Minimum amounts define the smallest amount of memory you require for this partition. If this memory amount is not available at the time you attempt to activate the profile, the partition does not activate.

   Maximum
   Maximum amounts define the largest amount of memory you can assign to this partition. If you attempt to dynamically move an amount of memory to this partition that exceeds this number, an error message displays and the operation stops.

   Enter the amount of desired and required memory in 1 gigabyte (GB) increments and 256 megabyte (MB) increments. You must have a minimum of 1 GB for each partition.

   If you plan on installing AIX 5.2 or Linux on this partition, you should select the **Small Real Mode Address Region** option. Other special memory issues must be considered when you assign memory to partitions. For more information about these memory issues, see “Assigning Memory” on page 23.
10. Click **Next**.
11. The left side of the new window displays the I/O drawers available and configured for use. To expand the I/O tree to show the individual slots in each drawer, click the icon next to each drawer. Because the HMC groups some slots, if you attempt to assign a member of one of these grouped slots to a profile, the entire group is automatically assigned. Groups are indicated by a special icon named **Group**_*XXX*.

    Click on the slot for details about the adapter installed in that slot. When you select a slot, the field underneath the I/O drawer tree lists the slot’s class code and physical location code.

    Note: The slots in the I/O Drawers field are not listed in sequential order.
12. Select the slot you want to assign to this partition profile and click **Add**. If you want to add another slot, repeat this process. Slots are added individually to the profile; you can add slots one at a time, unless they are grouped. Minimally, add a boot device to the **required** list box.

    You can add adapters to the *Required* and *Desired* groups. Desired adapters will be used if they are available at the time of activation. Required adapters are adapters that you require for this partition. If the adapters in this group are not available at the time of activation, the partition does not activate.

    If you want to install an operating system on this partition using the managed system’s CD-ROM drive, assign the CD-ROM drive to this partition profile.

13. Click **Next**. This window allows you to set service authority and boot mode policies for this partition profile.

    If you want this partition to be used by service representatives to perform system firmware updates and set other system policy parameters, select the **Set Service Authority** check box.

    If you want the HMC to monitor the partition and ensure it is active, select the **Enable SFP Surveillance** check box.

    Select the boot mode that you want for this partition profile. For a description of each boot mode, see “Power-On Options” on page 76.
14. Click **Next**. This window supplies you with summary information about this partition.
15. Review the information to ensure that you have the appropriate resources assigned to this partition.
16. If you want to change the configuration, click **Back**. Otherwise, click **Finish** to create the partition and profile.
17.

The new partition, along with the default profile you just created, displays underneath the Managed System tree in the Contents area.

After you have created a partition, you must install an operating system and configure Inventory Scout Services on the HMC and on the partition. To install an operating system on the partition and configure Inventory Scout Services on that partition, see the installation information provided with your operating system. To configure Inventory Scout Services for this partition on the HMC, see “Configuring the Inventory Scout Services Profile” on page 59.

Note: If you want to use the managed system’s CD-ROM to install operating systems on your partitions, create at least two profiles for each partition. Create one profile that has the managed system’s CD-ROM assigned to it, and another profile without the managed system’s CD-ROM. Using this method, you can release the managed system’s CD-ROM by deactivating the profile that has the CD-ROM and activating the profile that does not have the CD-ROM. For more information about creating partition profiles, see “Creating Additional Partition Profiles” on page 109.

Creating Affinity Partitions

Depending on your managed system’s configuration, you may be able to create a special group of logical partitions called *affinity partitions*. The process of creating a group of affinity partitions is similar to the process of creating logical partitions. The only difference is that when you create affinity partitions, the system does the processor and memory assignment for you.

To determine if your managed system is capable of running affinity partitions, check your managed system’s properties. For more information about viewing your managed system’s properties, see “Viewing Managed System Properties” on page 78.

To create an affinity partition, do the following:

1. In the Contents area, select the managed system.
2. From the selected menu, select **Affinity Logical Partition—> Create**. The Affinity Partition Setup wizard opens.
3. In the first window of the Create Affinity Partition wizard, select the type of affinity partition you want to create.
4. Click **OK**.
5. In the second window of the Create Affinity Partition wizard, type a name for the first affinity partition that you are creating. Use a unique name that is up to 31 characters long.

   In the second field, type a name for the default profile.

   Then select which boot mode this affinity partition will use when you activate it.

If you want this partition to be used by service representatives to perform system-firmware updates and set other system policy parameters, select the **Set Service Authority** check box.

Enter this information for each of the affinity partitions you want to create. To select another affinity partition, click on the appropriate ALPAR tab on the top of the window.

6. Click **Next**.
7. The left side of the new window now displays the I/O drawers that are available and configured for use. To expand the I/O tree to show the individual slots in each drawer, click the icon next to each drawer. Because the HMC groups some slots, if you attempt to assign a member of one of these grouped slots to a profile, the entire group is automatically assigned. Groups are indicated by a special icon named **Group**_*XXX*.

   Click on the slot for details about the adapter installed in that slot. When you select a slot, the field underneath the I/O drawer tree lists the slot's class code and physical location code.

   Note: The slots in the **I/O Drawers** field are not listed in sequential order.
8. Select the slot you want to assign to this default affinity profile and click **Add**. If you want to add another slot, repeat this process. Slots are added individually to the profile; you can only add slots one at a time, unless they are grouped. Minimally, add a boot device to the **required** list box.

   If you want to install an operating system on this partition using the managed system's CD-ROM drive, assign the CD-ROM drive to this partition profile.
9. Perform steps 6-9 for each affinity partition tab shown at the top of the screen.
10. If you want to change the configuration for any affinity partition, click **Back**. Otherwise, click **Finish** to create the group of affinity partitions.
11. The new affinity partitions, along with the default profiles you just created, display underneath the Managed System tree in the Contents area. A System Profile is also created and is displayed underneath the managed system tree.
12. After you have created a partition, you must install an operating system on the partition. To install an operating system on the partition, see the installation information provided with your operating system.

    Note: If you want to use the managed system's CD-ROM to install operating systems on your partitions, create at least two profiles for each partition. Create one profile that has the managed system's CD-ROM assigned to it, and another profile without the managed system's CD-ROM. Using this method, you can release the managed system's CD-ROM by deactivating the profile that has the CD-ROM and activating the profile that does not have the CD-ROM. For more information about creating partition profiles, see "Creating Additional Partition Profiles" on page 109.

Updating Affinity Partitions After Adding or Removing Managed System Resources

To update affinity partitions after a service representative has added or removed resources on the managed system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To update affinity partitions after adding or removing managed system resources, do the following:

1. In the Contents area, select the managed system.
2. From the selected menu, select **Affinity Logical Partition—> Update**.
3. The HMC assesses what resources have been added or removed and asks you if you would like to add or remove affinity partitions as appropriate. For more information about adding new affinity partitions, see "Creating Affinity Partitions" on page 95. If you have removed resources from your managed system, the HMC lists the affinity partitions associated with the removed resources. Click **OK** to remove these affinity partitions.

Activating Partitions

To activate a partition, select the partition itself, and click **Activate** from the Selected menu. A window opens that lists activation profiles. The default partition profile is automatically highlighted, but you can activate the partition with any of the listed profiles.

If the required resources you specified in the partition profile that you are using to activate the partition exceed the amount of available resources, this partition does not activate. All resources currently not being used by active partitions are considered available resources. It is important that you keep track of your system's resources at all times.

For service, you must also configure Inventory Scout Services for each partition that you activate. For more information about configuring Inventory Scout Services, see "Configuring the Inventory Scout Services Profile" on page 59.

To activate partitions, you must be a member of one of the following roles:

- Operator
- Advanced Operator
- System Administrator
- Service Representative

Activating a Specific Partition Profile

To activate a partition profile, do the following:

1. In the Contents area, select a partition profile.
2. From the menu, click **Selected—> Activate**.
3. The profile name is highlighted. Click **OK** to activate the partition profile.

The virtual operator panel next to the partition cycles through hardware boot sequence error and information codes, and then displays the operating system error and information codes. For a complete description of these codes, see the hardware service documentation for your managed system and the documentation provided with your operating system.

Activating a Partition without Selecting a Specific Partition Profile

To activate a partition without selecting a specific partition profile, do the following:

1. In the Contents area, select the partition.
2. From the menu, click **Selected—> Activate**.
3. The default profile name is highlighted. Click **OK**. If you want to activate a different profile, select another profile and then click **OK**.

Reactivating a Partition with a Partition Profile

Reactivating a partition with a different profile requires shutting down the operating system that is running in that partition and activating another profile.

To reactivate a partition with a partition profile, you must be a member of one of the following roles:

- Operator
- Advanced Operator
- System Administrator
- Service Representative

To reactivate a partition with a different profile, do the following:

1. In the Contents area, select the partition for which you want to change profiles.
2. Open a virtual terminal window for that partition to look at the operating system. To learn more about opening a terminal window, read "Opening a Virtual Terminal Window" on page 116.

3. Run an appropriate **shutdown** command. The system shuts down the operating system, and the partition's state changes from *Running* to *Ready* in the Contents area.
4. In the Contents area, select the new partition profile that you want to activate for that partition.
5. From the menu, click **Selected—> Activate**.

Reassigning Partition Resources Dynamically

You can logically attach and detach a managed system's resources to and from a logical partition's operating system without rebooting. To reassign partition resources dynamically, you must have AIX Version 5.2 installed on your partitions. You must also allocate at least 512 MB of memory to each partition you want to activate.

Users with the System Administrator role can reassign resources dynamically.

Note: You can dynamically reassign I/O resources between affinity logical partitions, but not processor or memory resources.

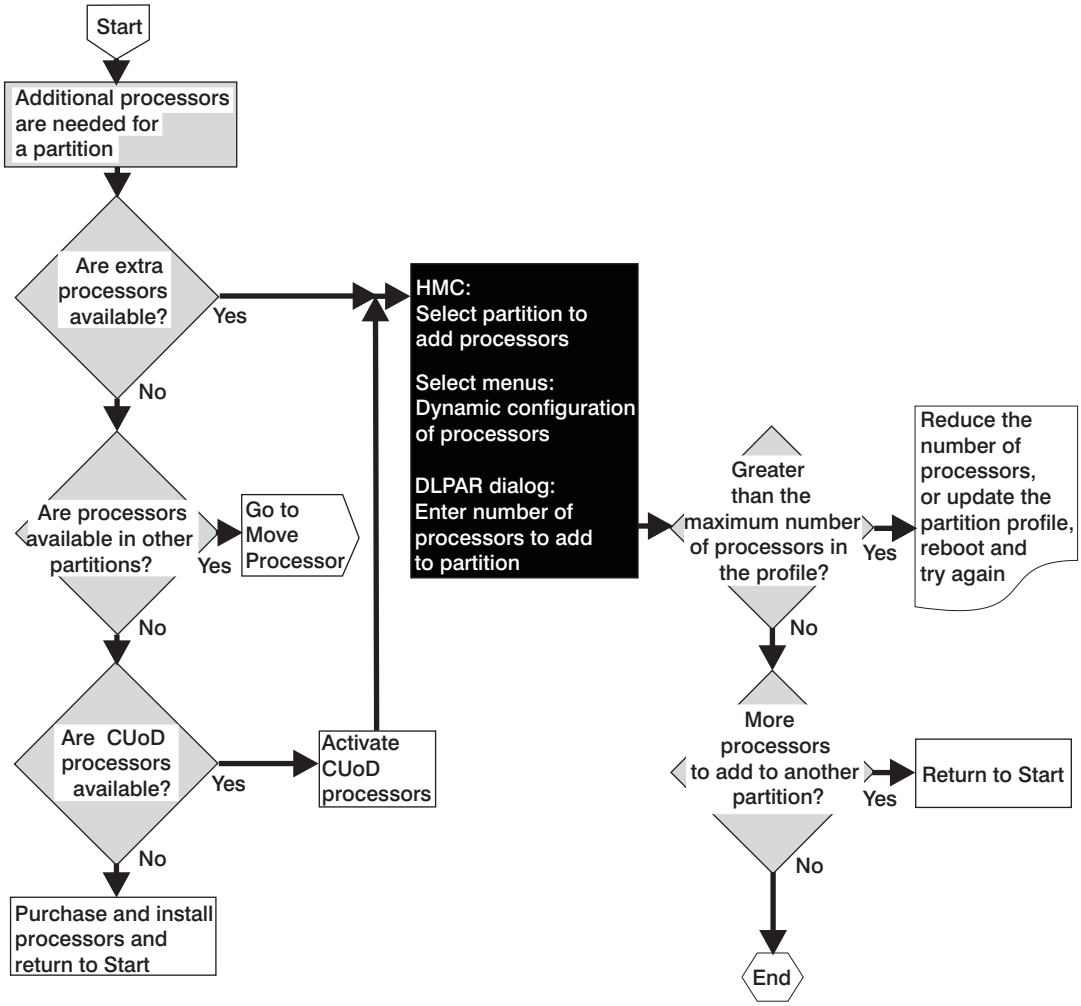
Adding Resources

You can dynamically add processors, memory, and adapters to partitions.

Adding Processors to A Partition Dynamically: This task allows you to add processors to a partition without rebooting the partition's operating system.

You can add only up to the amount of free system processors, or processors that are not assigned to a running partition. This number cannot exceed the maximum number specified in this partition's active profile. To learn more about this partition's active profile, view the activated profile's properties. To view profile properties, see "Viewing Partition Profile Properties" on page 110.

The following illustrates how processors are added to a partition:



To add available processor resources without rebooting the partition, do the following:

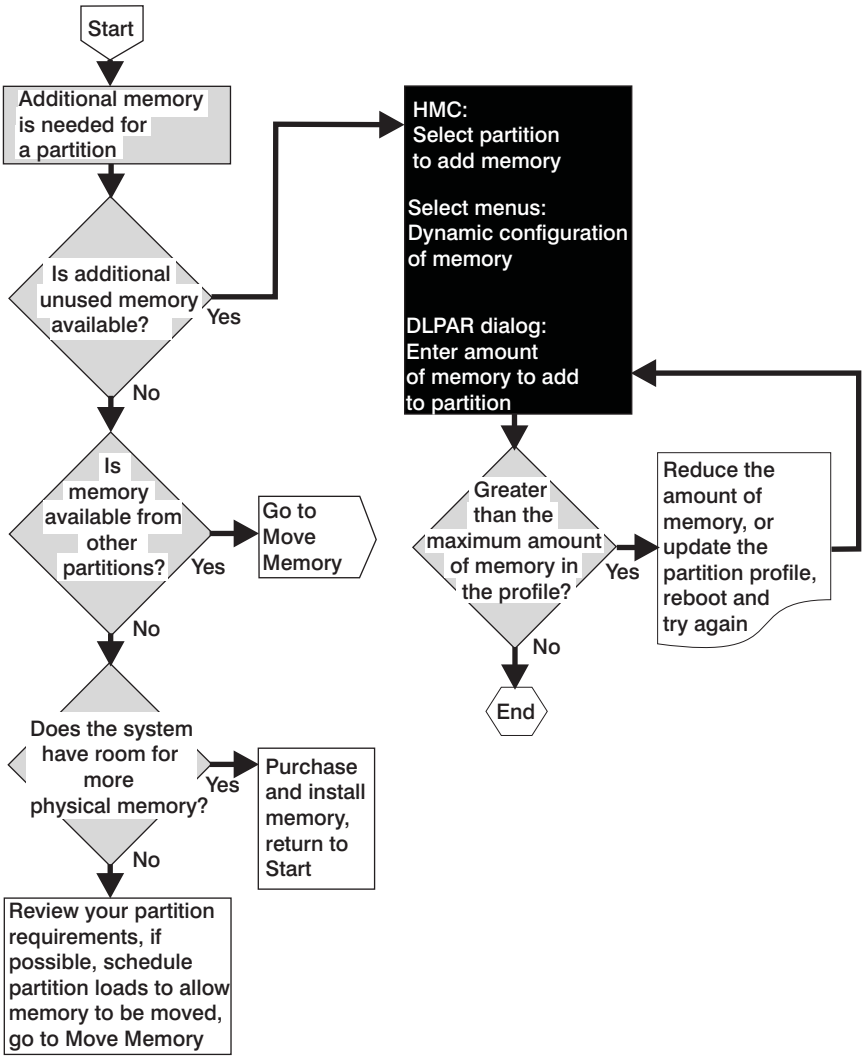
1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition to which you want to add the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Processors**. The **Dynamic Logical Partitioning** window opens.
9. Click **Add resources to this partition**.
10. Select the number of processors you want to add to this partition.

    Note: If there is a **Processor Information** button underneath the **Number of CPUs to add** field, the HMC has discovered disabled processors that you might be able to deconfigure and release for system use. For more information about restoring these processors, see "Restoring Processor Resources" on page 255.
11. In the **Task timeout** field, select the number of minutes that you want the system to wait before it stops the task.

12. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
13. When you have finished selecting the information, click **OK**.

Adding Memory to A Partition Dynamically: This task allows you to add memory to a partition without rebooting the partition's operating system.

The following illustrates how memory is added to a partition dynamically:



To add available memory resources without rebooting the partition, do the following:

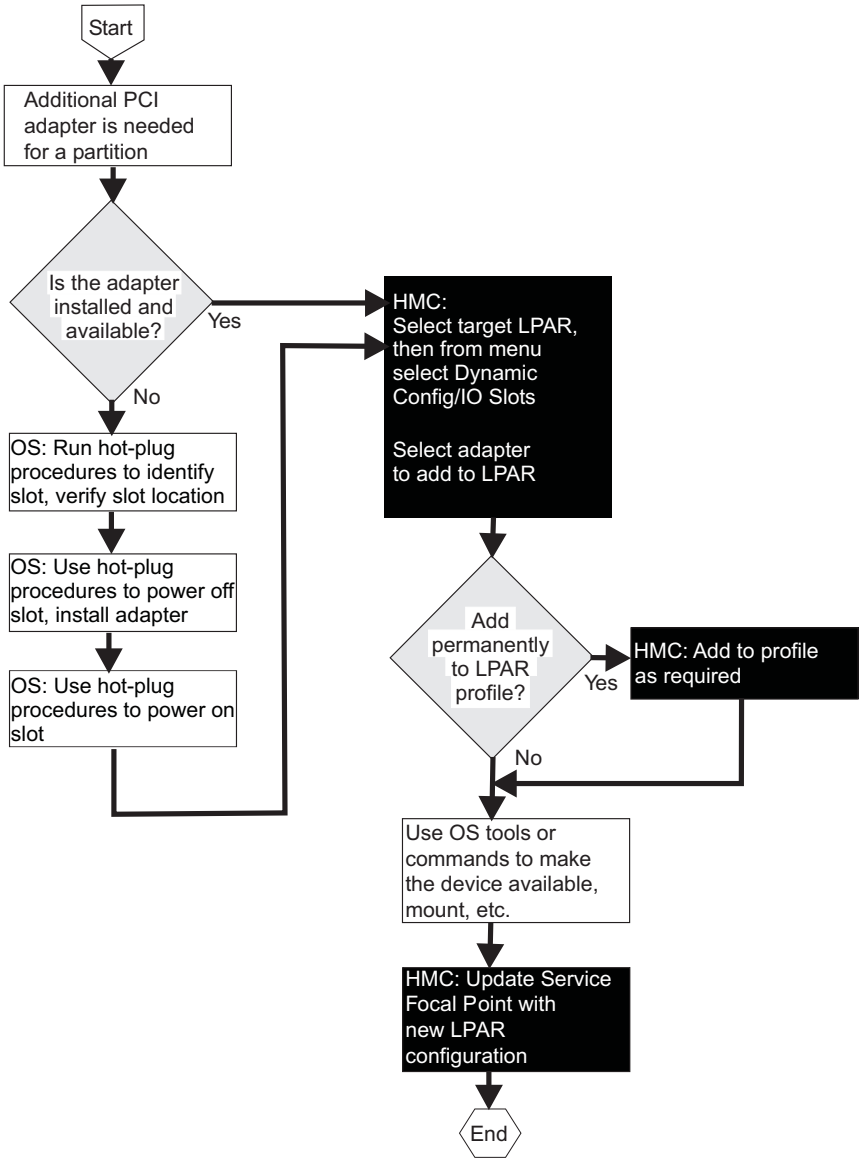
1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition to which you want to add the memory.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Memory**. The **Dynamic Logical Partitioning** window opens.
9. Click **Add resource to this partition**.

10. Select the amount of memory you want to add to this partition. The window the amount of available memory the system has for this partition's use.

    Note: If there is a **Memory Information** button underneath the **Amount of memory to add** field, the HMC has discovered an inconsistency between any partition's allocated and requested memory amounts. Click this button to correct the requested memory value and free memory resources to the system. For more information about restoring memory, see "Restoring Memory Resources" on page 256.
11. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
12. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
13. When you have finished selecting the information, click **OK**.

Adding Adapters to A Partition Dynamically: This task allows you to add I/O adapters to a partition without rebooting the partition's operating system.

The following illustrates how adapters are added to a partition dynamically:



Note: An SNI (serial) adapter cannot be dynamically reconfigured.

To add available adapter resources without rebooting the partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition to which you want to add the adapters.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Adapters**. The **Dynamic Logical Partitioning** window opens.
9. Click **Add resource to this partition**.
10. Select the available system adapters that you want to add to this partition.

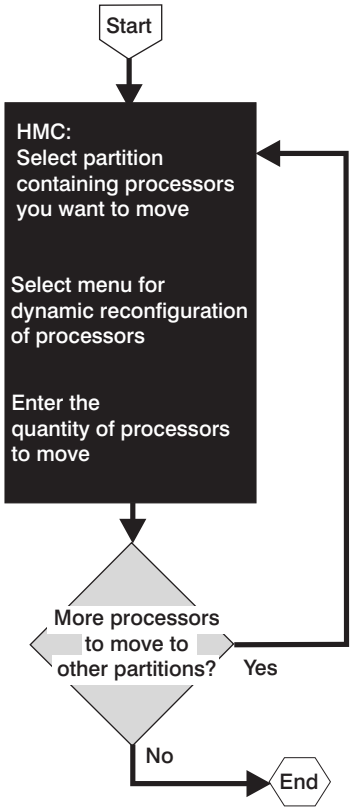
    Note: If there is an **Adapter Information** button underneath the **Free system adapters** field, the HMC has discovered disabled adapters that you might be able to release and restore for system use. For more information about restoring these adapters, see "Restoring Adapter Resources" on page 256.
11. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
12. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
13. When you have finished selecting the information, click **OK**.

Moving Resources

You can dynamically move processors, memory, and adapters among partitions.

Moving Processors from One Partition to Another: This illustrates how processors are moved from one partition to another without rebooting either partition's operating system.

The following is a task description of moving processors from one partition to another:



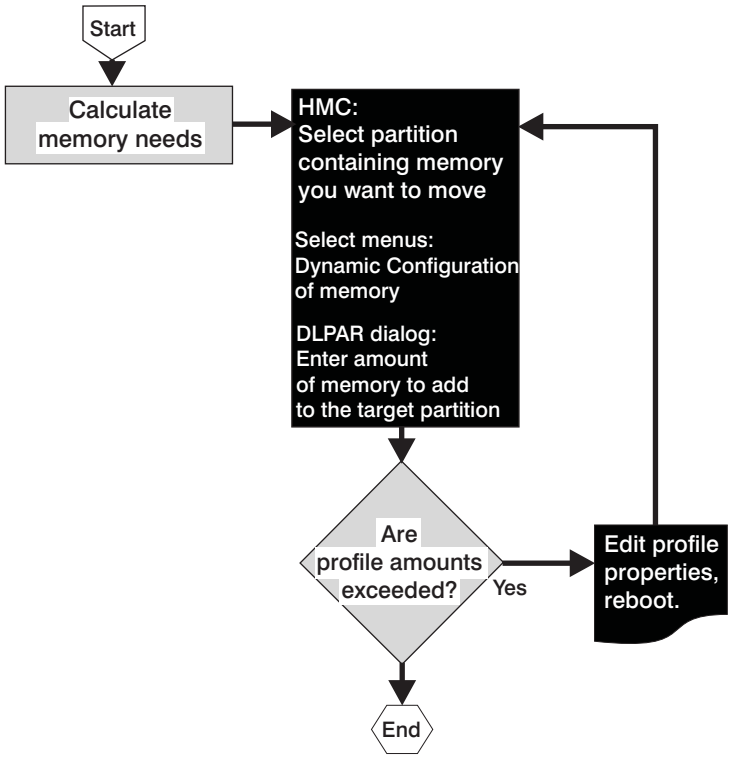
To move processors from one active partition to another without rebooting either partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition from which you want to move the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Processors**. The **Dynamic Logical Partitioning** window opens.
9. Click **Move resources to a partition**.
10. Select the number of processors you want to move from this partition.

    Note: The number you are removing cannot make the remaining number of processors be less than the minimum number specified in this partition's active profile. Likewise, the number you are adding to the other partition cannot exceed the destination partition's maximums. To learn more about the resources being used by each activated partition, click the **Details** tab of each partition's Properties folder.
11. Select name of the partition to which you want to move the processors.
12. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
13. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
14. When you have finished selecting the information, click **OK**. Processors are moved from this partition to the partition you selected.

Moving Memory from One Partition to Another: This task allows you to move memory from one partition to another without rebooting the partition's operating system.

The following illustrates how memory is moved from one partition to another partition:



To move memory from one active partition to another without rebooting either partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition from which you want to move the memory.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Memory**. The **Dynamic Logical Partitioning** window opens.
9. Click **Move resource to a partition**.
10. Select the amount of memory you want to move from this partition.

    Note: The number you are removing cannot make the remaining memory amount be less than the minimum number specified in this partition's active profile. To learn more about the resources being used by the activated partition, click the **Details** tab of this partition's Properties folder.
11. Select the name of the partition to which you want to move the memory.

    Note: If there is a **Memory Information** button in this window, the HMC has discovered an inconsistency between any partition's Allocated and Requested memory amounts. Click this button to correct the requested memory value and free memory resources to the system. For more information about restoring memory, see "Restoring Memory Resources" on page 256.
12. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.

13. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
14. When you have finished selecting the information, click **OK**.

Moving Adapters from One Partition to Another: This task allows you to move I/O adapters from one partition to another without rebooting the partition's operating system. Before moving an adapter, you must log in to the operating system on the source partition and unconfigure the adapter.

An SNI adapter cannot be dynamically reconfigured.

Note: To ensure that Service Focal Point and dynamic operations continue to function correctly, do not dynamically move an adapter physically connected to the HMC.

To move adapter resources from one active partition to another without rebooting either partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. Make sure that this partition's operating system is not currently using the adapter. For more information about determining if the operating system is using the adapters, refer to the documentation provided with the partition's operating system.
3. In the Navigation area, click the console's icon to expand the tree.
4. In the Navigation area, click the **Server and Partition** folder.
5. In the Contents area, click the **Server Management** icon.
6. In the Contents area, click the managed system's icon to expand the tree.
7. Select the partition from which you want to move the adapters.
8. From the Selected menu, select **Dynamic Logical Partitioning**.
9. Select **Adapters**. The **Dynamic Logical Partitioning** window opens.
10. Click **Move resource to a partition**.
11. Select the I/O adapters you want to move from the list. Adapters designated as **required** in this partition's active profile are not included in this list and cannot be removed. To learn more about the partition's active profile, look at the activated profile's properties.
12. Select the partition to which you would like move the adapters.
13. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
14. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
15. When you are finished selecting the information, click **OK**. Adapters are then moved from this partition to the partition you selected. Now you must log on to the other partition's operating system and configure the adapter.

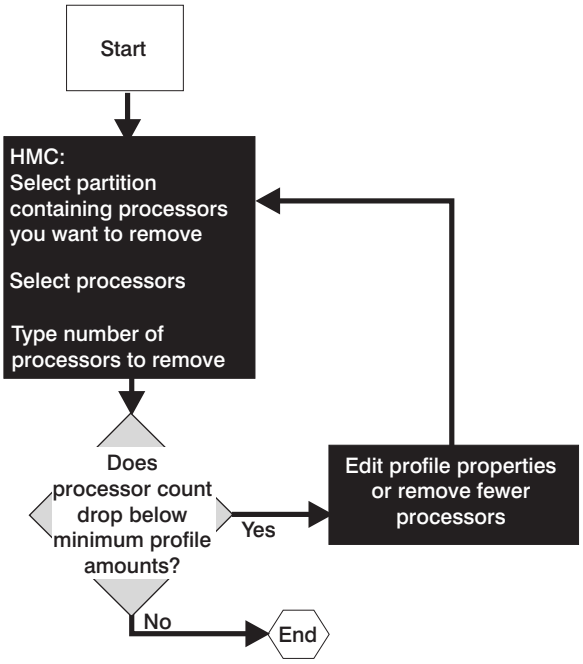
Removing Resources

You can dynamically remove processors, memory, and adapters from partitions.

Removing Processors from A Partition Dynamically: This task allows you to remove processors from a partition without rebooting the partition's operating system.

When you remove a processor, it is released by the partition and available for use by other partitions. The number of processors remaining after the Remove operation cannot be less than the minimum number specified in this partition's active profile. To learn more about this partition's active profile, view the activated profile's properties. To view profile properties, see "Viewing Partition Profile Properties" on page 110.

The following illustrates how processors are removed from a partition:

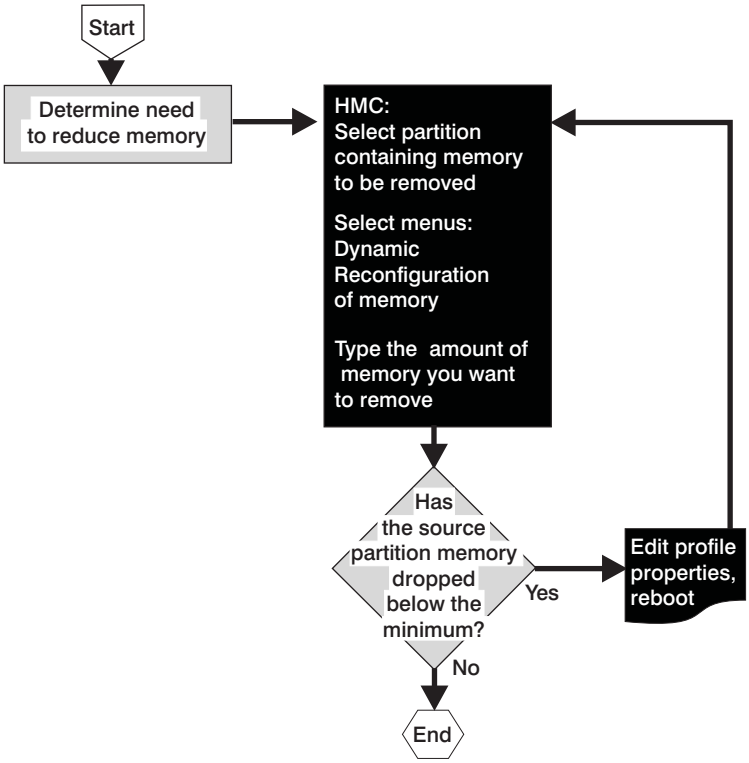


To remove processor resources from an active partition without rebooting the partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition from which you want to remove the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Processors**. The **Dynamic Logical Partitioning** window opens.
9. Click **Remove resource from this partition**.
10. Select the number of processors you want to remove from this partition.
11. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
12. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
13. When you have finished selecting the information, click **OK**.

Removing Memory from A Partition Dynamically: When you remove memory, it is released by the partition and available for use by other partitions. The memory amount remaining after the Remove operation cannot be less than the minimum number specified in this partition's active profile. To learn more about this partition's active profile, view the activated profile's properties. To view profile properties, see "Viewing Partition Profile Properties" on page 110.

The following illustrates how memory is removed from a partition:



To remove memory resources from an active partition without rebooting the partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition from which you want to remove the memory.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Memory**. The **Dynamic Logical Partitioning** window opens.
9. Click **Remove resource from this partition**.
10. Select the amount of memory you want to remove from this partition.

    Note: If there is a **Memory Information** button in this window, the HMC has discovered an inconsistency between any partition's Allocated and Requested memory amounts. Click this button to correct the requested memory value and release and restore memory resources to the system. For more information about restoring memory, see "Restoring Memory Resources" on page 256.
11. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
12. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
13. When you have finished selecting the information, click **OK**.

Removing Adapters from A Partition Dynamically: This task allows you to remove I/O adapters from a partition without rebooting the partition's operating system. Before continuing with this task, you must use the partition's operating system to manually deconfigure each adapter that you want to remove.

Note: Adapters designated as **required** in this partition's active profile are not included in this list and cannot be removed. To learn more about this partition's active profile, view the activated profile's properties.

An SNI adapter cannot be dynamically reconfigured.

To remove adapter resources from an active partition without rebooting the partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. Make sure that this partition's operating system is not currently using the adapter. For more information about determining if the operating system is using this adapter, refer to the documentation provided with the partition's operating system.
3. In the Navigation area, click the console's icon to expand the tree.
4. In the Navigation area, click the **Server and Partition** folder.
5. In the Contents area, click the **Server Management** icon.
6. In the Contents area, click the managed system's icon to expand the tree.
7. Select the partition from which you want to remove the adapters.
8. From the Selected menu, select **Dynamic Logical Partitioning**.
9. Select **Adapters**.
10. Select the adapters used by this partition that you want to remove. The **Dynamic Logical Partitioning** window opens.
11. Click **Remove resource from a partition**.
12. In the **Task timeout** field, select the number of minutes you want the system to wait before it stops the task.
13. In the **Details** field, select the level of feedback that you want to see while the HMC performs the task. Details shown include the operating system's standard output and standard error information.
14. When you have finished selecting the information, click **OK**.

Deleting Partitions

To delete a partition, the managed system must be powered on using the Partition Standby power-on option. If you delete a partition, all of the profiles associated with that partition are also deleted. The partition is also automatically deleted from all system profiles.

You can delete partitions if you are a member of the System Administrator role.

Note: You cannot delete an activated partition.

To delete a partition, do the following:

1. Select the partition from the Contents area.
2. From the menu, click **Selected—> Delete**.

For information about deleting a partition *profile*, see "Deleting Partition Profiles" on page 112.

Deleting Affinity Partitions

You can delete affinity partitions only as a group; you cannot delete them individually.

To delete a group of affinity partitions, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To delete a group of affinity partitions, do the following:

1. In the Contents area, select the affinity partition group you want to remove.

2. From the selected menu, select **Affinity Logical Partition—> Delete**.
3. After confirming that the affinity partitions listed are the ones you want to remove, click **OK**. The affinity partitions are removed from the Contents area.

Restarting the Operating System

When a partition is running an operating system and the system hangs, use the HMC to restart the operating system.

Attention: This operation can damage data. Perform this procedure *only* after you have attempted to restart the operating system manually.

You can perform either a ″hard″ and ″soft″ reset.

- Soft reset actions are determined by your operating system's policy settings. Depending on how you have configured these settings, the operating system may:
  - Perform a dump of system information
  - Restart automatically

  For more information about configuring your operating system's policy settings, see you operating system documentation.
- A hard reset acts as a virtual powering off of the system. Issuing a hard reset forces termination and can damage information. Use this option only if the operating system is disrupted and cannot send or receive commands.

To restart the operating system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To restart the operating system you have installed on a partition, do the following:

1. In the Contents area, select the partition you want to reset.
2. From the menu, click **Selected—> Operating System Reset**.
3. Select the appropriate check box and click **Yes**.

Managing Partition Profiles

A partition profile defines the set of resources that you need to create a partition. You can create more than one partition profile for a partition, but you can *activate* only one partition profile for a partition at a time.

When you create a partition profile, the HMC shows you all the resources available on your system. The HMC does not, however, check to see if another partition is currently using a portion of these resources. For example, the HMC might show 16 processors on your system, but will not indicate that other partitions are using nine of them. You can conceivably create two partition profiles, each using a majority of system resources. However, you can do this only if you do not intend to use them at the same time. If you attempt to activate both of these partition profiles, the second activation attempt will fail.

Creating Additional Partition Profiles

To create partition profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To create a partition profile, do the following:

1. In the Contents area, select the *partition* for which you want to create a profile. If you select the managed system, you create a new partition, not a profile.
2. From the menu, click **Selected—> Create—> Profile**. A profile creation wizard opens and guides you through the creation of a new profile.

You can now begin to assign resources to the new partition profile. This partition profile does not take effect until you use it to activate the partition.

Viewing Partition Profile Properties

You can view partition profile information from your HMC. Depending on your access levels, you can also restore, back up, and remove this data from the local file system.

Any user can view partition profile properties.

To view a partition profile's properties, do the following:

1. In the Contents area, select the profile.
2. From the menu, click **Selected—> Properties**.

Setting Service Authority

Service representatives use the partition designated with service authority to perform system firmware updates. If you set service authority for one partition, a service representative can use this partition to perform system updates without having to power off the managed system.

Only one partition can be activated with service authority. If you change the active profile of a running partition by selecting Service Authority, you must reactivate the modified profile.

To set service authority, you must be a member of one of the following roles:

- Advanced Operator
- System Administrator

To set service authority, do the following:

1. In the Contents area, select the profile.
2. From the menu, click **Selected**.
3. Select **Properties** to open the Properties window.
4. Click the **Other** tab.
5. Select the **Set Service Authority** check box.
6. Click **OK**.

You can activate one partition with service authority at a time. You must set service authority on a partition profile that is not currently active. To switch Service Authority from one running partition to another running partition, do the following:

1. Deactivate both partitions.
2. Deselect the **Service Authority** check box in one partition's activation profile.
3. Select the **Service Authority** check box in the other partition's activation profile.
4. Activate both partitions.

Copying Partition Profiles

The HMC allows you to copy the contents of a profile that you have already created. For example, you might decide that you need a partition profile that is similar to one that you have already created, but with a small change in resource allocation.

To copy partition profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To copy a partition profile, do the following:

1. In the Contents area, select the existing partition profile that you want to copy.
2. From the menu, click **Selected—> Copy**.
3. Type a unique name for the new copy.
4. Click **OK**.

Changing Default Partition Profiles

When you create a partition, the HMC requires that you create at least one profile called the *default profile*. In the Contents area, the default profile is represented by an icon that looks similar to the following illustration:

When activating a partition, the HMC highlights the default profile as the one to use during activation unless you specify that it activate a different partition profile.

To change default profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To change the default partition profile, do the following:

1. In the Contents area, select the default partition profile that you want to change.
2. From the menu, click **Selected—> Change Default Profile**.
3. Select the profile that you want to be the default profile.

Understanding Partition Boot Errors

If a partition is in an error state after you attempted to activate it, you can review the boot error value, which indicates why the boot failed.

For more information about boot error values, see “Boot Error Values” on page 260.

To review a partition boot error, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Service Representative

To review a partition boot error, do the following:

1. In the Contents area, right-click the partition that is in the *Error* state.
2. Click **Read Boot Error Value**. A window opens that gives you more information about why the boot failed.

Deleting Partition Profiles

To delete partition profiles, you must be a member of the System Administrator role.

To delete a partition profile, do the following:

1. In the Contents area, select the profile.

   Note: Be sure to select the profile and not the partition itself, to avoid deleting an entire partition.
2. From the menu, click **Selected—> Delete**.

Managing System Profiles

System profiles are a collection of one or more partition profiles. When you activate a system profile, you also activate each associated partition profile. You can use a system profile at any time, including when you power on the managed system.

For more information about partition profiles, see “Managing Partition Profiles” on page 109.

Creating System Profiles

To create system profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To create a system profile, do the following:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected —> Create—> System Profile**.
3. Name the system profile and select the available partition profiles that you want to add to the new system profile.
4. Click **Add** for each selected partition profile. Select one profile for each partition to place into a system profile.
5. Click **OK**.

Viewing System Profile Properties

Any user can view system profile properties.

To view the properties of the system profile, do the following:

1. In the Contents area, select the system profile.
2. From the menu, click **Selected—> Properties**.

Modifying System Profile Properties

To modify system profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To modify system profiles, do the following:

1. In the Contents area, select the system profile you want to modify.
2. From the menu, click **Selected—> Properties**.
3. Change the system profile information as appropriate.

Copying System Profiles

Because some system profiles are complex, the HMC allows you to copy the contents of a profile that you have already created.

To copy system profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To copy a system profile, do the following:

1. In the Contents area, select the existing profile that you want to copy.
2. From the HMC menu, click **Selected—> Copy**.
3. In the Copy Profile window, type the new profile name.
4. Click **OK**.

Deleting System Profiles

To delete a system profile, you must be a member of the System Administrator role.

To remove a system profile, do the following:

1. In the Contents area, select the system profile.
2. From the menu, click **Selected —> Delete**. The Delete System Profile window opens.
3. Click **Yes** to delete the profile.

Activating System Profiles

To activate system profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Operator
- Service Representative

To activate a system profile, do the following:

1. In the Contents area, select the system profile.
2. From the menu, click **Selected—> Activate**.

Validating That System Profiles Will Activate Successfully

If a partition profile in a system profile requires a resource that is currently in use by the system or another partition, the system profile does not activate.

To validate system profiles, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Operator
- Service Representative

To determine whether a system profile will activate successfully, do the following:

1. In the Contents area, select the system profile.
2. On the menu, click **Selected**.
3. Select **Validate**.

If a situation exists that prevents the profile from activating successfully, a window displays that provides you with the details.

Note: This validation is approximate, and depends on which part of the memory block is being allocated to the current running partitions.

Activating System Profiles When Other Partition Profiles Are Running

To activate a system profile, shut down the operating system for any active partition, so that the partition's state changes from *Running* to *Ready*.

Powering On Using a System Profile

You can power on your managed system by using a predefined system profile. For more information about powering on using a system profile you have already created, see "System Profile" on page 77.

Chapter 18. Virtual Terminal Window

Because the physical serial ports on the managed system can only be assigned to one partition, the virtual terminal window implementation enables an AIX system console to be accessed on logical partitions that have no physical serial port assigned. A telnet connection directly to the partition is not sufficient, because AIX needs a terminal for restarts, installations, and for some service functions.

One virtual terminal window is available for each partition. Likewise, one virtual terminal window is available for each managed system.

The communication link between the HMC and the managed system is an RS-232 serial line running at 19,200 bits per second. All virtual terminal window sessions send and receive data on this shared serial line.

The virtual terminal window is a terminal with limited function. After you create a partition and configure its operating system, the typical operating system connection method is through a serial port, telnet, or rlogin. The virtual terminal window is meant to be used for support and service. Performance cannot be guaranteed due to the limited bandwidth of the serial connection.

The virtual terminal window supports the following:

- AIX system-management applications such as **smitty**.
- Other curses-driven applications.
- Standard POSIX line-discipline behaviors, so that applications that use serial ports do not need to be rewritten. However, some General Terminal Interface characteristics are not applicable.

The virtual terminal window emulates a vt320 terminal.

As a limited function terminal, the virtual terminal does not support the following:

- Printing to a virtual terminal
- Transparent print services
- Modem connection for the virtual console port
- Real-time applications

The tty that is configured on the AIX Virtual TTY Adapter is predefined as a vt320. To set the terminal type on a virtual terminal window, use the following AIX command:

```
export TERM=vt320
```

Virtual Terminal Windows on a Full System Partition

For a Full System Partition, the output of the S1 serial port is redirected, or *wrapped* to the virtual terminal window. When the S1 serial port is wrapped, the output of any command is directed from the S1 serial port to the virtual terminal window. If you close the virtual terminal window on the managed system, normal function is restored to the S1 serial port.

If a physical device is attached to the S1 serial port and that device is asserting the Data Carrier Detect (DCD) signal, the session on the S1 serial port does not wrap to the virtual terminal window until the device is powered off or removed. Likewise, if the S1 port has been wrapped to the virtual terminal window and a device is attached to the S1 serial port, the virtual terminal window must be closed to unwrap the S1 session.

When the managed system is in the *No Power* state, you can access the service processor configuration menus from this console session.

Opening a Virtual Terminal Window

To open a virtual terminal window, you must be a member of one of the following roles:

- Operator
- Advanced Operator
- System Administrator
- Service Representative

You can have only one virtual terminal window per partition open at a time.

To open a virtual terminal window, do the following:

1. Click the plus sign (**+**) next to the managed system in the Contents area to expand the tree.
2. Select a partition underneath the managed system.
3. Select **Open Terminal Window**. A virtual terminal window opens on your HMC desktop.

Opening Virtual Terminal Windows on a Partition

One terminal window is available for each defined partition. You can also open a terminal window for a managed system, but there is no interaction with the managed system after the partition has been powered to the *Running* state. The S1 serial port is not wrapped when the managed system is partitioned.

A terminal window can be opened at any time, regardless of the state of the partition, similar to powering on or off a tty terminal. The virtual terminal window might be blank until the partition is activated.

Installing and Using AIX in a Virtual Terminal Window

This section provides information about installing and using AIX in a virtual terminal window.

Installing AIX on a Full System Partition

If you install AIX for a Full System Partition, select the S1 serial port as the console. The virtual terminal window device driver installs, but it does not load. If you then choose to boot the installed disk in a partition, one of the following may occur:

- If the S1 serial port is assigned to the partition you want to boot, the S1 serial port continues to have the AIX console assigned to it. If you open the virtual console port, the screen may remain blank, because no virtual terminal window device has been enabled for that port.

  To get a login to that port, use SMIT or Web-based System Manager to configure and enable a tty on the virtual terminal serial adapter. Another option is to assign that port as the AIX console. The following AIX commands are helpful when assigning the port:

  – The **lscons** command tells you which port the console is assigned to.
  – The **chcons** command allows you to permanently switch the default console to another serial port.
  – The **swcons** command allows you to temporarily switch the console to another port.
- If the S1 serial port is not assigned to that partition, AIX recognizes the missing console and displays prompts on all valid console devices, including the virtual console driver. If no console is selected within 30 seconds, AIX continues to boot without a console. If the console prompt times out, the virtual terminal window might remain blank until a console is defined.

Installing AIX on a Partition

If you install AIX in a partition that has the native serial adapter as one of its resources, the installation terminal is the default AIX console. If the virtual terminal is the console and the disk is booted for a Full System Partition, the virtual console device driver is not loaded.

To install AIX on a partition, do the following:

1. Open a virtual terminal window on the managed system so the S1 serial port is wrapped to that terminal. Because the original console is now no longer available, you have 30 seconds to select the S1 port as your console. Otherwise, that port may appear to hang.
2. Use the **chcons** command to change the console to avoid the 30-second timeout if you plan to use the Full System Partition with an operating system that was installed in a logical partition.

If you install AIX in a partition that does *not* have the native serial adapters as one of its resources, the device driver for the built-in serial adapter is not installed in that partition. AIX does not install device support for a physical device unless the device is present at the time of installation. Do not attempt to boot that image as a Full System Partition until you first install the correct device support.

The following steps describe one method of adding device support:

1. Add the native serial adapter and the CD device to your partition profile.
2. Boot the partition with the new resources.
3. Run the following command to add the device support:

   ```
   cfgmgr -i /dev/cd0
   ```

Managing AIX Device Drivers on Partitions

When you activate AIX in a partition, the operating system loads a device driver that emulates a serial port device driver. AIX considers this device driver to be a serial device adapter. For example, the following command:

```
lsdev -C | grep sa
```

Returns output similar to the following:

```
LPAR Virtual Serial Adapter
```

A tty device is assigned to that adapter.

To install and boot, the AIX operating system requires a console window. On installation, AIX prompts you to select a serial port from which to install. This port becomes the default console port unless you change it.

One difference between the virtual terminal window device driver and a typical AIX console is that the virtual terminal window does not have to be opened in order to boot the AIX operating system. You can boot all defined partitions simultaneously without opening a virtual terminal window, provided that the partition profiles' boot mode is set to **Power On Normal**.

Copying and Pasting Within a Virtual Terminal Window

You can copy and paste within a virtual terminal session only. To copy and paste in a virtual terminal, do the following:

1. Use the mouse to draw a box around the text you want to copy.
2. Press and hold the Ctrl key and then press the Insert key to copy the text.
3. Press and hold the Shift key and then press the Insert key to paste the text.

For HMC Release 3, use the cut and paste method for Xwindows. To copy, hold down the left mouse button and highlight the text you want to copy. To paste, press the center mouse button. To paste using a 2-button mouse, click the left and right buttons simultaneously.

Closing a Virtual Terminal Window

There are two ways to close a virtual terminal window. The usual method of closing a terminal window is to click on the **X** in the upper-right corner of the terminal window. This action removes the window from the HMC desktop and closes the connection. Any user can close a terminal window in this way.

You can also force a virtual terminal window to close in the following situations:

- The terminal is open on another HMC and you want to turn off that session.
- The terminal has been opened by another HMC.

To force a virtual terminal window to close, you must be a member of one of the following roles:

- Operator
- Advanced Operator
- System Administrator
- Service Representative

To force a virtual terminal window to close, do the following:

1. Select the managed system from the Contents area.
2. Select **Close Terminal**.

Chapter 19. Software Maintenance for the HMC and the Frame

The applications in the Software Maintenance folder allow you to do the following:

- Receive corrective service
- Install corrective service
- Back up critical console data
- Save upgrade data
- Format removable media
- Manage a frame of managed systems and resources

To open the Frame and HMC Software Maintenance applications, double-click the **Software Maintenance** icon in the Navigation area.

The Software Maintenance application contains the service tasks for a Frame of managed systems and resources and the HMC. Use the Frame application to manage installed software to a Frame connected to the HMC. When you select the Frame application, you can receive and apply service from a diskette or from a remote system. The HMC application in the Software Maintenance folder allows you to manage installed HMC software.

Backing up Critical Console Data

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

- User-preference files
- User information
- HMC platform-configuration files
- HMC log files

The Backup Critical Console Data function saves the HMC data stored on your HMC hard disk to the DVD-RAM and is critical to support HMC operations. Back up the HMC after you have made changes to the HMC or to the information associated with partitions.

To back up critical console data, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Operator
- Service Representative

To back up critical console data, do the following:

1. In the Navigation area, click the **Software Maintenance** icon.
2. In the Contents area, double-click the **HMC** icon.
3. In the Contents area, select **Backup Critical Console Data**.
4. Select **Backup** to store your critical console data on the DVD-RAM.
5. Click **OK**.

Saving Upgrade Data

You can store system information onto the HMC hard drive in preparation for an HMC upgrade.

Note: Only perform this task immediately prior to upgrading your HMC software from one release to another. Any configuration changes made after performing this task will not be migrated to the new HMC software release.

When you complete this process, the HMC saves configuration data that includes the following:

- System preferences
- Profile information
- Service Agent files
- Inventory Scout Services files

To save upgrade data, you must be a member of one of the following roles:

- System Administrator
- Service Representative
- Advanced Operator

To save upgrade data to your HMC's hard disk, do the following:

1. In the Navigation area, click the **Software Maintenance** icon.
2. In the Contents area, double-click the **HMC** icon.
3. In the Contents area, select **Save Upgrade Data**.
4. Select **Save to hard drive** and follow the onscreen instructions.

Installing Corrective Service for the HMC

This task allows you to update the level of code on the HMC. Corrective fixes are available through ftp and CD-ROM.

Note: Because the HMC is a closed system, you cannot install additional applications on your Hardware Management Console. All the tasks you need to maintain the managed system, the underlying operating system, and the HMC application code are available by using the HMC's management applications.

To install a corrective fix, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To install a corrective fix, do the following:

1. In the Navigation area, click the **Software Maintenance** icon.
2. In the Contents area, double-click the **HMC** icon.
3. In the Contents area, click **Install Corrective Service**. The Install Corrective Service window opens.
4. Do one of the following:

   If you have a corrective fix on removable media, insert the media in the appropriate drive and click **Apply corrective service from removable media**.

   OR

   If you want to download the fix from a remote site and have the necessary information from your support representative, click **Download corrective service from remote system, then apply downloaded service file**. Then type the Web address, patch file, ID, and password information in the appropriate fields. This information is available from your software support representative.
5. Click **OK**.

Formatting Removable Media

You must format removable media before it can be used in the HMC.

To format removable media, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator
- Operator
- Service Representative

To format removable media, do the following:

1. In the Navigation area, click the **Software Maintenance** icon.
2. In the Contents area, double-click the **HMC** icon.
3. In the Contents area, select **Format Removable Media**.
4. Insert the media, either diskette or DVD-RAM, into its appropriate drive.
5. Click **Continue** to format the media.

Receiving Corrective Service for the Frame

This task allows you to receive corrective service for the frame from either the HMC's diskette drive or by downloading the service from a remote site.

To receive a corrective service for the frame, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To receive a corrective fix, do the following:

1. In the Navigation area, open the **Software Maintenance** folder.
2. In the Contents area, double-click the **Frame** icon. The Frame application opens in the Contents area.
3. In the Contents area, click **Receive Corrective Service**. The Receive Corrective Service window opens.
4. Do one of the following:

   If you have a corrective fix on removable media, insert the media in the appropriate drive and click **Upload corrective service from diskette**.

   OR

   If you want to download the fix from a remote site and have the necessary information from your software support representative, click **Download corrective service from remote system**. Then type the Web address, patch file, ID, and password information in the appropriate fields. This information is available from your software support representative.
5. Click **OK**.

Installing Corrective Service on the Frame

This task allows you to update the level of code on the frame after you have received a corrective service. Corrective fixes are available through ftp and diskette.

Note: Because the HMC is a closed system, you cannot install additional applications on your Hardware Management Console. All the tasks you need to maintain the managed system, the underlying operating system, and the HMC application code are available by using the HMC's management applications.

To install a corrective fix on the frame, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To install a corrective fix, do the following:

1. In the Navigation area, open the **Software Maintenance** folder.
2. In the Contents area, double-click the **Frame** icon. The Frame application opens in the Contents area.
3. In the Contents area, click **Install Corrective Service**. The Install Corrective Service window opens.
4. Select the Corrective Service Version, and select the Frame where the service will be applied.
5. Click **Install**.
6. After the service has been applied, click **Cancel** to return.

Downloading and Installing Firmware and Microcode Updates

You can use your HMC to download and install newer system firmware and adapter and device microcode levels. This section describes how to download and install a managed system's firmware, and adapter and device microcode.

The IBM Service Web site maintains the latest firmware and microcode levels, and is updated from time to time. Therefore, available firmware and microcode levels can change from one day to the next. If you are attempting to update more than one managed system and want to maintain the same firmware and microcode levels across all of your systems, use the CD-ROM repository for updates. This way, you can ensure that each of your systems install the same update.

System firmware cannot be installed without interrupting the use of your managed system. You must reboot each system after you install system firmware.

1. In the Navigation area, select **Software Maintenance**.
2. Select **Microcode Updates**. The Microcode updates screen opens in the Contents area.
3. In the Contents area, click **Microcode Updates**.
4. In the **Select Repository Location** window, select the location from which you will install the update.

   Note: Note, in order to access the IBM Service Web site, your HMC must have direct access to the internet. If you do not have direct access to the internet, you must order service on a CD-ROM. This CD-ROM can be used on the HMC or can be made available on the internal network via an FTP Server.
5. In the **Download and Apply Microcode** window, select which resources and systems you want to survey to determine if they need an update.
6. The **Microcode License Agreement Message** opens. Read the agreement and accept it.
7. In the **Microcode Survey Results** window, the results of the survey display. For each device, a suggested action displays. Checkboxes in the **Install** column are already selected for any devices where an update is suggested, but you may select or deselect which devices you want to update by clicking the checkbox next to that device. If an update is not recommended for a device, the device will not be selectable.

   Attention: Updating managed system firmware is not a concurrent operation. When you click **Apply**, the managed system will shut down, apply the update, and then reboot.

   After reviewing all information and selecting which adapters or devices you want to update, click **Apply**. A message displays asking the you to verify all devices that will be updated. If the update requires a system reboot, another message displays asking you to confirm this action.

   The **Microcode Survey Results** window is then updated to reflect the new microcode levels.

Chapter 20. Service Agent

Service Agent (SA) accepts information from the Service Focal Point (SFP). It reports serviceable events and associated data collected by SFP to IBM for service automatically. The Service Agent Gateway HMC maintains the database for all the Service Agent data and events sent to IBM, including any Service Agent data from other Client HMCs.

This chapter provides an introduction to the Service Agent application. For a more detailed description of configuring and using Service Agent, see the *Electronic Service Agent for pSeries Hardware Management Console User's Guide*, available on the Web at ftp://ftp.software.ibm.com/aix/service_agent_code/HMC.

To access the Service Agent application, click the **Service Agent** icon in the Navigation area.

You can use Service agent to perform the following tasks:

- Report problems automatically; service calls are placed without intervention.
- Automatically send extended vital product data.
- Receive error notification automatically
- Support a networked environment with minimum telephone lines for modems

Any user can access Service Agent.

Working With Service Agent

You can use the Service Agent application to define machines. After machines are defined, they are registered with the IBM Service Agent Server (SAS). During the registration process, an electronic key is created, which becomes part of your resident Service Agent program. This key is used each time Service Agent places a call for service. The IBM Service Agent Server verifies the current customer service status from the IBM entitlement database. If you are entitled for customer service, the service call is placed.

Service Agent reports information to IBM to help with problem resolution. In some cases, this information may be used by IBM for other purposes. This information consists of the problem or error information itself, as well as Vital Product Data (VPD) or Inventory data.

In the event that the user is concerned about whether the information to be sent to IBM is sensitive, you can review the actual data by using either the Service Agent user interface or from the command line using file display programs. If, after reviewing the data and determining you do not want Service Agent to send data, you can use either of the following methods to prevent data from going to IBM.

- Within Service Agent, turn off the VPD-gathering feature. This action prevents VPD from being gathered and sent to IBM.

OR

- After registering, turn off the modem itself and configure the Service Agent Notification process to use e-mail to notify a help desk or have the help desk monitor Service Agent (in real time) using the Service Agent Alerts function. When Service Agent detects an error, you can then call IBM manually (instead of having Service Agent place the call).

Activating Service Agent

Service Agent for HMC is part of the HMC software. It is either preinstalled or is part of the HMC Recovery CD.

Activating Service Agent the First Time

Service Agent processes are turned off on a new system or after recovery. On new installations, the HMC host name is a default name. Assign a new HMC host name to fit your network environment. For more information about setting host names, see “Setting Host Names” on page 42.

On the Change SA mode window for a gateway server, both the gateway and client host names should be the same. If the settings are for a client, the client host name matches the HMC host name. You must update the gateway host name to reflect the HMC Service Agent gateway host. For more information about updating the gateway host name, see “Changing the Service Agent Mode” on page 127.

Use the Service Agent window for starting the processes when your account is ready to support Service Agent. On the HMC gateway, ensure that the modem and phone are connected correctly. Start Service Agent only after the network is set up correctly. Do not start Service Agent processes if the network is not configured on the HMC. For more information about setting up the network on the HMC, see “Customizing Network Settings” on page 40.

When you change the HMC host name for a client HMC, you must change the Service Agent gateway database before starting the client Service Agent to match the new client host name.

Configuring and Using Service Agent

The Service Agent interface is divided vertically into two panes, a navigation pane on the left and a detail viewing pane on the right.

The buttons at the top of the navigation pane are called *category selectors*. Each category determines the type of information that is displayed in the detail window to the right. The two menu items **File** and **Help** are also near the top of the navigation pane.

The bottom of the navigation pane contains two buttons labeled **Add** and **Delete**. These buttons are enabled, in Properties category view only, when they apply to the item selected. For example, you cannot add or delete when the Error view category is selected. If you want to delete a machine, you must switch to the Properties category first.

For more information about how to use Service Agent, read the *Electronic Service Agent for pSeries User's Guide*, available on the Web at

ftp://ftp.software.ibm.com/aix/service_agent_code/HMC .

Registering and Customizing the Service Agent User Interface

To start the Service Agent user interface, click **Service Agent UI - Registration/Customization**.

Any user role can use any Service Agent task.

To make an HMC report to another gateway HMC, see “Changing the Service Agent Mode” on page 127.

The first time you open Service Agent from the Hardware Management Console (HMC), you must type contact information, configure the modem, and confirm that Service Agent is correctly licensed. When you complete these tasks, Service Agent can correctly communicate with Service Focal Point, and error warnings can be sent to the appropriate service technician.

To configure Service Agent on the HMC, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double click the **Service Agent** icon.
3. In the Contents area, click **Service Agent Registration or Configuration**.

4. The Password window opens. Type the default password provided with your Service Agent interface. The default password, which is case sensitive, is:

   ```
   password
   ```

5. The License Agreement window opens. After reviewing the agreement, click **Accept**.
6. Type your contact information. The following describes the information for each field (fields marked with an **!** are required):

   Name Contact needed by the support center when making a service call.

   Phone Number
   Contact's telephone number

   Email Address
   Contact's e-mail address

   Country/Region
   Country or region

   Type Four-digit machine type of the first managed system attached to this HMC. This information is automatically updated if your HMC is connected to the managed system. If you want to select another managed system, click **Browse** and select the managed system.

   Serial Number
   Seven-digit serial number of the first managed system attached to this HMC. This information is automatically updated if your HMC is connected to the managed system.

   Model Three-digit model of the first managed system attached to this HMC. This information is automatically updated if your HMC is connected to the managed system.
7. Configure the modem. In the Navigation area, click the turnkey next to the **Network** icon.
8. In the Navigation area, click the turnkey next to the HMC host name that has the modem you want to configure.
9. In the Navigation area, click the **Dialer** icon.
10. In the Contents area, click **Browser** and select your primary work location. When you select a primary location, the following fields are automatically completed with the required information:

    Primary Phone Number

    Account

    User ID

    Password

    Primary Route

    Note: You must correct the telephone number for local calling standards. Remove the `1-area code` prefix if it is not needed. If it is necessary to dial 9 to get to an outside line, add the `9` prefix
11. In the Baud Rate field, select the appropriate modem from the list. Select a baud rate of **57600**.
12. In the **Dial Type** field, select the appropriate dial type.
13. Click **OK**. The modem is now configured.
14. Register your HMC with Service Agent and ensure that it is correctly licensed. In the Navigation area, click the turnkey next to the **Administration** icon.
15. In the Navigation area, click the **Register** icon.
16. At the bottom of the Machines area, click **Register**. The Service Agent Registration window opens.
17. Click **Yes** to connect to IBM.
18. A message window opens that prompts you to check the CallLog. Click **OK**.
19. Check the CallLog to make sure that the information was sent. In the Navigation area, click the **CallLog** icon. In the Contents area, review the status and ensure that the information was sent.

20. Ensure that Service Agent is correctly licensed. If Service Agent is not correctly licensed, it will not communicate correctly with Service Focal Point. In the Navigation area, click the **Network** icon.
21. Above the Navigation area, click the lock icon. The lock icon represents the Licensing action.
22. In the Contents area, check the **Status** column to ensure that Service Agent is correctly licensed.

Configuring Service Agent for Use in a Firewall Environment

There are two different ways to make Service Agent work in a firewall environment. If an internet connection is available through a firewall, then you can change the Connection Manager (CM) settings to make use of this connection (with or without proxy). If Service Agent must use the modem attached to an HMC to dial IBM, then you can use the CM process on an HMC outside the firewall with a modem. Then you can make changes to the CallController on the gateway to use this external HMC to dial in to IBM.

The Connection Manager and Dialer icons on any gateway can be used to control the CM process. However, you should only assign one Gateway User Interface per Connection Manager process and remove these icons from other gateways. The gateway system which has the CM process running can be called a Master Gateway

You must have a password to update the Service Agent Connection Manager (SACM) process. The password is stored in the **/usr/svcagent/cfg/sacmdef.cfg** file. The default password is `password` and can be changed by editing this file. (Key=CfgUpdatePassword). The UI (in CallController) stores this default password.

Configuring Service Agent with an Available Internet Connection

If an internet connection is available, you do not need to use a modem to configure Service Agent. To configure Service Agent with an available internet connection, do the following:

1. Disable dialing by selecting the **Connection Manager** icon. Then deselect the **Use Dialer to connect to SDR flag**. This tells CM that a direct connection to an IBM Server is available.
2. Configure proxy settings in the connection manager. Select the **Connection Manager** icon and type the appropriate information. Required information includes the following:
   - Type of proxy. (socks or HTTP)
   - Name of the proxy Server
   - Proxy Port
   - User ID & Password (Only if proxy authentication is required)
3. Click OK.

Configuring Service Agent without an Available Internet Connection

When an internet connection is not available, you can start CM on an HMC that is outside the firewall. A modem can be attached to this HMC and CM dials to IBM using this modem. In this scenario, the gateway HMC resides inside the firewall and the CallController on it can be configured to talk to this external CM. Only a single port must be opened for SA. By default this port is 1198. CallController can also utilize the proxy settings. HTTP & HTTPS proxies are supported in this scenario.

To configure a gateway to talk to a CM outside a firewall, do the following:

1. Open the Gateway SA user interface. Expand **Network** and **Gateway** and Select **CallController**.
2. Change the URLs in ConnectionManager to point to the external HMC system on which CM is running.
3. Type the proxy details (if required).

Stopping the Service Agent Interface

If the interface does not respond, you can close the Service Agent interface. From the Service Agent interface menu, select **File** and then **Exit**.

Any user role can stop the Service Agent user interface.

To stop the active Service Agent user interface, in the Contents area, click **Stop Service Agent UI**.

Starting Service Agent Processes

When you activate the Service Agent processes, all other menu options also become active.

Any user role can start the Service Agent processes.

To start the Service Agent Processes, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Start Service Agent Processes**.

Changing the Service Agent Mode

An HMC can be configured to report to another HMC. When you change the Service Agent mode, the actual call home is performed through the second HMC, therefore necessitating only one modem for a group of HMCs. Service Agent refers to the HMC with a modem as a *gateway* and the HMCs that are reporting errors as Service Agent *clients*. The gateway's machine type, model, and serial number are automatically completed. Client machine type, model, and serial number information must be manually completed.

Any user role can change the Service Agent mode.

To change the Service Agent mode, do the following:

1. On the gateway HMC, open the Service Agent user interface. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Service Agent user interface, do the following:
   a. Click the **Network** icon.
   b. Click **Add**.
   c. Select **Child**.
   d. From the menu, select **Machines**.
   e. Type the client information. In the **Node Name** window, type the following details for the HMC that you want to set up as a client:
      - Name: The IP name of the client HMC
      - IP Address: The IP address of the client HMC
      - Processor ID (optional): The managed system's ID
      - Type: The 4-digit type of the first managed system connected to this HMC
      - Serial No: The 7-digit serial number of the first managed system attached to the HMC
      - Model: The 3-digit model of the first managed system attached to this HMC
      - Manufacturer (optional): The name of the manufacturer of the managed system
4. On the client system, select **Service Applications –> Service Agent –> Change Service Agent Mode**. The Change Service Agent Mode window opens.

5. Click **Change Service Agent Mode**.
6. Type the client and gateway IP names.
7. Click **OK**.
8. On the gateway HMC, verify that the client is reporting to the gateway.
9. In the Contents area, click the icon that looks like a lock. This is the **License Status** icon.
10. In the Contents area, look at the column under the heading `Heartbeat`. Ensure that this client has successfully contacted the gateway HMC. To ensure that the client is correctly licensed, check the `License` column.

Enabling E-mail Notification

You can have Service Agent notify you by e-mail.

To enable E-mail notification, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Service Agent Registration or Configuration**.
4. The Service Agent application opens. Expand **Network**.
5. Select an HMC.
6. Click **Add**.
7. Select **Child —> Email Alert**.
8. Type the e-mail information as appropriate. To type more than one e-mail address in the E-mail address field, separate each address with a comma. The E-mail Server can be any mail server on the network. The E-mail Wait Time is the time that the system waits to collect information before sending the mail. Configure the type of error you want to be sent by enabling and disabling the options shown on the window. For more information about each of these options, refer to the Service Agent User's Guide.

Configuring the HealthCheck Interval

You can have Service Agent check on a regular basis to make sure that it is working properly. This check is called a *HealthCheck*.

To configure the HealthCheck interval, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Service Agent Registration or Configuration**.
4. The Service Agent application opens. Expand **Network**.
5. Expand the gateway HMC.
6. Click the **Call Controller** icon.
7. Complete the information as appropriate. For a description of each field, refer to the Service Agent User's Guide.
8. Click **OK**.

Sending Information Manually to IBM

You can send Service Agent information to IBM manually.

To send Service Agent Information manually, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Service Agent Registration or Configuration**.
4. The Service Agent application opens. Expand **Manual Tools**.
5. Select the information type you want to send to IBM.
6. Select the HMC and the appropriate action button.

Enabling Performance Management Data Collection

You can collect performance data from each of your partitions and send it to IBM every day. IBM uses this information to create performance reports for your system.

To collect performance management data, you must install the Performance Management application on your AIX partitions.

To enable performance management data collection, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Service Agent Registration or Configuration**.
4. The Service Agent application opens. Expand the **Network** icon.
5. Select the HMC that is monitoring the corresponding partitions for which you want to collect performance data.
6. Click the **Performance Management** icon.
7. Select the **false** check box so that it changes to **true**. Type the time you want this collection to occur. (default is between 2:00 a.m. and 5:00 a.m.).
8. If you want to ignore the errors generated during the performance management collection, select the check box underneath Enable generating Internal Errors so that it changes to **false**.
9. Click **OK**.

Stopping Service Agent Processes

This operation prevents all call-home functions.

Any user role can stop the Service Agent processes.

To stop all the Service Agent processes, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Contents area, double-click the **Service Agent** icon.
3. In the Contents area, click **Stop Service Agent Process**.

Service Agent Status Indicators

The status section in the Contents area displays the current status of all Service Agent processes as follows:

SA Mode

Indicates whether the primary server is a gateway server or a client server.

Gateway Machine
Displays the name of the gateway machine. On a gateway machine, the primary server and the client name are the same.

Secondary Server
Displays the server you have configured to be the secondary server.

Tertiary Server
Displays the server you have configured to be the tertiary server.

Client Name
Displays the name of the client and matches the node name that you entered using the Service Agent interface.

Service Agent Status
Displays whether the Electronic Server System (ESS) or the On Demand Server (ODS) applications are currently running.

Chapter 21. Service Focal Point

The Service Focal Point application is used to help the service representative diagnose and repair problems on partitioned systems. Service representatives use the HMC as the starting point for all service issues. The HMC groups various system management issues at one control point, allowing service representatives to use the Service Focal Point application to determine an appropriate service strategy.

Traditional service strategies become more complicated in a partitioned environment. Each partition runs on its own, unaware that other partitions exist on the same system. If one partition reports an error for a shared resource, such as a managed system power supply, other active partitions report the same error. The Service Focal Point application enables service representatives to avoid long lists of repetitive call-home information by recognizing that these errors repeat, and by filtering them into one error code.

The following types of errors are reported to Service Focal Point:

- Permanent hardware errors (detected by the managed system or operating system)
- LAN Surveillance errors detected by Service Focal Point
- Hardware boot failure errors

The following errors are not reported to Service Focal Point:

- Software errors
- Temporary hardware errors
- Undetermined hardware errors
- Informational hardware errors

Errors that require service are reported to the HMC as *serviceable events*. Because the HMC stores these serviceable events for 90 days and then discards them, it is important to have the partition and HMC date and time set correctly. For instance, if the date on a partition's software is set 90 days *behind* the HMC's set time, the serviceable events reported from this partition are immediately discarded. For more information about setting the HMC's date and time, see "Setting and Viewing the Console Date and Time" on page 39. To set the partition's date and time, see the documentation provided with the operating system that is running on that partition.

Getting Started

When you are setting up Service Focal Point, keep the following in mind:

- If the time configured on a partition is 90 days older than time configured on the HMC, serviceable events cannot be reported.
- Verify that the HMC host names are defined. For more information about using fully qualified and short host names, see "Setting Host Names" on page 42.
- If you need to add or change a partition name, see the "Assigning a Host Name to Your Partition" on page 26.

Testing Error Reporting

To ensure that Service Focal Point is configured correctly, generate a test error by doing the following:

1. In the partition, run diagnostics to test the managed system's operator panel.
2. When the diagnostics window asks you if you see 0000 on the managed system's operator panel, select **NO**. This action generates an error.
3. In the SRN window, press Enter to proceed.
4. When the system asks you if you want the error sent to Service Focal Point, select **YES**.
5. Type F3 to exit diagnostics.

6. Wait for one minute while the managed system sends the error to Service Focal Point.
7. Check the Serviceable Event window to ensure that the error was sent to Service Focal Point and that Service Focal Point reported the error. For more information about working with serviceable events, see “Working With Serviceable Events” on page 133.

Service Focal Point Settings

The Service Focal Point Settings task in the HMC Contents area allows you to configure your Service Focal Point application.

Note: The Advanced Operator, Operator, and Viewer roles have read-only access to the following tasks.

Automatic Call-Home Feature

You can configure the HMC to automatically call an appropriate service center when it identifies a serviceable event.

To enable or disable the call-home feature, you must be a member of one of the following roles:
- System Administrator
- Service Representative

To enable or disable the call-home feature for one or more systems, do the following:

Note: It is strongly recommended that you not disable the call-home feature. When you disable the call-home feature, serviceable events are not automatically reported to your service representative.

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, click **Service Focal Point Settings**.
4. The Service Focal Point Settings window opens. Select the **CEC Call Home** tab at the top of the window.
5. Click on the managed system you want to enable or disable.
6. Click **Enable** to enable call-home for the selected system, or click **Disable** to disable call-home for the selected system.
7. Click **OK**.

Setting Up Surveillance

Service Focal Point surveillance generates serviceable events when it detects communication problems between the HMC and its managed systems.

You can configure how you want the HMC to survey the following:
- The number of disconnected minutes that are considered an outage
- The number of connected minutes you want the HMC to consider a recovery
- The number of minutes between outages that are considered a new incident

To set up surveillance, you must be a member of one of the following roles:
- System Administrator
- Service Representative

To set up surveillance, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, select **Service Focal Point Settings**.

4. The Service Focal Point Settings window opens. Select the **Surveillance Setup** tab on the top of the window.
5. In the first field, select the number of minutes you want the HMC to wait before sending a disconnection error message.
6. In the second field, select the amount of connection time that the HMC is considered to be recovered. This amount is expressed in minutes.
7. In the third field, select the number of minutes between outages that you want the HMC to wait before sending a new incident report.
8. Select one or more managed systems from the table in the lower part of the window, then click **Enable** or **Disable**. Surveillance is then either enabled or disabled for the selected managed systems.

Enabling Surveillance Notifications

You can enable or disable surveillance-error notification from this HMC to connected managed systems. Enabling this notification causes errors to be passed to the Service Agent application for notification.

Note: You must further configure Service Agent to handle notifications sent by Service Focal Point. For more information about Service Agent, see Chapter 20, “Service Agent,” on page 123.

To set up surveillance, you must be a member of one of the following roles:

- System Administrator
- Service Representative

To set up surveillance-error notification, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, select **Service Focal Point Settings**.
4. The Service Focal Point Settings window opens. Select the **Surveillance Notification** tab at the top of the window.
5. Select one or more managed systems from the list, and click **Enable** or **Disable**. Surveillance notification is then either enabled or disabled for the selected managed systems.

Working With Serviceable Events

You can view, add, or update serviceable event information, including error details.

Viewing Serviceable Events

To view serviceable events, you must be a member of one of the following roles:

- System Administrator
- Service Representative
- Advanced Operator
- Operator
- Viewer

To view a serviceable event, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, click **Select Serviceable Event**.
4. Designate the set of serviceable events you want to view. When you are finished, click **OK**.
5. The Serviceable Event Overview window opens, and the entries displayed are ordered by time stamp. Each line in the Serviceable Event Overview window corresponds to one error within a serviceable

event. On this window, designate the set of serviceable events you want to view by specifying your search criteria (such as event status or error class).

Note: Only events that match *all* of the criteria that you specify are shown.

6. When you are finished, click **OK**.

When you select a line in the Serviceable Event Overview window, all lines in the same serviceable event are selected. To open the Serviceable Event Details window for the selected event, select the event and click **Event Details**.

Viewing Serviceable Event Details

To view serviceable event details, do the following:

1. Perform the steps in "Viewing Serviceable Events" on page 133.
2. The Serviceable Event Details window opens, showing extended serviceable event information, including the following:
   - Status
   - Earliest original time stamp of any managed object
   - AIX error log. (The Linux system error log does not place entries into Service Focal Point.)
   - Should this error ever get called home?
   - Error was called home
   - Pointer to extended error-data collection on the HMC

   The window's lower table displays all of the errors associated with the selected serviceable event. The information is shown in the following sequence:
   - Failing device system name
   - Failing device machine type/model/serial
   - Error class
   - Descriptive error text

Viewing Serviceable Event Error Details

To view serviceable event error details, do the following:

1. Perform the steps in "Viewing Serviceable Event Details."
2. Select an error in the lower table, and click **Error Details**.

Viewing Service Processor Error Details

To view service processor error details, do the following:

1. Perform the steps in "Viewing Serviceable Event Error Details."
2. If the serviceable event error details you are viewing are for a service processor-class error, the lower table on the resulting window contains service processor errors. Select a service processor error from the lower table, and click **Service Processor Error Details** to see further details.

Saving and Managing Extended Error Data

To save extended error (EE) data, do the following:

1. Perform the steps in "Viewing Serviceable Event Details."
2. Click **Save EE Data**. To save extended error data for only *one* error associated with the serviceable event (rather than for the entire serviceable event), select the error from the lower table, and click **Error Details**. In the next menu, click **Manage EE Data**.

Viewing and Adding Serviceable Event Comments

To add comments to a serviceable event, you must be a member of the Service Representative or System Administrator roles.

To add comments to a serviceable event, do the following:

Note: You cannot edit or delete previous comments.

1. Perform the steps in “Viewing Serviceable Event Details” on page 134.
2. Select the error to which you want to add comments to and click **Comments**. If you want to close the event and add comments, click **Close Event** from this window. The Serviceable Event Comments window opens.
3. Type your name and add comments as appropriate. You can also review previous comments, but you cannot edit this information.
4. If you clicked **Comments** on the Serviceable Event Details window, clicking **OK** commits your entry and returns you to the Serviceable Event Details window.

If you clicked **Close Event** on the Serviceable Event Details window, clicking **OK** commits all changes and opens the Update FRU Information window. For more information about updating field replaceable unit information, see “Updating Field Replaceable Unit (FRU) Information.”

Closing a Serviceable Event

To close a serviceable event, do the following:

1. Perform the steps in “Viewing Serviceable Event Details” on page 134.
2. Click **Close Event** from this window. The Serviceable Event Comments window opens.
3. Click **OK** to commit your comments. The Update FRU Information window displays. For information on completing this window, see “Updating Field Replaceable Unit (FRU) Information”. To close the serviceable event, click **OK** on the Update FRU Information window .

   Note: You must close a serviceable event after it has been serviced to ensure that if a similar error is reported later, it is called home. If an old problem remains open, the new similar problem is reported as a duplicate. Duplicate errors are neither reported nor called home to a service center. Close a serviceable event when the partition that reports the error is active. Closing the event causes the new status of the serviceable event to be correctly sent to the partition.

Updating Field Replaceable Unit (FRU) Information

This task allows you to update the FRU information you changed or modified as a result of this serviceable event. From this panel, you can also activate and deactivate LEDs and search for other serviceable events that contain the same FRU entries.

To update FRU information, do the following:

1. Perform the steps in “Viewing Serviceable Event Details” on page 134.
2. Click **FRU Information**. The Update FRU Information window opens.

   The lower table shows any parts that you have replaced or added during your current update session but that have not been committed to the serviceable event. The changes from the lower table are committed by clicking **OK** or **Apply**.

From this window, you can also activate and deactivate LEDs and search for other serviceable events that contain the same FRU entries.

Replacing an Existing FRU

To replace a part already listed for this serviceable event, do the following:

1. Perform the steps in “Updating Field Replaceable Unit (FRU) Information.”
2. In the upper table, double-click the part you want to replace.
3. If the FRU has a new part number, type it in the New FRU Part Number field.
4. Click **Replace FRU**. The Update FRU Information window displays the FRU replacement information in the lower table. Click **OK** or **Apply** to commit the changes to the serviceable event.

Adding a New FRU

You can add a part to the serviceable event that was not listed in the upper table of the Update FRU Information window. To add a new FRU for this serviceable event, do the following:

1. Perform the steps in “Updating Field Replaceable Unit (FRU) Information” on page 135.
2. Click **Add New FRU**.
3. Type the FRU’s location code and its part number in the appropriate fields.
4. Click **Add to List**. The Update FRU Information window opens and displays the newly added FRU in the lower table.
5. Click **OK** or **Apply** to commit these changes to the serviceable event.

   Note: After you click **OK** or **Apply**, you cannot change this information. If you clicked the **Close Event** button in the Serviceable Event Details window, then clicking **OK** also completes the close dialog and changes the status of the serviceable event to *Closed*.

Viewing Serviceable Event Partition Information

You can view partition information associated with this serviceable event. This information includes each affected partition’s state and resource use.

1. Perform the steps in “Viewing Serviceable Event Details” on page 134.
2. Click **Partition Information**.

Activating and Deactivating FRU LEDs

This task allows you to activate or deactivate a managed system’s system attention LED or any FRU LED. FRU LEDs are helpful in determining which FRUs need servicing.

To activate or deactivate a managed system’s system attention LED, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, select **Hardware Service Functions**. The LED Management window opens.
4. In the LED Management window, select one or more managed systems from the table.
5. Select either **Activate LED** or **Deactivate LED**. The associated System Attention LED is then either turned on or off.

To activate or deactivate a FRU associated with a particular managed system, do the following:

1. In the Navigation area, click the **Service Applications** icon.
2. In the Navigation area, double-click the **Service Focal Point** icon.
3. In the Contents area, click **Hardware Service Functions**. The LED Management window opens.
4. In the LED Management window, select one managed system from the table.
5. Click the **List FRUs...** button. The list of FRU slot indexes and their respective current LED states display.
6. Select one or more FRU slot indexes.
7. Click either the **Activate LED** or the **Deactivate LED** button.

The associated FRU LEDs are now either enabled (blinking) or off.

Chapter 22. Using the Command Line

This chapter describes the remote commands that you can run to perform HMC functions.

Note: The command line must not be used for a Controlled Access Protection profile and Evaluation Assurance Level 4+ configuration, because they apply to dynamic configuration only.

Remote Commands

You can perform basic HMC functions remotely by using the command line. These commands are located in the **/opt/hsc/bin** subdirectory. To enable or disable remote commands, see “Enabling and Disabling Remote Commands” on page 45.

Notes:

1. When using ssh to run HMC commands, the shell available on the HMC is restricted to the commands described in this chapter. Only a small subset of Linux commands is supported.
2. If you list elements using commas, no not use a space after the comma unless it is actually part of the element’s name.

Return Codes

If an error occurs throughout the execution of one of the commands described in this section, the command returns an exit code of 1. If no error occurs, the return code is 0.

bkprofdata Command

Backs up profile data.

Syntax

bkprofdata -m *"managed system"* **-f** *file-name* **[** *--help* **]**

Description

The **bkprofdata** command backs up profile data from a managed system onto a file.

Flags

-m	The name of the managed system where the profile data is located. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.
-f	The file that will contain the profile data.
--help	Prints help message.

Example

The following command backs up the profile data onto a file called myFile. The example assumes the user has already inserted a floppy diskette into the diskette driver and had issued the mount command. To back up the profile data onto a file called myFile, type the following:

```
bkprofdata -m "7040-681*3413444" -f /mnt/floppy/myFile
```

chcuod Command

Purpose
Changes a Capacity Upgrade on Demand (CUoD) attribute.

Syntax
chcuod -c [cuod | onoff] -o [d | e | s | m] -m *"managed system"* **-r [cpu | mem] [-k** *"activation key"* **-q** *quantity of cpu/mem to enable/disable* **[--help]**

Description
The **chcuod** command is used to change a Capacity Upgrade on Demand attribute.

Flags

-c Type of CUoD operation

- **cuod** for Permanent CUoD or Trial CoD
- **onoff** for On/Off CoD

-o The operation to perform.

- **s** Indicates a set activation key operation.
- **d** Indicates enabling Trial CoD.
- **e** Indicates enabling Trial CoD.

-m The name of the managed system where the CUoD attribute should be changed. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-k The activation key to be sent to the managed system.

-q The quantity of processors or memory to enable Trial CoD.

-r The resource type. Valid values are cpu for processors or mem for memory.

Examples
1. To enable Trial CoD for processors, type:
   ```
   chcuod  -c cuod -m  7040-111*1234567  -o  e  -r  cpu -q 1
   ```
2. To enable Trial CoD for memory, type:
   ```
   chcuod  -c cuod -m  7040-111*1234567  -o  e  -r  mem -q 2
   ```
3. To set the activation key, type:
   ```
   chcuod  -c cuod -m  7040-111*1234567  -o  s  -k  1234
   ```
4. To activate On/Off CoD processors, type:
   ```
   chcuod  -c onoff -m  7040-111*1234567  -r cpu -o m -q quantity
   ```
   where *quantity* is the number on on/off processors you want to deactivate.
5. To deactivate On/Off CoD processors, type:
   ```
   chcuod  -c onoff -m  7040-111*1234567  -r cpu -o m -q quantity
   ```
   where *quantity* is the final number of on/off CoD processors you want to have. For example, To deactivate 4 processors from a previously activated 6 processors, you would type the following:
   ```
   chcuod  -m  7040-111*1234567  -r cpu -o m -q 2
   ```
   2 is a result of 6 - 4.

chhmc Command

Modifies the Hardware Management Console's configuration.

Syntax

chhmc -c [*network* | *ssh* **] -s [** *enable* | *disable* | *add* | *modify* | *remove* **] [-i** *eth0* | *eth1* **[-a** *ip-address* **] [-nm** *network-mask* **]] [-d** *network-domain-name* **] [-h** *host-name* **] [-g** *gateway* **] [-ns** *DNS-Server* **] [-ds** *Domain-suffix* **] [** *--help* **]**

Description

The **chhmc** command modifies the Hardware Management Console's configuration.

Flags

-c	The type of configuration to modify. Valid values are ssh and network.
-s	The new state value of the configuration. When the configuration type is ssh, the valid values are enable and disable. When the configuration type is network, the valid values are add, modify and remove. Add and remove are valid only when specifying -ns or -ds.
-i	The interface to configure. Valid values are eth0 and eth1. This parameter can be used only with -s modify.
-a	The new network IP address. This parameter can be used only with the -i parameter.
-nm	The new network mask. This parameter can be used only with the -i parameter.
-d	The new network domain name. This parameter can be used only with -s modify.
-h	The new host name. This parameter can be used only with -s modify.
-g	The new gateway address. This parameter can be used only with -s modify.
-ns	The DNS server to add or remove. This parameter can be used only with -s add or -s remove.
-ds	The domain suffix to add or remove. This parameter can be used only with -s add or -s remove.
--help	Prints help message.

Examples

1. To change the Hardware Management Console host name, type the following:

   ```
   chhmc -c network -s modify -h mynewhost
   ```

chhmcusr Command

Modifies a user's properties on the Hardware Management Console.

Syntax

chhmcusr -u *user-name* **-t** *property-type* **-v** *new-value* **[** *--help* **]**

Description

The **chhmcusr** command changes a user's properties on the Hardware Management Console.

Flags

-u	The user name to be modified.
-t	The type of property to change. Valid values are passwd for changing a user's password, access for changing a user's access group name, desc for changing a user's description, and name for changing a user's name.
-v	The new value of the property. When changing access group name, valid values are op, advop, sysadmin, usradmin, svcrep, viewer. When changing the user's password, if no value is specified, the user will be prompted to enter the password on the command line.
--help	Prints help message.

Example

To change the user ″tester″ to ″sysadmin,″ type the following:

```
chhmcusr -u tester -t access -v sysadmin
```

chswpower Command

Purpose
Powers switch boards on and off.

Syntax
chswpower [**--help**] | **-f** *frame* **-g** *cage* **-s** {on | off }

Description
The **chswpower** command powers switch boards on and off. The switch represented by the input values is powered on or off according to the value of the **-s** option.

Flags

--help	Displays the command's usage statement to standard output.
-f *frame*	Specifies the frame to which the switch that is to be powered on or off belongs.
-g *cage*	Specifies the cage to which the switch that is to be powered on or off belongs.
- s {on | off }	Specifies whether the switch is to be powered on or off.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **chswpower** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples
1. To power off the switch in Frame 4, Cage 3, type:
   ```
   chswpower -f 4 -g 3 -s off
   ```
2. To power on the switch in Frame 1, Cage 4, type:
   ```
   chswpower -f 1 -g 4 -s on
   ```

Files

/opt/hsc/bin/command/chswpower	Location of the **chswpower** command.

Related Information
The **lsswtopol** command.

chhwres Command

Changes the hardware resource configuration.

Syntax

chhwres -r [mem | cpu | slot | led] -o [a | r | m | s] -m *"managed-system"* **[-p** *"source-partition-name"* **][-t** *"target-partition-name"* **][-i** *"drawer-id"* **][-s** *slot-id* **] [-l***physical location***][-q***quantity* **][-w** *timeout* **][-v** *LED setting* **][-d** *detail- level* **][-x** *LED index* **][-y** *LED type* **][--help]**

Description

The **chhwres** command changes hardware resource configuration and allows processors, memory, and slots to be reconfigured dynamically.

Flags

-r	The hardware resource type to change. Specify mem for memory, cpu for processor, slot for IO slot and led for LED.
-o	The operation to perform. For adding hardware resource specify a, for removing hardware resource r, for moving resources, m, and for setting led value, s.
-m	The name of the managed system where the hardware resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form mmmm*sssss, where mmmm is the machine model type and sssss is the machine's serial number.
-p	The user-defined name of the partition to perform the operation.
-t	The user-defined name of the partition to move the new hardware resource to.
-v	The value to set for the LED
-i	The drawer ID. This argument needs to be specified for slot resource only.
-s	The slot ID. This argument needs to be specified for slot resource only.
-l	The physical location code of the IO slot. This argument cannot be specified with the -i or -s flags.
-q	The quantity of hardware resource to change. For processor, this value will specify the number of processor to add, remove or move. For memory, this value will specify the number of LMBs only.
-w	The timeout value to be used by the Dynamic Resource Manager command running on the partition. Default value is 0, indicating that no timeout is used, and that the command on the partition will take as much time as it needs to complete the operation.
-x	The index number of the LED to set.
-y	The LED type. For system attention, specify sys, for identify, specify ident.
-d	The detail level to be used by the Dynamic Resource Manager command running on the partition. Valid values are 0 through 5.

Examples

1. To remove three processors from the partition named p1, type:

```
chhwres -m "7040-681*8386522" -p "p1" -r cpu -o r -q 3
```

2. To move 1 LMB from partition p1 to partition p2, type:

```
chhwres -m "7040-681*8386522" -p "p1" -t "p2" -r mem -o m -q 1
```

chswnm Command

Purpose
Enables and Disables the System Network Manager (SNM) Software and returns information about the enablement status of the SNM Software.

Syntax
chswnm [**-a** | **-d** | **-q** | **--help**]

Description
The **chswnm** command enables or disables the SNM Software. It performs the same function as the corresponding tasks on the SNM Overview panel of the SNM GUI. It also can be used to display the enablement status of the SNM Software.

Flags

-a	Enables the SNM Software. If the SNM Software is already activated, a return code of 1 is returned.
-d	Disables the SNM Software. If the SNM Software is already disabled, a return code of 1 is returned.
-q	Queries the enablement status of the SNM Software. If the software is activated a return code or 0 is returned. If the software is disabled, a return code of 0 is returned.
--help	Displays the command's usage statement to standard output.

Exit Status

0 0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **chswnm** command is restricted to users with the role of HSC_Sys_Prog.

Examples
1. 1. To enable the SNM Software, type:

   ```
   chswnm -a
   ```

2. To query the enablement status of the SNM Software, type:

   ```
   chswnm -q
   ```

chsyscfg Command

Changes hardware resource configuration.

Syntax

chsyscfg -r [*alpar* / *lpar* / *prof* / *sysprof* **] -m** *"managed system"* **[-p** *"partition-name"* **] [-f** *configuration-file* / **-i** *attribute-value ="value" ...* **] –n name [** *--help* **]**

Description

The **chsyscfg** command changes the hardware resource configuration.

Flags

-r The system resource type to modify. Valid values include the following:

alpar Affinity logical partition

lpar Partition

prof Profile

sysprof System profile

-m The name of the managed system where the hardware resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-p If the resource type is prof, the user-defined name of the partition where the hardware resource will be removed.

-f The file containing the configuration information needed to modify the resource object. Format of data in this file must be of the form: attribute-name=attribute value There must be no spaces surrounding the equal sign (=). Each attribute/value pair must be on separate lines.

-i This option allows user to enter configuration information on the command line, instead of using a file. Data entered at the command line must follow the same format of data in the configuration file. For LPAR profile resource type:

-name (String)

-minimum_cpu (number)

-maximum_cpu (number)

-desired_cpu (number)

-minimum_mem (number of MBs)

-maximum_mem (number of MBs)

-desired_mem (number of MBs)

-desired_io (comma separated)

Physical location code:

-service_authority (0 - off, 1 - on)

- required_io (comma separated)

-sfp_surveillance (0 - off, 1 - on)

-sni_config_mode (0 - basic, 1- advanced)

-sni_device_id (numbers comma separated)

-sni_windows (numbers that are a multiple of 16 and comma separated

In this form:

-boot_mode

Valid values are:

norm Normal

dd Diagnostic default boot list

sms SMS

of OpenFirmware OK prompt

ds Diagnostic Stored Boot List

-small_rmo (1 - off, 2- on) For partition resource type:

-name (String)

-default_profile_name (String) For system profile resource type:

name (string)
The partition name

partitions (string)
The system profile's partition names

profile_names (string)
The system profile's profile names

-n The name of the object whose attribute will be modified.

--help Prints help message.

Examples

1. To change the user-defined name of a system profile from sysprof to sysprof1, type the following:

```
chsyscfg -r sysprof -m 7040-345*1234567 -n sysprof -i "name=sysprof1"
```

2. To change various attributes of a partition profile, type the following:

```
chsyscfg  -r  prof  -m  cec1  -p lpar1 -n prof1 -i  minimum_cpu=3 maximum_cpu=6
   desired_io+=UP13*2-3
    required_io+=UP13*2-4,UP13*2-7
```

3. To change various attributes of a partition profile using an input file, type the following:

```
chsyscfg -r prof -m cec1 -n lpar1 -f /home/hscroot/inputfile
```

The input file contains the following:

```
minimum_cpu=3
maximum_cpu=6
desired_io+=UP1.3*2-3
required_io+=UP1.3*2-4,UP1.3*2-7
```

chsysstate Command

Changes System State.

Syntax

chsysstate -r [*sys* / *lpar* / *sysprof* **] -o [** *on* / *off* / *reset* / *rebuild* / *shutdown* **] -m [**″*managed system*″**][-n** ″*object name*″] [-f *profile-name* **] [-c** *full* / *lpar* **] [-b** *norm* / *dd* / *sms* / *of* / *ds* / *std* **] [** *--help* **]**

Description

The **chsysstate** command changes the system state

Note: This command only works when the system is powered down.

Flags

-r The system resource type to modify. Valid values `lpar` for partition, `sys` for managed system, and `sysprof` for system profile.

-m The name of the managed system where the resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-n The name of the system resource object, whose state will be modified.

-o The operation to be performed on the object. Valid values are:

- **on** Powers on the managed system or activates a partition.
- **off** Powers off a managed system or issues a hard reset on a partition.
- **reset** Performs a soft reset on a partition.
- **rebuild** Rebuilds a managed system.
- **osshutdown** Shuts down a partition.

-b The boot setting option to use when powering on the managed system. Valid values are:

- **norm** Normal
- **dd** Diagnostic default boot list
- **sms** SMS
- **of** OpenFirmware OK prompt
- **std** Standby
- **ds** Diagnostic Stored Boot List
- **auto** Diagnostic Stored Boot List

-f The name of the profile to use when activating a partition.

--help Prints help message.

Examples

1. To power on a single LPAR, type:

```
chsysstate -m cec1 -r lpar -o on -n part1 -f prof1
```

2. To auto-start all valid LPARs, type:

```
chsysstate -r sys -o on -n cec1 -c lpar -b auto
```

hmcshutdown Command

Shuts down the Hardware Management Console.

Syntax

hmcshutdown -t {*number-of-minutes* | *now* **} [-r] [** *--help* **]**

Description

Use the **hmcshutdown** command to shut down the Hardware Management Console. Before the system is shut down, console surveillance will also be disabled.

Note: Only users belonging to System Administrator, PE, and Advanced Operator roles can issue the **hmcshutdown** command.

Flags

-r	Reboot the console. If this option is not specified, the system will be halted.
-t	The number of minutes to wait before halting or rebooting the system. The default value is 1 minute.
--help	Prints help message.

Examples

1. To reboot the hardware management console after 3 minutes, type the following:

   ```
   hmcshutdown -r -t 3
   ```

2. To halt the hardware management console immediately, type the following:

   ```
   hmcshutdown -t 0
   ```

lscuod Command

Lists information related to Capacity Upgrade on Demand.

Syntax

lscuod -c [cuod | onoff] -r [cpu | mem] -t [reg | order] -m *managed system* **[-F** *format names*]**[--help]**

Description

The **lscuod** command lists information related to Capacity Upgrade on Demand.

Flags

-c The type of CUoD operation. Valid values are *cuod* for Permanent CUoD or Trial CoD, and *onoff* for On/Off CoD

-m The name of the managed system for which CUoD information should be listed. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-r The type of resources to query the information. Valid values are cpu for processor and mem for memory.

-t The type of listing to display. Valid values are reg for regular CUoD resource information, or order for CUoD resource order information.

-F A delimiter separated list of name representing the desired properties to query. Valid values are:

- capacity_card_ccin
- capacity_card_id
- capacity_card_serial_num
- cpu_activated
- cpu_capacity_cond
- cpu_days_hours
- cpu_entry_check
- cpu_seq_num
- immed_cpu
- immed_mem
- installed_cpu
- installed_mem
- mem_activated
- mem_capacity_cond
- mem_days_hours
- mem_entry_check
- mem_seq_num
- not_perm_cpu
- not_perm_mem
- perm_cpu
- perm_mem
- resource_id
- system_serial_num
- system_type

--help Prints help message.

Example

To print the processor's CUoD order information, type the following:

```
lscuod -c cuod -m cecl -r cpu -t order -Fcpu_days_hours:system_type
```

lshmc Command

Displays the Hardware Management Console's configuration.

Syntax

lshmc [-n] [-v] [-V] [-r] [-F *format* **] [** *--help* **]**

Description

The **lshmc** command displays the Hardware Management Console's configuration.

Flags

-n	Displays network information.
-v	Displays console's VPD information.
-V	Displays HMC version information.
-r	Displays remote command execution settings.
-F	If specified, a delimiter separated list of property names to be queried. Valid values are: hostname domain nameserver domainsuffix gateway ipaddr networkmask ssh
--help	Prints help message.

Examples

1. To display the Hardware Management Console host name, type the following:

   ```
   lshmc -n -Fhostname
   ```

2. To display the Hardware Management Console host name and network IP address, type the following. The ':' is used as a delimiter in the output string.

   ```
   lshmc -n -Fhostname:ipaddr:
   ```

lshmcusr Command

Displays a user's properties on the Hardware Management Console.

Syntax

lshmcusr -u {ALL | *user-name*}**[-F** *format*]**[**--*help*]

Description

The **chhmcusr** command displays a user's properties on the Hardware Management Console.

Flags

-F	If specified, a delimiter-separated list of names of properties to be queried. Valid values are name, access, role, description. Specifying access will return the user's access group as a keyword, such as sysadmin, that can be used as input to a subsequent mkhmcusr or chhmcusr command. Specifying role will return the user's access group as a printable string, such as System Administrator. When this option is specified, the output will be returned as a delimiter-separated list of the values requested
-u	The user name to be displayed.
--help	Prints help message.

Example

To display information about user hscroot, type the following:

```
lshmcusr -u hscroot
```

lshwinfo Command

Displays hardware information.

Syntax

lshwinfo -r *sys* **-e** *frame-name* **[-n** *object-name* **| --all] [-F** *format* **] [** *--help* **]**

Description

The **lshwinfo** command displays hardware information.

Flags

-n	The name of the object to perform listing on. This parameter cannot be specified with **--all**.
-r	The resource type to display. Valid value is sys for system.
--all	List all the objects of a particular resource type. This parameter cannot be used with **-n**.
-F	If specified, a delimiter separated list of property names to be queried. Valid value is `temperature`.
--help	Prints help message.

Example

To display the temperature information of the frame, type the following.

```
lshwinfo -r sys -e "frame1" -n "740-010*D1300K0" -Ftemperature
```

lshwres Command

Lists hardware resource configuration.

Syntax

lshwres -m *"managed-system"* **[-p** *"partition-name"* | **--all] -r [** *resource-type* **] [-y** *"led-type"* **][-F** *format* **][** *--help* **]**

Description

The **lshwres** command lists the hardware resource configuration.

Flags

-m — The name of the managed system where the hardware resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-p — The user-defined name of the partition where the hardware resource will be queried.

--all — Retrieve information from all partitions on the given managed system.

-r — The hardware resource type to view. Possible values are ALL, cpu (processor), mem (memory), slot (PCI slot) sma or led.

-y — Type of LED to list. To list system attention led, use the keyword sys. To list identify LED, use the keyword identify.

-F — If specified, a delimiter separated list of names representing desired properties to be queried. Valid values are:

- system
- name
- key
- state
- status
- id
- parent
- location
- classcode
- assigned_to
- index
- location_code
- max
- min
- allocated
- free
- lmb_size
- drawer_id
- slot_id
- slot_type
- phys_loc
- partition
- partition_name
- sni_windows
- sni_device_id
- network_id

--help — Prints help message.

Examples

1. To list all processors in the system, along with the status and the partition assignment, type the following:

   ```
   lshwres -m "7040-681*8386522" -r cpu
   ```

2. To list all processor information for partition p1, type the following:

   ```
   lshwres -m "7040-681*8386522" -r cpu -p p1
   ```

3. To print the partition name, along with the minimum and maximum memory value for partition p1, type the following. The ':' is used as the delimiter on the resulting output.

   ```
   lshwres -m "7040-681*8386522" -r mem -p p1 -Fpartition_name:min:max
   ```

4. To indicate that there are 2 CPUs whose name is blank, whose IDs are 2 and 3, and to indicate that one is currently assigned to lpar0, type the following:

   Note: CPU 2 is not assigned to any partition, so the last token is set to null.

   ```
   lshwres -m "system1" -t cpu -Fname:id:state:assigned_to:

   Will print:

   :2:1::
   :3:1:lpar0:
   ```

   Note: Using the **-F** flag returns the actual value stored, while the next example shows how the command formats the CPU state and status into user-readable text.

5. To print a header line followed by rows of information (CPU belonging to system system1), type:

   ```
   lshwres -m "system1" -r cpu
   ```

   Output will be similar to the following:

   ```
   id  Status          partition       assigned_to
   2   Configured by System
   4   Configured by System
   0   Configured by System
   6   Running         001*740-681*8888  lpar1
   ```

lslpars Command

Purpose
Displays a table of information about all systems, partitions and profiles managed by the HMC.

Syntax
lsswenvir [**-m** *managed system*] [**--wide**] [**-help | -h**]

Description
The **lslpars** command displays a table of information about all systems, partitions and profiles managed by the HMC.

Flags

--help | -h	Prints the command's usage statement to standard output.
--wide	Prints the full partition and profile names and complete operator panel code values.
-m	Reports information about a specific managed system.

Examples
1. To view information about systems profiles and partitions managed by the HMC, type the following:

   ```
   lslpars
   ```

   The following is an example of information displayed:

   ```
   ================================================================================
    Managed System/LPAR     State               Operator Panel   Activated Profile
   ================================================================================
    R4EMUL1                  Ready               LPAR.       ....
      FullSystemPartit...     Not Available
      lp1                     Ready
    --------------------------------------------------------------------------------
   ```

lssvccevents Command

Purpose
Lists HMC events.

Syntax
lssvcevents -t { *hardware* | *console* **} [-d** *number-of-days-to-go-back* **] [-m** *"managed-system"* **] [-s {***ALL* | *sp* | *lpar***}] [-p** *"partition-name"* **] [-F** *format* **] [** *--help* **]**

Description
The **lssvccevents** command lists HMC events.

Flags

-t — The type of events to query. Valid values are hardware for Serviceable Events, or console for Console type events.

-d — The number of days to go back and query for Serviceable Events. By default, 7 will be used.

-m — The name of the managed system to gather events from. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system. This argument is ignored if the type of events to query is from the console.

-s — The source of the events to query. Valid values are:

- **sp** — Queries events from the Service Processor
- **lpar** — Queries events from the partitions
- **ALL** — Queries all events

This argument is valid only for hardware (serviceable) events.

-p — The name of the partition where the serviceable events come from. This argument is valid only for hardware (serviceable) events.

-F — If specified, a delimiter-separated list of property names to be queried. Valid values are name, time, callhome, calledhome, errorclass, description. When this option is specified, the output will be a delimiter-separated list of the values requested.

--help — Prints help message.

Examples
1. To display serviceable events from all partitions, type the following:
   ```
   lssvcevents -t hardware -m cec1 -s ALL
   ```
2. To display serviceable events from partition p2, type the following:
   ```
   lssvcevents -t hardware -m cec1 -s lpar -p p2
   ```
3. To display console events, type the following:
   ```
   lssvcevents -t console
   ```

lsswendpt Command

Purpose
Displays status about the end points and servers known to the Switch Network Manager (SNM).

Syntax
lsswendpt [**--help**] [**-F** *format*]

Description
The **lsswendpt** command displays the same data that is displayed in the End Point View panel of the Switch Network Manager GUI. If the **-F** *format* option is not specified, all of the fields are written to standard output, preceded by a header line. When the **-F** *format* option is specified, a colon-separated list of fields that you specify is displayed. Valid field names are status, frame, cage, server, adapter, network, plane, and port. In addition the total entities that are active (up_total) can be specified.

Flags

-F *format* Displays a colon-separated list of fields specified by the user to standard output. Valid field names are:

adapter
Displays the values for the adapter IDs in the adapter field. These values are returned for the server. The network, plane, and status fields also are associated with the server.

cage Displays the numbers that represent the physical location of the cages.

frame Displays the numbers that represent the physical locations of the frames. These values are returned for the server.

network
Displays the numbers that represent the logical configuration of the networks. These values are returned for the server.

plane Displays the numbers that represent the logical configuration of the planes. These values are returned for the server.

port Displays the numbers for the ports on an adapter (may be zero or one) These values are returned for the adapter.

server Displays the MTMS (machine, type, model, and serial number) of the server.

status Displays the status of the entity that is the subject of inquiry.

up_total
The number of links out of the total number for the server that are available and active.

--help Displays the command's usage statement to standard output.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **lsswendpt** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples
1. To display all fields with a header, type:

```
lsswendpt
```

```
frame  cage        server MTMS  up/total  adapter  network  plane  port       status
    1     4   7041-CIH*3456004       1/2                                    Partial
                                                0        2      0              Bad
                                                                     0          Bad
                                                                     1          Bad
                                                1        2      1             Good
                                                                     0         Good
                                                                     1         Good
```

2. To display the frame, cage, and up/total fields, type:

```
lsswendpt -F frame:cage:up_total:

1:4:1/2:
```

Files

/opt/hsc/bin/command/lsswendpt Location of the **lsswendpt** command.

Related Information

The **lsswmanprop** and **lsswtopol** commands.

lsswenvir Command

Purpose
Displays the power environment for a switch board.

Syntax
lsswenvir [**--help**] | **-f** *frame* **-g** *cage*

Description
The **lsswenvir** command command displays the power environment for switch boards. For the switch board represented by the input values, each of two measurements for each of the two DCAs (distributed converter assemblies) in the switch is written to standard output, as follows:

- 1.8V Voltage [V] (biased)
- 1.8V Current [A]
- 3.3V Voltage [V]
- 3.3V Current {A]
- Internal DCA Temperature (Celsius)
- Switch Chip Temperature (Celsius)

Flags

--help	Prints the command's usage statement to standard output.
-f *frame*	Specifies the frame associated with the switch board whose power environment will be viewed.
-g *cage*	Specifies the cage associated with the switch board whose power environment will be viewed.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **lsswenvir** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples
1. To see power environmentals for the switch in Frame 2, Cage 2, type:

```
lsswenvir -f 2 -g 2
```

Files

/opt/hsc/bin/command/lsswenvir	Location of the **lsswenvir** command.

Isswmanprop Command

Purpose
Displays information about hardware management consoles (HMCs), networks, and planes. This is the same data that is displayed in the Management Properties panel of the Switch Network Manager GUI.

Syntax
Isswmanprop [**--help**] | **-t** {man | top | ver} [**-F** *format*]

Description
The **Isswmanprop** command displays information about hardware management consoles (HMCs), networks, and planes. This is the same data that is displayed in the Management Properties panel of the Switch Network Manager GUI.

To find out the current HMC master, including how long it has been the master, use the **-t** *man* option. A line is written to standard output with this information, followed by a line of data for each HMC in the switched cluster.

When the **-t** *top* option is specified, a line of data is written to standard output for each plane in each network in the switched cluster.

When the **-F** *format* option is specified, a colon-separated list of fields that you specify is displayed. Valid field names for the **-t** *man* option are hostname, ip, uptime, and version. Valid field names for the **-t** *top* option are endpoints_up, network, plane, and sw_links_up. The **-F** option is not valid with the **-t** *ver* option.

When the **-t** *ver* option is specified, information about the code level of the local HMC is written to standard output. This is the same data that is displayed when the Version tab on the Management Properties panel of the SNM GUI is selected.

Flags

-F *format* Displays a colon-separated list of fields specified by the user to standard output. This operand is valid only for the -t man and -t top option. -F may not be specified with the -t ver option. Valid field names for the **-t** *man* option are:

hostname
Displays the host name of the HMC.

ip Displays any IP addresses associated with the HMC.

uptime Displays the length of time (in days, hours, and minutes) that the HMC has been active since the last time the connection to the switch was lost.

version
Displays the version of the switch management RPM.

Valid values for the -t top option are:

endpoints_up
Displays the number of adapter connections that are working out of the optimal number of ports that are available on the fabric.

network
Displays the numbers that represent the logical configuration of the networks.The number of lines of output is determined by the number of combinations of networks and planes.

plane Displays the numbers that represent the logical configuration of the planes. The number of lines of output is determined by the number of combinations of networks and planes.

sw_links_up
Displays the number of links that are active on the fabric.

--help Displays the command's usage statement to standard output.

-t man | top | version Specifies the component about which you would like information:

man Management properties

top Topology information

version
Level of code of the HMC

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security

The **lsswmanprop** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples

1. To display management properties, type:

```
lsswmanprop -t man

ip-addr          host-name               up-time      version
9.117.7.122      hscf2.pok.ibm.com       Sep18,10:11  1.0-1
9.117.7.29       hscf1.pok.ibm.com       Aug21,12:11  2.0-3
9.114.27.123     c96hmc2.ppd.pok.ibm.com Apr12,8:34   1.2-2
```

2. To display topology information for the fields network, plane and endpoints_up, type the following:

```
lsswmanprop -t top -F network:plane:endpoints_up:

1:0:4:
1:1:0:
2:0:8:
2:1:8:
```

3. To display version information, type:

```
lsswmanprop -t ver

Release      Version       Build-Level     Driver      Efix-Level
3            1.2            20021021.1      -           -
```

Files

/opt/hsc/bin/command/lsswmanprop	Location of the **lsswmanprop** command.

Related Information

The **lsswendpt** and **lsswtopol** commands

lsswtopol Command

Purpose
Displays the information known to the Switch Network Manager about switches and links. The information is displayed on the basis of an individual plane of a single network.

Syntax
lsswtopol [**--help**] | **-n** *network* **-p** *plane* [**-F** *format*]

Description
The **lsswtopol** command displays the information known to the Switch Network Manager about switches and links. This is the same data that is displayed in the Switch Topology View panel of the Switch Network Manager GUI. The information is displayed on the basis of an individual plane of a single network. You specify the network and plane to view. When the **-F** format option is specified, a colon-separated list of fields that you specify is displayed. Valid field names are frame, cage, power, chip, port, slot_riser, and status. When the **-F** option is not specified, all fields are written to standard output, preceded by a header line.

Flags

-F *format* Displays a colon-separated list of fields specified by the user to standard output. Valid field names are:

- **cage** Displays the numbers that represent the physical locations of the cages.
- **chip** Displays the chip number on the switch board (may be 0–7).
- **frame** Displays the numbers that represent the physical locations of the frames.
- **slot_riser** Displays the slot and riser port where the link is externally connected to the switch.
- **port** Displays the numbers of the ports on an adapter (may be 0–7).
- **power** Displays the power state of switch (may be on or off).
- **status** Displays the status of the entity that is the subject of inquiry.

--help Displays the command's usage statement to standard output.

-n *network* Specifies the network about which you would like information.

-p *plane* Specifies the plane about which you would like information.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **lsswtopol** command is restricted to users with roles of **HSC_Admin**, **HSC_Adv_Operator**, **HSC_Operator**, or **HSC_Serv_Rep**.

Examples
1. To display all fields with a header, type:

```
lsswtopol -n 2 -p 0
frame  cage  power  chip  port  slot-riser  status
    3     1     ON                          Good
                       0                     Good
                             0      S10-T1    Good
                             1      S10-T2    Good
                             2      S9-T1     Good
                             3      S9-T2     Good
                             4        -       Good
```

```
                                5        -       Good
                                6        -       Good
                                7        -       Good
etc.
```

2. To display the frame, cage, port, slot-riser, and status fields, type:

```
lsswtopol -n 2 -p 0 -F frame:cage:port:slot_riser:status:

3:1:::Good:
::::Good:
::0:S10-T1:Good:
::1:S10-T2:Good:
::2:S9-T1:Good:
::3:S9-T2:Good:
::4:-:Good:
::5:-:Good:
::6:-:Good:
::7:-:Good:
etc.
```

Files

/opt/hsc/bin/command/lsswtopol	Location of the **lsswtopol** command.

Related Information

The **chswpower**, **lsswendpt**, **lsswenvir**, and **lsswmanprop** commands.

lsswtrace Command

Purpose
Displays Switch Network Manager (SNM) log information.

Syntax
lsswtrace [**--help**] | [**--all** | **-F** *format*] [**-f** *filename*]

Description
The **lsswtrace** command displays Switch Network Manager trace log information. When the **-F** *format* option is specified, a colon-separated list of fields that you specify is displayed. The valid field names are described in the Options section. When neither the **-F** nor the **--all** option is specified, the default set of fields are written to standard output, preceded by a header line. The default set of fields is time, appl_name, network, plane, chip, port, and message. If **--all** is specified, all fields are written to standard output, preceded by a header line. The **-f** option is used to specify the name of a file on the HMC from which trace data is to be displayed. If **-f** is not specified, trace data is retrieved from the active trace file, **/var/hsc/log/fnmtrace.txt**.

Flags

--all Displays all trace fields, not just the default ones. May not be used with **-F**.

-F *format* Displays a delimiter-separated list of fields specified by the user to standard output. May not be used with **--all**. Valid field names are:

bpa_time
Displays the time that the event was observed by the BPA (bulk power assembly). The timing of events occurs in the following order (from earliest to latest): sw_tod, bpa_time, invoke_time, and log_time.

cage Displays the numbers that represent the physical location of the cages.

chip Displays the chip number on switch board (may be 0–7).

details Displays different data depending on the trace entry. It may be the MTMS (machine, type, model, and serial number) of the switch board that is associated with this trace entry, or it may be the routine name associated with this trace entry, or it may not be used.

file_name
Displays the name of the source file that invoked this trace entry.

file_ver
Displays the version of the source file that invoked this trace entry.

frame Displays the number that represents the physical location of the frame.

host_name
Displays the host name of the HMC that is reporting the trace entry. level Displays the severity level of the trace entry (there are seven possible levels).

line_num
Displays the line number in the source file where the trace call was made.

log_time
Displays the time when the trace entry was logged on the HMC. The timing of events occurs in the following order (from earliest to latest): sw_tod, bpa_time, invoke_time, and log_time.

message
Displays the text that the issuer of the trace entry wished to display. network Displays the logical number of the fabric with which this trace entry is associated.

plane Displays the logical number of the plane with which this trace entry is associated.

port Displays the ports on the adapter (may be zero or one) that are associated with this trace entry.

raw_data
Displays a hexadecimal dump of the information that the trace entry contains.

sw_tod
Displays the switch time of day when this event occurred on the fabric.The timing of events occurs in the following order (from earliest to latest): sw_tod, bpa_time, invoke_time, and log_time.

invoke_time
Time when the application source code invoked this trace entry. The timing of events occurs in the following order (frome earliest to latestr): sw_tod, bpa_time, invoke_time, and log_time.

type Location ID of the type of hardware where the event occurred.

-f *filename* Displays trace data from the file filename on the HMC, not the active trace file.

--help Displays the command's usage statement to standard output.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security

The **lsswtrace** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples

1. To see the default trace fields with a header, type:

```
lsswtrace

        time            appl_name       board MTMS   network   plane  type   chip   port
message
1040415692.402560        FNM_Init    7041-CIH*3456004          2      0       0     0       0
" list size is 0 "
etc.
```

2. To see all the trace fields with a header, type:

```
lsswtrace -a

      time        level       appl_name        board MTMS       network      plane     type
frame slot chip port log_time sw_tod bpa_time host_name
file_name file_ver line_num message
1040765798.576400 trace_notify         FNM_Init      7041-CIH*3456004     0     0     0
0      0      0      0   1040765798.577034      0        0  c409hmc2.ppd.pok.ibm.com
/afs/aix/u/cxhong/sbox/db/src/hmcpok/exp_restrict/fnmd/fnm_init/FNM_Init.cpp %I
2432 "cleanCSPInitList:               CSPInit list (size is 2):
etc.
```

3. To see the trace fields time, appl. name, and type from the trace data in the file /tmp/problem_trace.txt, type:

```
lsswtrace -F time:appl_name:type: -f /tmp/problemtrace.txt
1040765798.576305:FNM_Ela:1:

etc.
```

Files

/opt/hsc/bin/command/lsswtrace	Location of the **lsswtrace** command.

Related Information

lssyscfg Command

Lists system configuration information.

Syntax

lssyscfg -r [*ALL* | *sys* | *frame* | *alpar* | *lpar* | *prof* | *sysprof* **] -n** *object-name* | **--all [-m** *"managed system"***] [-p** *"partition-name"* **] [-F** *format* | *-z***] [** *--help* **]**

Description

The **lssyscfg** command lists system configuration information.

Flags

-r — The system resource type to query. Valid values are:

- **alpar** Affinity logical partition
- **lpar** Partition
- **prof** Profile
- **sysprof** System profile
- **sys** Managed system
- **frame** Frame object
- **ALL** All configuration information

-n — The name of the object to perform the query on.

--all — If specified, retrieve information for all resource specified. This argument cannot be used with the -n flag.

-m — The name of the managed system where the resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-p — If the resource type is prof, the user-defined name of the partition where the resource will be queried.

-F A delimiter separated list of property names to be queried. Valid values are:

affinity_capability
boot_mode
cage_number
cec_capability
csp_surveillance_policy
csp_version
default_profile
desired_cpu
desired_io
desired_mem
lmb_size
maximum_cpu
maximum_mem
minimum_cpu
minimum_mem
mode
model
name
op_panel_value
op_panel_window_count
partition_profile
power_off_policy
required_io
runtime_capability
serial_number
service_authority
sfp_surveillance
small_rmo
sni_config_mode
sni_device_id
sni_windows
state
type
total_mem
total_cpu

-z Alternate format to display. Using this flag, attributes are displayed in the form attr=value per line. This flag cannot be specified with the -F.

--help Prints help message

Examples

1. To list system information, type:

```
lssyscfg -r sys -n cec1
```

The output will be similar to the following:

```
Name  CageNumLMBSize   Mode   State      CSPVersion    Model        OpPanel           S/N
cec1    256            255    Ready      V4.0          7041-606                      12345
```

2. To list profile information, type:

```
lssyscfg -r prof -m cec1 -p lpar1 -n prof1
```

The output will be similar to the following:

```
name=lpar1
maximum_cpu=4
maximum_mem=64
minimum_cpu=1,
minimum_mem=1,
desired_cpu=3,
desired_mem=3,
service_authority=1
sfp_surveillance=0
small_rmo=1,
sni_config_mode=1,
sni_device_id=0,1,
sni_windows=16,16,
desired_io=UP13-5
required_io=UP13-6
```

3. To list system profile information, type:

```
lssyscfg -r sysprof -m cec1 -n sysprof1
```

The output will be similar to the following:

```
Name    Profile
sysprof1   prof1/001*7040-600*1234567
```

4. To list LPAR information, type:

```
lssyscfg -r lpar -m cec1 -n lpar1 -z
```

The output will be similar to the following:

```
name=lpar1
dlpar_capability=0,
default_profile=prof2,
state=1
op_panel_value=1111
os_level=1.1, os_type=2,
phys_loc=1.14
```

5. To list affinity partition information, type:

```
lssyscfg -r alpar -m cec1 --all
```

The output will be similar to the following:

```
Name  id  DLPAR  State  Profile   OpPanel
lpar1  1  0     Ready  prof1
lpar2  2  0     Ready  prof2
lpar3  3  0     Ready  prof3
lpar4  4  0     Ready  prof3
```

6. To list state, type and operator panel value information about partition lp1, type the following:

```
lssyscfg -r sysprof -m 7040-345*1234567" -n lp1 -Fstate:type:op_panel_value:
```

The output will be similar to the following:

```
Ready:1111 002:
```

mkauthkeys Command

Adds or removes authentication keys on the HMC. Given an authentication key generated by running ssh-keygen on a a remote client, this command updates the key file in the user's home directory on the HMC.

Syntax

mkauthkeys [-a | -r | --add | --remove] < string >

Description

The **chhmc** command modifies the Hardware Management Console's configuration.

Flags

-a	Adds the ssh key
--add	
-r	Removes the key for the specified user id and host. < string > is the ssh key to add, or the id to remove.
--remove	

Examples

1. To add an ssh key generated for user *joe* at *somehost*, type the following:

   ```
   mkauthkeys -a 'adB8fqeZs2d-gg+q joe@somehost'
   ```

2. To remove an ssh key generated for user *joe* at *somehost*, type the following:

   ```
   mkauthkeys -r 'adB8fqeZs2d-gg+q joe@somehost'
   ```

3. To remove all ssh keys generated for user *joe* at *somehost*, type the following:

   ```
   mkauthkeys -r 'joe@somehost'
   ```

mkhmcusr Command

Creates a user on the Hardware Management Console.

Syntax

mkhmcusr -u *user-name* **-a** *access-name* **[-d** *"description"* **] [** *--help* **]**

Description

The **mkhmcuser** command creates a user on the Hardware Management Console.

Flags

-u — The user name to be created. The name must be between 1 and 32 characters in length and not begin with a digit (0-9).

-a — The access group name. Valid values are:

- op
- advop
- sysadmin
- usradmin
- svcrep
- viewer

-d — A string containing the description associated with the user.

--help — Prints help message.

Example

1. To create user tester, type the following:

   ```
   mkhmcuser -u tester -a op -d "Testing"
   ```

2. To create user user1, type the following:

   ```
   mkhmcusr -u user1 -a myuser1 -d super user
   ```

mksyscfg Command

Creates a hardware resource configuration.

Syntax

mksyscfg -r [*alpar* | *lpar* | *prof* | *sysprof* **] -m** *"managed-system"***[-p** *partition-name* **] [-f** *configuration-file* | **-i** *attribute-value ="value" ...* **] [** *--help* **]**

Description

The **mksyscfg** command creates a hardware resource configuration.

Flags

-r The system resource type to create. Valid values are:

alpar Affinity logical partition

lpar Partition

prof Profile

sysprof
System profile

-m The name of the managed system where the resource is configured. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.

-p If the resource type is prof, the user-defined name of the partition where the hardware resource will be removed.

-f The file containing the configuration information needed to create the resource object. Format of data in this file must be of the form: attribute-name=attribute value. There must be no space between the equal sign (=) and each attribute/value pair must be on separate lines.

-i This option allows the user to enter configuration information on the command line, instead of using a file. Data entered at the command line must follow the same format of data in the configuration file. For Affinity Logical Partition resource type:

-name (String)

-profile_name (String)

-partition_type

Valid values are:

2 - 4 processor configuration

3 - 8 processor configuration

-desired_io (comma separated)

In this form:

-service_authority(0 - off, 1 - on)

-sfp_surveillance(0 - off, 1 - on)

-sni_config_mode (0 - basic, 1- advanced)

-boot_mode

Valid values are:

norm normal

dd diagnostic default boot list

sms SMS

of OpenFirmware OK prompt

ds Diagnostic Stored Boot List

small_rmo (1 - off, 2- on)
Small RMO

For LPAR Profile resource type:

-name (String)

-minimum_cpu (number)

-maximum_cpu (number)

-desired_cpu (number)

-minimum_mem (number of MBs)

-maximum_mem (number of MBs)

-desired_mem (number of MBs)

-desired_io (comma separated)

In this form:

-required_io (comma separated)

In this form:

-service_authority (0 - off, 1 - on)

-sfp_surveillance (0 - off, 1 - on)

-sni_config_mode (0 - basic, 1- advanced)

-sni_device_id (numbers comma separated)

-sni_windows (numbers that are a multiple of 16 and comma separated

-boot_mode

Valid values are:

norm normal

dd diagnostic default boot list

sms SMS

of OpenFirmware OK prompt

ds Diagnostic Stored Boot List

small_rmo (1 - off, 2- on)
Small RMO

-name (String)
-profile_name (String)
-minimum_cpu (number)
-maximum_cpu (number)
-desired_cpu (number)
-minimum_mem (number of MBs)
-maximum_mem (number of MBs)
-desired_mem (number of MBs)
-desired_io (comma separated)

In this form:
-required_io (comma separated)

In this form:
-service_authority (0 - off, 1 - on)
-sfp_surveillance (0 - off, 1 - on)
-sni_config_mode (0 - basic, 1- advanced)
-sni_device_id (numbers comma separated)
-sni_windows (numbers that are a multiple of 16 and comma separated)
-boot_mode

Valid values are:

norm normal

dd diagnostic default boot list

sms SMS

of OpenFirmware OK prompt

ds Diagnostic Stored Boot List

small_rmo (1 - off, 2- on)
Small RMO

For system profile resource type:
-name
-sys_prof_partition_names (comma separated, cannot have 2 same values)
-sys_prof_profile_names (comma separated, cannot have 2 same values)

--help Prints help message.

Examples

1. To create a logical partition, type:

```
mksyscfg  -r  lpar  -m  cec1  -i  name=part1 minimum_cpu=1 maximum_cpu=2
desired_cpu=2 minimum_mem=256 maximum_mem=16384
    desired_mem=4 profile_name=prof1
   desired_io=U1.9-P13-I9
    required_io=U1.9-P13-I8,U1.9-P13-I7
```

2. To create a system profile, type:

```
mksyscfg  -r  sysprof  -m  cec1 -i name=sysprof1
partition_names=lpar1,lpar2  profile_names=prof2,prof4
```

3. To create an 8-way ALPAR using data from file **alpar_4.data**, do the following. The content of the **alpar_4.data** file is shown below (on separate lines):

   <RECSP>
   name=cl_alpar_1
   profile_name=cl_profile_1
   boot_mode=dd
   service_authority=1
   sfp_surveillance=0
   desired_io=U1.9-P13-I9
   required_io=U1.9-P13-I7
   <RECSP>
   name=cl_alpar_2
   profile_name=cl_profile_2
   boot_mode=sms
   service_authority=1
   sfp_surveillance=0
   desired_io=U1.9-P12-I8
   required_io=U1.9-P10-I7
   <RECSP>
   name=cl_alpar_3
   profile_name=cl_profile_3
   boot_mode=sms
   service_authority=1
   sfp_surveillance=0
   desired_io=U1.9-P12-I5
   required_io=U1.9-P12-I4
   <RECSP>
   name=cl_alpar_4
   profile_name=cl_profile_4
   boot_mode=sms
   service_authority=1
   sfp_surveillance=0
   desired_io=U1.9-P12-I3
   required_io=U1.9-P12-I2
   <RECSP>

   The command issued is: `mksyscfg -r alpar -m cec1 -f alpar_4.data`.

mkvterm Command

Opens a virtual terminal session.

Syntax

mkvterm -m *"managed system"* **[-p** *partition-name* **] [** *--help* **]**

Description

The **mkvterm** command opens a virtual terminal session. The session can be ended by typing ~ and **.** as the first characters on a line.

Flags

-m	The name of the managed system to open a Virtual Terminal session on. If there are multiple managed systems with the same user defined name, specify the managed system name enclosed in double quote and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.
-p	The user-defined name of the partition to open a virtual terminal session on.
--help	Prints help message.

Example

To open a virtual terminal session on partition lp1, type the following:

```
mkvterm -m "7040-681*3413444" -p lp1
```

rmhmcusr Command

Removes a user from the Hardware Management Console.

Syntax

rmhmcusr -u *user-name* **[** *--help* **]**

Description

The **rmhmcusr** command removes a user from the Hardware Management Console.

Flags

-u	The user name to be removed.
--help	Prints help message.

Example

To remove user tester, type the following:

```
rmhmcusr -u tester
```

rmsplock Command

Removes a lock set on the Service Processor.

Syntax

rmsplock -m *"managed-system"* **[--help]**

Description

The **rmsplock** command removes a lock set on the Service Processor.

Flags

-m	The name of the managed system on which to remove the lock. If there are multiple man- aged systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form mmm*ssss, where mmm is the machine type and ssss the serial number of the managed system.
--help	Prints help message.

Example

To remove any lock set in the Service Processor, type the following:

```
rmsplock -m "7040-681*3413444"
```

rmsyscfg Command

Removes a hardware resource configuration.

Syntax

rmsyscfg -r [*lpar* | *prof* | *sysprof* | *sys* **] -n name [-e** *frame-name* **] -m [-p** *partition-name* **] [** *--help* **]**

Description

The **rmsyscfg** command removes hardware resource configurations.

Flags

-r	The system resource type to be removed. Valid values are lpar for partition, prof for profile, sys for managed system and sysprof for system profile.
-n	The user defined name of the system object to be removed
-e	If the system resource type is sys, the frame where the managed system is contained in must be specified here.
-m	The name of the managed system where the hardware resource is configured. If there are multiple managed systems with the same user defined name, specify the managed system name enclosed in double quote and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.
-p	If the resource type is `prof`, the user defined name of the partition where the hardware resource is will be removed.
--help	Prints help message.

Examples

1. To remove a system, type:

   ```
   rmsyscfg  -r  sys -n  cec1
   ```

2. To remove an affinity partition, type:

   ```
   rmsyscfg  -r  alpar  -m cec1
   ```

3. To remove a logical partition, type:

   ```
   rmsyscfg  -r  lpar  -m  cec1  -n  lpar1
   ```

rmvterm Command

Closes a Virtual Terminal session.

Syntax

rmvterm -m *"managed system"* **[-p** *"partition-name"***] [***--help***]**

Description

The **rmvterm** command closes a Virtual Terminal session.

Flags

-m	The name of the managed system for which the virtual terminal session is to be closed. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.
-p	The user-defined name of the partition for which the virtual terminal session is to be closed.
--help	Prints help message.

Example

To close a virtual terminal session on partition lp1, type the following:

```
rmvterm -m "7040-681*3413444" -p lp1
```

rsthwres Command

Restores a hardware resource configuration.

Syntax

rsthwres -m *"managed-system"* **[-p** *"partition-name"* **] -r [** cpu | mem | slot **] [-u** *processor id* **][-i** *drawer id* **-s** *slot id* | **-l***"physical location code"***][--help]**

Description

The **rsthwres** command restores a hardware resource configuration, following failure in dynamic logical partitioning reconfiguration.

Flags

-m	The name of the managed system where the profile data is located. If there are multiple managed systems with the same user-defined name, specify the managed system name enclosed in double quotes and of the form *mmm*ssss*, where *mmm* is the machine type and *ssss* the serial number of the managed system.
-p	The user defined name of the partition to perform restore on. This argument must be enclosed in double quotes.
-r	The hardware resource type to restore. Possible values are: **cpu** Processor **mem** Memory **slot** Slot
-u	The processor ID of the processor to restore.
-i	The machine type and serial number of an I/O slot's scoping drawer. This argument should not be specified if the resource type is not slot.
-s	The slot number of a PCI slot to restore.
-l	The physical location code of the IO slot. This argument cannot be specified with the **-i** and **-s** flags.
--help	Prints help message.

Example

To restore memory on partition p1, type the following:

```
rsthwres -m "7040-681*8386522" -r mem -p "p1"
```

rstprofdata Command

Restores profile data.

Syntax

rstprofdata -m *"managed system"* **-f** *file-name* **-l** *restore-type* **[** *--help* **]**

Description

The **rstprofdata** command restores profile data for a managed system from a file.

Flags

-m The name of the managed system where the profile data is to be restored. If there are multiple managed systems with the same user defined name, specify the managed system name enclosed in double quote and of the form mmm*ssss, where mmm is the machine type and ssss the serial number of the managed system.

-f The file that contains the profile data.

-l The type of restore to performed. Valid values are:

1 full restore from file

2 merge current profile with the backup having priority

3 merge current profile with the managed system having backup priority

--help Prints help message.

Example

The following command restores the profile data from a file called myFile. The example assumes the user has already inserted a floppy diskette into the diskette driver and had issued the mount command. To restore the profile data from a file called myFile, type the following:

```
rstprofdata -m "7040-681*3413444" -f /mnt/floppy/myFile -l 1
```

testlinecont Command

Purpose
Allows you to perform the line-continuity diagnostic test.

Syntax
testlinecont [**--help**] | **-f** *frame* **-g** *cage* [**-c** *chip* [**-o** *port*]] [**-n**]

OR

testlinecont [**--help**] | **-f** *frame* **-g** *cage* [**-a** *adapter* [**-o** *port*]] [**-n**]

Description
The **testlinecont** command performs a diagnostic test on links. If the **-c** and **-o** options or the **-a** and **-o** options are not specified, the test is performed on all links on the switch or server specified by **-f** *frame* and **-g** *cage*. If the **-o** option is not specified, the test is performed on all ports of the chip specified by **-c** chip in **-f** *frame* and **-g** *cage* or on all ports of the adapter specified by -a adapter in **-f** *frame* and **-c** *cage*. If all operands are specified, the test is performed on the link represented by the input values. The results are written to standard output. Since the line-continuity test is a disruptive test, a confirmation prompt is issued before each link is tested. The user must respond that he or she wishes the test to proceed. If the user desires to not have to respond to a confirmation prompt, the **-n** option maybe used to cause all tests to be issued without confirmation prompts.

Flags

--help	Displays the command's usage statement to standard output.
-a *adapter*	Specifies the adapter whose links are to be tested.
-c *chip*	Specifies the chip whose links are to be tested.
-f *frame*	Specifies the frame whose links are to be tested.
-g *cage*	Specifies the cage whose links are to be tested.
-n	Specifies that no confirmation prompts are to be used.
-o *port*	Specifies the port which is to be tested.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **testlinecont** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples
1. To run the Line Continuity diagnostic test against the link in Frame 1, Cage 3, Adapter 1, Port 1, type:

   ```
   testlinecont -f 1 -g 3 -a 1 -p 1

   Attention: This will affect cluster operation. The targeted link will be removed from the
   active configuration for the duration of the test. Do you wish to proceed? (yes/no)
   yes
   ```

2. To run the Line Continuity diagnostic test against all the links in Chip 7 in Frame 3, Cage 2, type:

   ```
    testlinecont -f 3 -g 2 -c 7
   ```

   (The prompt is issued for each of the eight links on the chip. The test is run against each prompt responded to with **yes**.)

Files

/opt/hsc/bin/commnad/testlinecont	Location of the **testlinecont** command.

updhmc Command

Updates code on the Hardware Management Console.

Syntax

updhmc -t m | s [-h *ftp server* -u *user id* [-p *password* | -i] -f *patch file on server*] [-r] [--help]

Description

The **rstprofdata** command updates code on the HMC. This command performs the equivalent of the Install Corrective Service task.

Flags

-t	The source type to update from. Valid values include the following: • m - media • s - server
-h	Host name or IP address of the FTP server where the patch file is located. Only valid when s is specified on the -t flag.
-u	User ID to use on the FTP server
-p	Password to use on the FTP server. The password will be in clear text. When running the command interactively, use the -i parameter for entering a password without echo.
-i	Prompts for password. Password will be hidden.
-f	File on the FTP server to obtain.
-r	Reboot HMC after applying the update.
--help	Prints help message.

Examples

1. The following command performs an update using media and reboots afterwards. To perform an update using media and reboot, type the following:

   ```
   updhmc -t m -r
   ```

2. The following command performs an update using a server and a viewable password. To perform an update using a server and a viewable password, type the following:

   ```
   updhmc -t s -h hostname -u user1 -p password -f /tmp/Update1.zip
   ```

3. The following command performs an update using a server and a password prompt. To perform an update using a server and a password prompt, type the following:

   ```
   updhmc -t s -h hostname -u user1 -i -f /tmp/Update1.zip
   ```

verifylink Command

Purpose
Allows you to perform the verify-link diagnostic test.

Syntax
verifylink [--help] | **-f** *frame* **-g** *cage* [**-c** *chip* [**-o** *port*]]

OR

verifylink [--help] | **-f** *frame* **-g** *cage* [**-a** *adapter* [**-o** *port*]]

Description
The **verifylink** command performs a diagnostic test on links. If the **-c** and **-o** options are not specified, the test is performed on all links on the switch or server in the frame specified by **-f** *frame* and **-g** *cage*. If the **-o** option is not specified, the test is performed on all ports of the chip specified by **-c** *chip* in **-f** *frame* and **-g** *cage* or on all ports of the adapter specified by **-a** *adapter* in **-f** *frame* and **-c** *cage*. If all operands are specified, the test is performed on the link represented by the input values. The results are written to standard output.

Flags

--help	Displays the command's usage statement to standard output.
-a *adapter*	Specifies the adapter whose links are to be tested.
-c *chip*	Specifies the chip whose links are to be tested.
-f *frame*	Specifies the frame whose links are to be tested.
-g *cage*	Specifies the cage whose links are to be tested.
-o *port*	Specifies the port which is to be tested.

Exit Status

0 Indicates successful completion of the command.

1 Indicates that an error occurred.

Security
The **verifylink** command is restricted to users with roles of HSC_Sys_Prog, HSC_Adv_Operator, HSC_Operator, or HSC_Serv_Rep.

Examples
1. To run the Verify Link diagnostic test against the link in Frame 1, Cage 2, Chip 0, and Port 4, type:
   ```
   verifylink -f 1 -g 2 -c 0 -p 4
   ```
2. To run the Verify Link diagnostic test against both ports in Adapter 1 in Frame 2, Cage 0, type:
   ```
   verifylink -f 1 -g 0 -a 1
   ```

Files

/opt/hsc/bin/command/verifylink	Location of the verifylink command.

Related Information
The **testlinecont** command.

The pesh Command

The **pesh** command is used by support personnel. To provide support personnel the ability to retrieve certain HMC trace and debug information, you can create a user named hscpe and assign this user a password. The hscpe user has similar access as the hscroot user on HMC. Support can then contact you,

obtain the password and remotely connect to the HMC. This allows support personnel the ability to perform additional functions, such as viewing logs or starting an HMC problem determination trace. When the hscpe user accesses the HMC remotely via ssh, you will also be operating in the restricted shell environment.

The **pesh** command allows this user to run in an unrestricted shell if the serial number of the HMC is correctly passed to the command. You must then enter a password obtained from support. If the password is correct, the user is now put into the unrestricted shell as user hscpe.

Converting Commands for HMC Release 3 Version 1.0, 1.1 (1st ptf), 1.2 (2nd PTF) to HMC Release 3 Version 2.0, 2.1 (1st ptf), 2.2 (2nd PTF) and Later Commands

The ″Old Commands″ listed in this table are no longer supported. Change scripts using these commands to use the new commands listed in “Remote Commands” on page 137.

Read the following table to learn about each old command’s new replacement:

HMC Release 3 Version 1.0, 1.1 (1st ptf), 1.2 (2nd PTF) Commands	HMC Release 3 Version 2.0, 2.1 (1st ptf), 2.2 (2nd PTF) and Later Commands
power_on_cec -c ″*managedSystem*″ -m mode -b boot_setting	**chsysstate** -r sys -o on -n ″*managedSystem*″ -c mode -b boot_setting
power_off_cec -m ″*managedSystem*″	**chsysstate** -r sys -o off -n ″*managedSystem*″
get_cec_state -m ″*managedSystem*″	**lssyscfg** -r sys -n ″*managedSystem*″
get_cec_mode -m ″*managedSystem*″	**lssyscfg** -r sys -n ″*managedSystem*″
get_op_panel -m ″*managedSystem*″	**lssyscfg** -r sys -n ″*managedSystem*″
query_cecs	**lssyscfg** -r sys --all
start_partition -p ″*partitionName*″ -f ″profile name″ -m ″*managedSystem*″	**chsysstate** -r lpar -o on -m ″*managedSystem*″ -n ″*partitionName*″ -f ″profile name″
reset_partition -m ″*managedSystem*″ -p ″*partitionName*″ -t hard	**chsysstate** -r lpar -o off -m ″*managedSystem*″ -n ″*partitionName*″
reset_partition -m ″*managedSystem*″ -p ″*partitionName*″ -t soft	**chsysstate** -r lpar -o reset -m ″*managedSystem*″ -n ″*partitionName*″
get_partition_state -m ″*managedSystem*″ -p ″*partitionName*″	**lssyscfg** -r lpar -m ″*managedSystem*″ -n ″*partitionName*″
get_op_panel -m ″*managedSystem*″ -p ″*partitionName*″	**lssyscfg** -r lpar -m ″*managedSystem*″ -n ″*partitionName*″
query_partition_names -m ″*managedSystem*″	**lssyscfg** -r lpar -m ″*managedSystem*″ --all
query_profile_names -m ″*managedSystem*″ -p ″*partitionName*″	**lsysscfg** -r prof -m ″*managedSystem*″ -p ″*partitionName*″ --all
get_cec_mtms -m ″*managedSystem*″	**lssyscfg** -r sys -n ″*managedSystem*″
get_cec_version -m ″*managedSystem*″	**lssyscfg** -r sys -n ″*managedSystem*″
get_cec_version -a	**lssyscfg** -r sys --all

Commands for HMC Release 3 Version 1.0, 1.1 (1st ptf), 1.2 (2nd PTF) and Earlier

Use the flags in the order shown in this table.

Command	Flags	Function
get_cec_mode	-m *"managed system"*	Indicates whether the managed system is in full mode or partition mode
get_cec_mtms	-m *"managed system"*	Returns the machine type and serial number in the following format: *machinetype_serialnumber*
get_cec_state	-m *"managed system"*	Returns the current state of a managed system
get_cec_version	-m *"managed system"*	Returns the managed system's supported version.
get_op_panel	-m *"managed system"* -p *"partition name"*	Displays operator panel LED contents for the specified partition
get_partiton_state	-m *"managed system"* -p *"partition name"*	Returns the current state of a partition
power_off_cec	-m *"managed system"*	Powers off a managed system
power_on_cec	-c *"managed system"* -m full | lpar -b *boot setting* where boot setting = norm | dd | sms | of | ds | std Use the Standby (std) boot setting when booting to Partition (lpar) mode. Use the other five boot settings when booting to Full Machine Partition (full) mode: Normal (norm), Diagnostic Default Boot List (dd), SMS (sms), OpenFirmware OK Prompt (of), and Diagnostic Stored Boot List (ds).	Powers on a managed system; -m starts it in either full or partition mode.
query_cecs	(none)	Returns the user-defined names of all the systems managed by the HMC.
query_partition_names	-m *"managed system"*	Returns the names of all defined partitions on a managed system
query_profile_names	-m *"managed system"* -p *"partition name "*	Returns profile names for the specified partition on the managed system
reset_partition	-m *"managed system"* -p *"partition name"* -t < *reset type* > where < *reset type* > = < hard | soft >	Performs a hard or soft reset of the operating system loaded on a partition
start_partition	-p *"partition name"* -f *"profile name"* -m *"managed system"*	Starts a partition with a given profile

Setting up Secure Script Execution Between SSH Clients and the HMC

To enable unattended script execution between an **ssh** client and an HMC, do the following:

Note: These steps assume that the SSH protocol is already installed on the system.

The following steps are examples from an ssh client running AIX:

1. Enable the SSH protocol on the HMC. In the Navigation area, select **HMC Maintenance**.
2. In the Navigation area, click **System Configuration**.
3. In the Contents area, click **Enable/Disable Remote Command Execution**.
4. When the window opens, select the box to enable ssh.
5. Create an HMC user with one of the following roles:
   - System Administrator
   - Service Representative
   - Advanced Operator
6. On the AIX system, run the the SSH protocol key generator. To run the SSH protocol key generator, do the following:
   a. To store the keys, create a directory named **$HOME/.ssh** (either RSA or DSA keys can be used).
   b. To generate public and private keys, run the following command:

      ```
      ssh-keygen -t  rsa
      ```

      The following files are created in the **$HOME/.ssh** directory:

      ```
      private key: id_rsa
      public  key: id_rsa.pub
      ```

      The write bits for both `group` and `other` are turned off. Ensure that the private key has a permission of 600.
7. On the AIX system, use the **scp** (secure copy) command to move **authorized_keys2** to a temporary file on the HMC by using the following command:

```
scp $HOME/.ssh/id_dsa.pub userid@hostname:/home/hmcmanager/.ssh/authorized_keys2
```

Deleting the Key from the HMC

To delete the key from the HMC, do the following:

1. On an AIX partition, use the **scp** command to copy the **authorized_keys2** file from the HMC to the AIX partition.

   ```
   scp userid@host name :.ssh/authorized_keys2 /tmp/mykeyfile"
   ```
2. Edit the **/tmp/mykeyfile** file and remove the line containing the key and host name that you want to disable password prompting when remotely executing HMC command with **ssh**.
3. On an AIX partition, use the **scp** command to copy the new file over to the HMC by using the following command:

   ```
   scp /tmp/mykeyfile userid@hostname ".ssh/authorized_keys2"
   ```
4. If you want to enable password prompting for all hosts accessing the HMC via **ssh**, use the following **ssh** command to remove the key file from the HMC:

   ```
   scp userid@hostname:.ssh/authorized_keys2 authorized_keys2
   ```

   Edit the authorized_keys2 and remove all lines in this file, then copy it back to the HMC.

   ```
   scp authorized_keys userid@hostname:.ssh/authorized_keys2
   ```

Appendix A. Communications Statements

The following statement applies to this product. The statement for other products intended for use with this product appears in their accompanying documentation.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer is responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

European Union (EU) Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. The manufacturer cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of option cards supplied by third parties. Consult with your dealer or sales representative for details on your specific hardware.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22 / European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

International Electrotechnical Commission (IEC) Statement

This product has been designed and built to comply with IEC Standard 950.

United Kingdom Telecommunications Safety Requirements

This equipment is manufactured to the International Safety Standard EN60950 and as such is approved in the UK under the General Approval Number NS/G/1234/J/100003 for indirect connection to the public telecommunication network.

The network adapter interfaces housed within this equipment are approved separately, each one having its own independent approval number. These interface adapters, supplied by the manufacturer, do not use or contain excessive voltages. An excessive voltage is one which exceeds 70.7 V peak ac or 120 V dc. They

interface with this equipment using Safe Extra Low Voltages only. In order to maintain the separate (independent) approval of the manufacturer's adapters, it is essential that other optional cards, not supplied by the manufacturer, do not use main voltages or any other excessive voltages. Seek advice from a competent engineer before installing other adapters not supplied by the manufacturer.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus meets the requirements of the Canadian Interference–Causing Equipment Regulations.

VCCI Statement

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 ＶＣＣＩ－Ａ

The following is a summary of the VCCI Japanese statement in the box above.

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Electromagnetic Interference (EMI) Statement - Taiwan

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

Radio Protection for Germany

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG–Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

The manufacturer may not offer the products, services, or features discussed in this document in other countries. Consult the manufacturer's representative for information on the products and services currently available in your area. Any reference to the manufacturer's product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any intellectual property right of the manufacturer may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any product, program, or service.

The manufacturer 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 the manufacturer.

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: THIS MANUAL IS PROVIDED ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED 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. The manufacturer may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

Appendix C. HMC Port Numbers

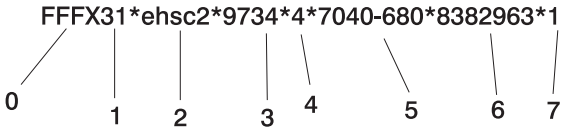
The following table describes an HMC open port protocol and the application used by each.

HMC Open Port Number/Protocol	Application
22/TCP	Secure Shell
80/TCP	Web Server
9090/TCP	WebSM initial connection
300000-300009/TCP	WebSM Communication
657/TCP	Resource Monitoring and Control
657/UDP	Resource Monitoring and Control

Appendix D. Using Scripts to Connect Remotely

You can open a virtual terminal to a partition remotely for maintenance purposes. This appendix describes how to connect to your HMC remotely.

The following script demonstrates one method for connecting to the HMC remotely, by using telnet. To connect to the virtual terminal without using the HMC Terminal Emulator, you must first build a connection string. The following is an example of an ASCII string that is sent to the HMC terminal server to establish a connection:



0: FFFX
Start of string indicator:

FFFX - connect and issue terminal open command

FFFF - connect but assume terminal is already open

1: 31 Count in integer ASCII. The number of characters that follow the `*` character, which follow the start of the string indicator. In the above example, count from `e` in `ehsc2` to the end of the string.

2: ehsc2
Host name or IP address of the HMC workstation.

3: 9734
Port number of control element. In this example, `9734` is the port number.

4: 4 Partition slot number. `0` is used to open a terminal on the managed system in both Partition Standby and Full System Partition modes. You can access the service processor menus from partition 0.

View the partition's properties to determine the partition slot number for a partition.

5: 7040-680
Machine type and model of the managed system. Use the managed system's properties panel to get the machine type and model. Do not use the user-assigned managed system name.

6: 382963
Serial number of the managed system. Use the HMC's properties panel to get the managed system serial number.

7: 1 TTY's session number.

After the connection string is built, you can connect to the HMC terminal server through a socket on port 9735. After the connection is made, the connection string is sent to the virtual terminal server.

You must set the telnet mode to `character`. To write the `ctrl ]` character into a script, you must use the sequence `ctrl v ctrl ]`.

To end the session, do one of the following:

- Press ctrl]

OR

- Click **Telnet** and then select **quit**.

This action runs the following script:

```
script_name hostname port partition machine_type/model*serial session_id
```

where:

- *hostname* = host name of the HMC
- *port* = fixed at 9734
- *partition* = the ID of the partition

The following example shows how you can use a script to connect to a remote system:

```
#!/usr/bin/expect -f

system "echo [string length $argv]"
system "echo [lindex $argv 0]"
system "echo [lindex $argv 1]"
system "echo [lindex $argv 2]"
system "echo [lindex $argv 3]"
system "echo [lindex $argv 4]"

spawn telnet [lindex $argv 0] 9735

expect "Escape"


# Note that the \r is not included in the send count
send -- "FFFX[string length $argv]*[lindex $argv 0]*
[lindex $argv 1]*[lindex $argv 2]*[lindex $argv 3]*[lindex $argv 4]\r"

sleep .5

# note: enter ^] using the sequence ctrl v ctrl ] on a unix system.
send -- "^]\r"


sleep .5

expect "telnet"

send -- "mode character\r"

interact
```

Appendix E. Error Messages and Recovery Information

The following tables contain information about error messages that can be displayed by the HMC during system configuration and operations.

Use this appendix to learn more about a specific error or information message. The table also includes recovery information (if applicable) to help you determine a recovery strategy.

Console Events Error Codes	Message	Recovery Action
HSCE2066	A scheduled backup of critical console data failed with a return code of {0}.	The possible return code values are: • 4 - A return code of 4 indicates the removable media could not be mounted. Recovery Action - Verify that the media is inserted properly in the drive and try the operation again. • 5 - A return code of 5 indicates that the removable media is write protected. Recovery Action - Remove the write protection and try the operation again. • Any value except 4 or 5 is an Internal HMC Error Recovery Action: 1. Perform Backup Critical Data task. 2. Call for HMC software support.

Inventory Scout Error Codes	Message	Recovery Action
HSCI0100	No managed systems were detected that are attached to this system console.	None
HSCI0101	No partitions have been defined for this managed system.	None
HSCI0102	A blank or invalid entry was entered in the partition password field.	Enter a valid password value.
HSCI0103	A blank or invalid entry was entered in the listening port field.	Enter a valid port value.
HSCI0104	A blank or invalid entry was entered in the IP address field.	Enter a valid IP address value.
HSCI0110	The Inventory Scout command completed successfully.	None
HSCI0111	The Inventory Scout command request failed	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.

Inventory Scout Error Codes	Message	Recovery Action
HSCI0112	The removable media cannot be mounted. Please make sure the media is inserted properly in the drive and retry the operation	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0113	The media specified is write protected. Please adjust the media and retry.	Remove the write protection and try the operation again.
HSCI0114	The Inventory Scout request failed. Ensure the removable media is properly inserted in the drive.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0115	An error occurred while copying the Inventory Scout data. Verify that a blank formatted diskette is inserted properly in the drive and retry the operation.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0116	An error occurred while compressing the Inventory Scout data. Please retry the operation.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0117	An error occurred while trying to unmount the media.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0118	The Inventory Scout daemon was restarted successfully.	None
HSCI0119	The Inventory Scout daemon could not be restarted.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware to determine if there is a hardware problem. 4. Call for HMC software support.

Inventory Scout Error Codes	Message	Recovery Action
HSCI0120	The internal managed system name is malformed. Please exit this task and retry the operation.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.
HSCI0121	The Inventory Scout request failed. An error occurred while copying data to removable media.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Call for HMC software support.

Inventory Scout Error Codes	Message	Recovery Action
HSCI0122	The system partition(s) did not respond to query attempts.	1. Check that the HMC host name and the host name of the partition are fully qualified domain name (not a short host name). If they are not, this must be corrected for remote security to work. 2. Verify the network routing is set up so the HMC can use ping to reach the partition and vice versa. If one or both cannot be reached from the other, correct the routing. 3. Check to make sure **/var** is not full on the partition, which would prevent certain processes from running correctly. 4. Verify that the following filesets have been installed properly on the AIX partitions: • **rsct.core** • **csm.client** • **devices.chrp.base.ServiceRM** 5. Log in to one of the partitions and issue the following command: `lssrc -s ctcas` . If the output shows ctcasd is inoperative, run an `ls -l` command on the **/var/ct/cfg/** directory. If the files **ct_has.pkf** and **ct_has.qkf** are zero-length, there was an (AIX) installation configuration problem. These zero-length files should be removed and then issue the command `startsrc -s ctcas`. If the `startsrc -s ctcas` command does not work, the AIX lpp may not have been installed. 6. If the output is still blank, reboot the HMC. After the reboot occurs, wait at least 10 minutes before trying again, to make sure all the partitions have resynchronized their information with the HMC. 7. If the problem persists, contact your software service support representative.

Profile Data Error Codes	Message	Recovery Action
HSCL0001	There is no more space for a new profile name. Reuse profile names being used by other profiles or remove the profiles that are no longer needed.	No more space for a new profile name is available. Reuse the profile names that are already used by other profiles, or remove the profiles that are no longer needed. Follow the procedures in this book to perform this action.
HSCL0002	Too many drawers are being used in profiles. Remove the drawers that no longer exist or are not needed.	Remove the drawers that no longer exist or are no longer needed. Follow the procedures in this book to perform this action.

Profile Data Error Codes	Message	Recovery Action
HSCL0003	The profile data save area is full. Remove any profiles that are no longer needed.	Remove the profiles that are no longer needed. Follow the procedures in this book to perform this action.
HSCL0004	A profile with name {0} already exists in the partition with ID {1} in profile data of the managed system. Provide another name for this profile.	Rename the profile to names that are not already in use in this partition. Follow the procedures in this book to perform this action.
HSCL0005	Cannot find information regarding profile data of the managed system. Execute a rebuild managed system operation.	1. Perform a rebuild managed system operation. 2. If the problem persists, contact your software service support representative.
HSCL0006	The managed system's profile data has been corrupted. You must either restore or reinitialize the profile data.	You must either restore or initialize the profile data. Follow the procedures in this book to perform this action.
HSCL0007	The profile data of the managed system cannot be accessed or modified. Execute a rebuild managed system operation	1. Perform a rebuild managed system operation. 2. If the problem persists, contact your software service support representative.
HSCL0008	Could not construct or initialize profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0009	Could not construct or initialize the profile data from the backup file, {0}. Repeat the operation.	Repeat the operation. Follow the procedures in this guide. If the problem persists, call for HMC software support..
HSCL000B	Could not get the activated LPAR profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL000C	Could not get the activated system profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL000D	Could not get all the system profiles from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL000E	Could not get the default LPAR profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL000F	Could not get the default system profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0010	Could not get the LPAR profiles for the partition from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.

Profile Data Error Codes	Message	Recovery Action
HSCL0011	Could not get the LPAR profiles at this partition from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0012	Could not get the system profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0013	Could not remove the LPAR profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0014	Could not remove the system profile from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0015	Could not save the LPAR profile to the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0016	Could not save the system profile to the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0017	Could not create the LPAR profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0018	Could not create the system profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0019	Could not set the activated LPAR profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL001A	Could not set the activated system profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL001B	Could not set the default LPAR profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL001C	Could not set the default system profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL001D	Could not clean up the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.

Profile Data Error Codes	Message	Recovery Action
HSCL001E	Could not update the profile data cache. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL001F	Could not check for duplicate LPAR name. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0020	Could not remove the LPAR profile from the system profile content in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0021	Could not add the LPAR profile to the system profile in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0022	Could not get the partition name from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0023	Could not get all the partition names from the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0024	Could not set the partition name in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0025	Could not build the profile data from the local file, {0}. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0026	Could not write the data to the managed system. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0027	Could not backup the profile data to a file. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0028	Could not read profile data from the managed system. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0029	Could not delete profiles at the partition with ID of {0} in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL002A	Could not modify the system profiles containing the LPAR slot ID of {0} in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.

Profile Data Error Codes	Message	Recovery Action
HSCL002B	Could not do a priority restore on the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL002C	Could not merge the profile information in profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL002D	Could not merge partition name data in the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL002E	Could not merge default and activated list data in profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL002F	Could not merge drawer and profile information data in profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0030	Unable to initialize the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0031	The profile data has been cleared. Either restore or reinitialize the profile data save area.	Perform restore profile data task or initialize the profile data. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL0032	Could not set the system profile’s user defined name to the profile data. Perform a Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL0033	This managed system version, {0}, is unknown to HMC. Update to an HMC release that can handle this version of managed system.	1. Perform the rebuild managed system operation. 2. If the same error occurs, update to an HMC release that can handle this version of managed system. 3. If you are not sure what version to use, contact software support.
HSCL0034	The levels of managed system and profile data area are not matching up. Managed system version: {0}, profile data area version: {1}. Upgrade the managed system version ″to proper level.″	1. Perform the rebuild managed system operation. 2. If the same error occurs, please update the managed system to a proper version. 3. If you are not sure what version to use, contact software support.
HSCL0035	Cannot restore profile data with 2 different versions of profile save data.	1. Perform the operation again. 2. If the same error occurs, restore using another profile data file.

Profile Data Error Codes	Message	Recovery Action
HSCL0036	Migrate profile data failed.	1. Perform the operation again. 2. If the problem persists, contact your software service support representative.
HSCL0037	This level of profile data, {0}, is unknown to this HMC. Please update to an HMC version that can handle this level of profile data.	1. Perform the operation again. 2. If the problem persists, update to an HMC version that can handle this level of profile data. 3. If you are not sure what version to use, contact software support.
HSCL0038	Creation of affinity logical partition profiles failed in profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, contact your software service support representative.
HSCL0039	Deletion of affinity logical partitions failed in profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, contact your software service support representative.
HSCL003A	Removal system profiles failed at profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, contact your software service support representative.
HSCL003B	Setting of partition information failed in profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, contact your software service support representative.
HSCL003C	Retrieval of all affinity logical partition information failed in profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, contact your software service support representative.
HSCL003D	Retrieval of partition information failed in profile data save area.	1. Perform the rebuild managed system operation. 2. Retry the operation again. 3. If the problem persists, call for HMC software support.
HSCL003E	Cannot build LPAR information from profile data save area when the managed system is not LPAR capable.	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL003F	Cannot build affinity logical partition information from profile data save area when the managed system is not Affinity LPAR capable.	The capabilities of your managed system are listed on the Machine tab of the property panel.

Profile Data Error Codes	Message	Recovery Action
HSCL0040	No more space for physical location code in the profile data save area.	1. Perform the rebuild managed system operation 2. Retry the operation again. 3. If the problem persists, call for HMC software support.
HSCL0041	Migration of partition information failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0042	Migration of profile names failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0043	Migration of default profile list failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0044	Migration of activated profile list failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0045	Migration of physical location code information failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0046	Migration of drawer and profile information failed in profile data save area	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0047	Migration of time stamps of profile data save area failed	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.
HSCL0048	Migration of checksums of profile data save area failed	1. Perform the rebuild managed system operation. 2. If the problem persists, call for HMC software support.

Managed System Error Codes	Message	Recovery Action
HSCL01F5	Unable to lock the Service Processor. Perform one of the following steps: (1) Check serial cable connection; (2) Check if another Console is communicating with the Service Processor; (3) Perform the Release Lock task; (4) Perform Rebuild task to re-establish the connection.	1. Wait for three minutes and retry the task. 2. If the problem persists, make sure other HMCs and remote login sessions of the HMCs are not performing any task. Then perform the Release HMC Lock task to unlock the service processor, and then try the task again. 3. Rebuild the managed system. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action. If the problem persists, contact the HMC support organization.
HSCL01F6	Unable to unlock the managed system lock. Perform the Release Hardware Management Console Lock to unlock the managed system.	1. Perform the Release HMC lock to unlock the service processor, and try the task again. 2. If the task still fails and a redundant HMC is present, turn off the redundant HMC power and try the task again. 3. Call for HMC software support.
HSCL01F7	Unable to get the current time from the managed system.	1. Try the task again. 2. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action. 3. Call for HMC software support.
HSCL01F8	This property cannot be altered.	None.
HSCL01F9	Unable to create managed system instance in object manager.	1. Try the task again. 2. Shut down and restart the HMC. 3. Try the task again. Follow the procedures in this guide.
HSCL01FA	The managed system is already powered off.	None.
HSCL01FC	The parameter specified is not valid. Specify a different value.	None.
HSCL01FD	Power on failed. Try again.	Retry the Power On task. If the problem persists, call for HMC software support.
HSCL01FE	The managed system is already powered on.	None.
HSCL01FF	Could not rebuild. Shut down and restart the Hardware Management Console.	1. Before rebooting, try the task again. 2. Reboot the HMC. 3. Refer to “Managed System States for the HMC” on page 259 and check the state of the managed system. Perform the appropriate actions to recover. 4. Try the task again. 5. Call for HMC software support.

Managed System Error Codes	Message	Recovery Action
HSCL0200	Unable to communicate with Service Processor. Check serial cable connection.	1. Check the serial cable connection from the HMC to the managed system. 2. Refer to “Managed System States for the HMC” on page 259 and check the state of the managed system. Perform the appropriate actions to put the managed system in the correct state. 3. Call for HMC software support.
HSCL0201	Service Processor Command failed after {0} attempts: Invalid Response.	Wait several minutes and try the task again.
HSCL0202	Service Processor Socket is corrupted.	1. Wait two minutes and retry the command 2. If the command still fails, wait an additional two minutes and try again. 3. If both tries fail, rebuild the managed system to re-establish the socket connection. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 4. Call for HMC software support.
HSCL0203	Command sent to Service Processor failed. Error Response {0}	1. Try the task again. 2. Refer to “Managed System States for the HMC” on page 259 and check the state of the managed system. Perform the appropriate actions to put the managed system in the correct state. 3. Call for HMC software support.
HSCL0204	Command failed. Unknown error.	1. Try the task again. 2. Refer to “Managed System States for the HMC” on page 259 and check the state of the managed system. Perform the appropriate actions to put the managed system in the correct state. 3. Call for HMC software support.
HSCL0205	The Managed System is in the Error State and is unable to continue with the Recover Partition Data Task.	The recovery partition data task cannot be run until the managed system is no longer in error state. 1. Record the error message. 2. Refer to the recovery procedures for the managed system.
HSCL0206	Failed to Power On the managed system in Partition Standby mode. Unable to continue with the Recover Partition Data task.	1. Check the operator panel value of the managed system to verify it is in the no power state and that the managed system is not in the error state. 2. Verify that no other task is being performed while executing this task, then retry the task. 3. If problem persists, call HMC software support.

Managed System Error Codes	Message	Recovery Action
HSCL0207	Failed to Power Off the Managed System. Unable to continue with the Recover Partition Data Task.	1. Check the operator panel value of the managed system to verify it is powered on and that the managed system is not in the error state. 2. Verify that no other task is being performed while executing this task, then retry the task 3. If problem persists, call HMC software support.
HSCL0208	Failed to Power On the Managed System. Unable to continue with the Power On Task	1. Check the operator panel value of the managed system to verify it is in the no power state and that the managed system is not in the error state. 2. Verify that no other task is being performed while executing this task, then retry the task. 3. If problem persists, call HMC software support.
HSCL0209	Remote virtual terminal sessions are not allowed. Please check the remote virtual terminal settings.	Virtual terminal cannot open remotely at this point. If open virtual terminal remotely is needed, enable your remote virtual terminal setting. Use the **Enable/Disable Remote Virtual Terminal** task in the System Configuration menu to enable remote connections.
HSCL020A	The power on system profile operation timed out. Activate the system profile manually once the managed system is powered on.	Activate the system profile manually after the managed system is powered on.
HSCL020B	The CUoD activation code you entered is incorrect. Please check the activation code and retry.	Make sure the key is correct, and enter it again. If it still fails, contact your service representative.
HSCL020C	The managed system does not allow Activation Codes for CUoD operations.	None
HSCL020D	The command you issued contained incorrect data.	Internal use only. Contact your next level of software support.
HSCL020E	The sequence number of this activation code indicates it has been used before. Please enter in a newer activation code.	Make sure the key is correct, and enter it again. If it still fails, contact your service representative.
HSCL020F	The activation code was not entered correctly. Re-enter your activation code.	Make sure the key is correct, and enter it again. If it still fails, contact your service representative.
HSCL0210	The managed system cannot currently process an activation code. This condition is temporary, please retry this operation.	The system is processing another CUoD function. Retry the operation.
HSCL0211	The requested function is currently disabled.	Power off the managed system, and power it back up.

Managed System Error Codes	Message	Recovery Action
HSCL0212	The managed system is not CUoD capable at the present time.	Make sure that the managed system is powered on. If it is powered on, check the managed system's properties panel to verify that the system is not CUoD capable. Contact your local representative for more information about this feature.
HSCL0213	The managed system does not support CUoD upgrades for processors.	Contact your local representative for more information about this feature.
HSCL0214	The managed system does not support CUoD upgrades for memory.	Contact your local representative for more information about this feature.
HSCL0215	There was an error trying to save processor order information to a diskette. Verify the diskette is writable, and retry the operation. If the error persists, contact your service representative.	Verify the diskette is writable, and retry the operation again. If the error persists, contact your service representative.
HSCL0216	There was an error trying to send processor order information to the remote system. Verify the network connection to the remote system and that the user has access to the remote system and directory where the file will be copied. If the problem persists, contact your software support representative.	Verify the network connection to the remote system and that user has access to the remote system and directory where the file will be copied. If the problem persists, contact your software support representative.
HSCL0216	The managed system cannot process the CUoD task at this time. The function has been disabled. You must power off and then power on the managed system to enable this task.	To enable the CUoD task, power off and then power on the managed system.
HSCL021F	The number of processors to activate immediate is greater than the number currently allowed.	Choose a number of processors that is fewer than the number allowed. Retry the operation.
HSCL0220	The Managed System cannot proceed with the CUoD Activate operation since another CUoD activation operation is being performed. Please make sure no other CUoD operation is taking place and then retry this operation	Ensure that no other CUoD operation is taking place and then retry this operation.
HSCL0221	The amount of memory to activate immediate is greater than the number currently allowed.	Choose an amount of memory that is less than the number allowed. Retry the operation.
HSCL3302	Partition {0} cannot be activated with SNI adapter {1} because {2} windows were requested, and only {3} windows are available on adapter {1}. Please remove this SNI adapter from your profile configuration, and retry the operation.	Remove this SNI adapter from your profile configuration and retry the operation.
HSCL305D	An error occurred while setting the frame number through the frame interface. Retry the operation.	Retry the operation.
HSCL305E	Unable to set the frame number for the following : {0}	Retry the operation. If the problem persists, make sure the serial connection to the frame is configured properly and then retry the operation again.

Managed System Error Codes	Message	Recovery Action
HSCL3303	The partition cannot be activated because the SMA adapter pair {0} was bad.	Retry the operation. If the problem persists, call for hardware support.
HSCL3304	Adapters should be sent down in pairs.	Retry the operation, sending down two adapters (or an even number of adapters). If the problem persists, call for HMC software support.
HSCL3305	The partition cannot be activated because because the SMA adapter pair {0} is not installed or has been removed.	Retry the operation with other installed SMA adapters. If there are no other adapters to select, delete the profile and recreate it. If this SMA adapter pair is installed, call for hardware support.

Managed System Resource Error Codes	Message	Recovery Action
HSCL03EA	There is an insufficient number of processors: Obtained - {0}, Required - {1}. Check that there are enough processors available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with the specified number of processors, deactivate any active partitions using the resource, then activate the partition.	1. Check the managed system properties panel to make sure that enough processors are available to activate the partition. 2. If there are not enough processors available, create a new profile or modify the existing profile with the available resources. Then, activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition that is using the resource and then activate the partition. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Managed System Resource Error Codes	Message	Recovery Action
HSCL03EB	Unable to allocate the I/O slot for activation in {0}. Check that the specified I/O is available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with these resources, deactivate any running partition(s) using the resource then activate this partition.	1. Check the managed system properties panel to make sure that enough I/O slots are available to activate the partition. 2. If there are not enough I/O slots available, then create a new profile or modify the existing profile with the available resources. Then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition that is using the resource and then activate the partition. **Note:** If you have tried to recover using the above actions and you are not successful, and you must activate the partition, edit the profile for the partition you are activating and remove all slots that are associated with the identified slot's PHB. See the *PCI Adapter Placement Reference*, order number SA38-0538 for information on PHB slot associations. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL03EC	There is not enough memory: Obtained - {0}, Required - {1}. Check that there is enough memory available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with these resources, deactivate any running partition(s) using the resource then activate this partition.	1. Check the managed system properties panel to make sure that enough memory is available to activate the partition. 2. If there is not enough available memory, create a new profile or modify the existing profile with the available resources and then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition using the resource and activate the partition. If the problem persists, call for HMC software support.
HSCL03ED	The I/O Drawer specified by this ID cannot be found and may have been deleted from the managed system. Modify the profile.	The I/O drawer defined in the profile may have been removed from the server. Check to verify that the I/O drawers defined in the profile are installed. Then, modify the profile to match the server configuration. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL03EE	The specified slot number cannot be found. Make sure the profile is not using I/O drawer slots that do not exist in the managed system.	An I/O slot defined in the profile may have been removed from the server. Verify that the I/O slots defined in the profile are installed. Then, modify the profile to match the server configuration. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Managed System Resource Error Codes	Message	Recovery Action
HSCL03EF	The number of drawers, slots, and I/O required/desired information stored in the properties do not match. The profile may be corrupted. Perform the Restore Profile Data task.	1. The profile may be corrupted. Perform the Restore Profile Data task. 2. If problem persists, delete the profile and create a new profile. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL03F0	Unable to allocate the I/O slot for activation in I/O drawer {0}. Slot {1} is currently being used by another partition. Perform one of the following three actions 1) remove this I/O slot from the profile or 2) change the I/O slot from Required to Desired in the profile or 3) remove the I/O slot from the other partition.	Perform one of the following actions: • Remove this I/O slot from the profile. • Change the I/O slot from Required to Desired in the profile. • Remove the I/O slot from the other partition.
HSCL03F1	Unable to allocate one or more I/O slots. The following slots are in error state: {0} slot {1}. Please complete one of the following actions: Remove this I/O slot from the profile, or change the I/O slot from required to desired in the profile, or reboot the managed system to restore the PCI slots in error to normal state.	Perform one of the following options: • Remove this I/O slot from the profile. • Change the I/O slot from required to desired in the profile. • Reboot the managed system to restore the PCI slots in error to normal state. • If the problem persists, call HMC software support.
HSCL03F2	Unable to allocate the I/O slot for activation in I/O drawer {0}. Slot {1} is not present. Remove this I/O slot from the profile or change the I/O slot from Required to Desired in the profile.	Remove this I/O slot from the profile or change the I/O slot from Required to Desired in the profile.
HSCL03F3	Unable to allocate the I/O slot for activation in I/O drawer {0}. Slot {1} is system deconfigured. Remove this I/O slot from the profile or change the I/O slot from Required to Desired in the profile.	Remove this I/O slot from the profile or change the I/O slot from Required to Desired in the profile.

Partition Error Codes	Message	Recovery Action
HSCL0591	Cannot activate logical partition when an affinity logical partition has already been activated since powering on	Activation of logical partitions is not allowed at this point. To activate this partition, do the following: 1. Power off the managed system. 2. Power on the managed system to partition standby. 3. Try the activation operation again.
HSCL0592	Cannot activate a 8-processor affinity logical partition when a logical partition or other type of affinity logical partition has already been activated since powering on	Activation of an 8-way affinity logical partition is not allowed at this point. To activate this partition, do the following: 1. Power off the managed system. 2. Power on the managed system to partition standby. 3. Try the activation operation again.

Partition Error Codes	Message	Recovery Action
HSCL0593	Cannot activate a 4-processor affinity logical partition when a logical partition or other type of affinity logical partition has already been activated since powering on	Activation of a 4-way affinity logical partition is not allowed at this point. If you need to activate this partition, do the following 1. Power off the managed system. 2. Power on the managed system to partition standby. 3. Retry the activation operation.
HSCL0594	Managed system is not capable of activating a 4-processor affinity logical partition	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL0595	Managed system is not capable of activating a 8-processor affinity logical partition	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL0596	Cannot activate a Full Machine Partition in a non-SMP capable managed system	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL0597	Cannot activate a logical partition in a non-LPAR capable managed system	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL0598	Cannot activate an affinity logical partition in a non-Affinity-LPAR capable managed system	The capabilities of your managed system are listed on the Machine tab of the property panel.
HSCL059A	Cannot activate the partition. The profile's maximum memory amount exceeds the managed system's memory limit. Please change the profile's maximum memory amount.	Change the profile's maximum memory amount, and retry the operation.
HSCL05DD	Unable to get partition state. Repeat the operation.	Repeat the operation. If the problem persists, call for HMC software support.
HSCL05DE	A partition in the managed system already uses the name {0}. Provide another name for this partition.	Rename the partition to another name that is not yet used by other partitions in the same managed system. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05DF	The partition is not in a state under which this operation can be performed. Check the state of the partition.	Verify that the operation is allowable under this partition state. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05E0	The partition {0} is in an undefined state. Rebuild the managed system.	Perform a Rebuild Managed System operation. Follow the procedures in "Rebuild is Indicated for Managed System" on page 257 to perform this action.
HSCL05E1	Only 16 partitions per managed system can be allocated. There are no more unallocated partitions available. Delete unused or unwanted partitions for this managed system and retry the operation. Partitions in the ready state are currently not in use.	Delete unused or unwanted partitions. Partitions in the ready state are currently not in use. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05E4	Unable to delete a full system partition. You do not have the necessary permission to delete a full system partition.	You do not have the necessary permission to delete a full system partition. Contact your user administrator to give you proper access.

Partition Error Codes	Message	Recovery Action
HSCL05E5	Unable to create partition when the managed system is in {0} state. Make sure that the managed system is in the ready state and was powered on with Partition Standby.	Verify the managed system is in the ready state and in Partition Standby. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05E6	Partition {0} delete failed. Cannot delete a partition when its state is in {1}. If the partition is not in the ready error state, perform a hard reset operation then delete the partition.	Verify the partition is not in running or booting state. If the state is ready or error state, perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again.
HSCL05E7	The profile you tried to activate does not belong to the partition {0} you specified. Select the correct LPAR profile.	Verify that you selected the correct LPAR profile to activate.
HSCL05E8	Cannot delete partition {0}. A partition cannot be deleted when the managed system is at the {1} state. Delete the LPAR when the managed system is in the Ready state and in Partition Standby.	If the managed system is in the Ready state and Partition Standby, rebuild the managed system. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, and then try the task again. Also refer to partition error message HSCL05H6.
HSCL05E9	Could not activate the partition. Make sure that the partition is not already activated and that the managed system is running.	Verify that the partition is not already activated, and the state and power-on condition of the managed system are correct, try the operation again. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05EA	Cannot activate the partition when it is in state {0}. Make sure the partition is not running, booting or in the open firmware state.	Verify the LPAR is not in the running, booting, or open firmware state. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05EB	Could not create partition. Make sure that all requirements are met for creating a logical partition.	Cannot create a partition. To verify that all the requirements for creating a logical partition are met, refer to “Creating Partitions” on page 93. If all requirements are met, do a rebuild of the managed system, follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, and try the task again. If the failure still occurs, call for HMC software support.
HSCL05EC	Could not delete partition {0}. Make sure that all requirements are met for deleting a logical partition.	Cannot delete a partition. Verify that all the requirements for deleting a partition are met, refer to “Deleting Partitions” on page 108. If all requirements are met, rebuild of the managed system Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, and try the task again. If it still fails, call for HMC software support.
HSCL05ED	Could not set the properties for partition {0}. Try again	Repeat the operation. If the operation still fails, call for HMC software support. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Partition Error Codes	Message	Recovery Action
HSCL05EE	Could not get the managed system's service processor log entry. Try again	Repeat the operation. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05EF	This new partition does not have a user defined name. Specify a name for the partition.	Set the user defined name for this partition. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05F0	Cannot create the partition when the managed system was powered on with {0}. Make sure the managed system is powered on with Partition Standby.	Verify that the managed system is in Partition Standby. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05F1	Could not delete partition {0}. A partition cannot be deleted when the managed system was power on with {1}. Make sure that the managed system was powered on with Partition Standby.	Verify that the managed system is in running in Partition Standby. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL05F2	No port or session number information for opening a virtual terminal partition on {0} with id {1}. Try again.	1. Wait for two minutes and then try the task again. 2. If the problem persists, refer to "Managed System States for the HMC" on page 259 to check the state of the managed system. Perform the appropriate actions to recover. 3. If the operation still fails, call for HMC software support.
HSCL05F3	Could not display the OS reset dialog for partition {0}. Try again.	1. Log off and then log back on to the HMC and try the operation again. 2. If this does not correct the problem, call for HMC software support.
HSCL05F4	Could not display the partition activate dialog for partition {0}. Try again.	1. Log off and then log back on to the HMC and try the operation again. 2. If this does not correct the problem, call for HMC software support.
HSCL05F5	Could not display the create partition dialog for the managed system: {0}. Try again.	1. Log off and then log back on to the HMC and try the operation again. 2. If this does not correct the problem, call for HMC software support.
HSCL05F6	Could not create the partition on the managed system {0} with partition name {1}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	Verify the newly created partition displays on the graphical user interface. If not, retry the create partition task and check the graphical user interface again. If the task still fails, log off and log back on to the HMC, and try the task again.
HSCL05F7	Could not open the virtual terminal for partition {0} with ID {1}.	1. Refresh the interface and check whether the operation was performed. 2. Reboot the HMC, and try the task again. 3. If the operation still fails, call for HMC software support.

Partition Error Codes	Message	Recovery Action
HSCL05F8	Could not perform the OS reset {0} reset on partition {1} with ID {2}.	1. Refresh the interface and check whether the operation was performed. If not, try the operation again. 2. If the partition has been reset. (If you performed a soft reset, check to see if the partition rebooted. If you performed a hard reset, verify that the partition state changed to ready.) 3. Retry the OS reset operation. 4. If a hard reset was performed, rebuild the managed system see “Rebuild is Indicated for Managed System” on page 257 and check the state, see“Managed System States for the HMC” on page 259.
HSCL05F9	Could not delete partition {0}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	1. Verify that the partition displays on the graphical user interface. 2. Retry the delete partition and check the graphical user interface to see if it is updated appropriately. 3. Log off and log back on to the HMC. 4. Call for HMC software support.
HSCL058A	Could not activate the partition on partition {0} with ID {1}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	1. Refresh the graphical user interface. 2. Perform a rebuild of the managed system, following the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action 3. Try the task again. 4. Call for HMC software support.
HSCL058B	Could not read the boot error value task on partition {0} with ID {1}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	1. Try the task again. 2. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Profile Error Codes	Message	Recovery Action
HSCL07D1	This partition profile is currently active in its logical partition and cannot be modified or deleted. To make the profile inactive, perform a hard operating system reset on the partition to bring it to the Ready state, then repeat the operation.	Partition Profiles that are active in a Logical Partition cannot be modified or deleted. Perform a Hard Operating System Reset on the Partition to bring it to the Ready state, at which time the profile will no longer be active. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Profile Error Codes	Message	Recovery Action
HSCL07D2	This partition profile is the logical partition's default profile and cannot be deleted. If you still want to delete it, change the default profile for this logical partition or, if necessary, create another partition profile to be the default profile.	All Logical Partitions must have at least one Partition Profile, which is designated as the Default Profile because it is the Profile implicitly used when the Partition is activated with no Profile specified. If you still wish to delete it, change the Default Profile for this Logical Partition (create another Partition Profile if necessary). Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07D3	The partition profile could not be found in the Hardware Management Console save area. The Hardware Management Console is either out of sync with the console save area or the console save area has been corrupted. Rebuild this partition profile's managed system.	The main causes of this condition are: 1. The HMC is out of sync with the profile data. 2. The profile data has been corrupted. This might cause the loss of the Partition Profile. 3. Rebuild the Partition Profiles for the managed system. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07D4	A profile named {0} already exists for this partition in the Hardware Management Console save area. Choose a different name for the new system profile.	All Partition Profiles for a logical partition must have unique names. Choose a different name for the new profile. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07D5	Creation of partition profiles for the full system partition is not allowed. You must use one of the predefined partition profiles for the full system partition.	You must use one of the predefined partition profiles for the Full System Partition. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07D6	You cannot delete full system partition profiles.	Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07D7	You cannot modify the full system partition profile's properties.	None
HSCL07D8	Deleting default profile associations within the current context is not allowed.	You can delete the Default partition Profile Association only by: 1. Deleting the Partition CIMInstance to which the Association connects. This will also delete the Partition Profile CIMInstance to which the Association connects the Partition. 2. Use createInstance to change the DefaultLparProfile Association to overwrite the previous Association you intended to delete. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Profile Error Codes	Message	Recovery Action
HSCL07D9	Setting a default profile association is only allowed during create.	You can alter the DefaultLparProfile Association only through createInstance, which overwrites the previous association. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07DA	The partition profile used for the operation cannot be found in the profile data.	Verify that you enter the correct information. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL07DB	An attempt to create a profile failed.	Try the task again.
HSCL07DC	An attempt to modify a profile failed.	Try the task again.

System Profile Error Codes	Message	Recovery Action
HSCL09C6	Could not find the system profile in memory. It may be corrupted. Restore the profile data.	The System Profile may be corrupted. 1. Perform the Restore Profile Data task. 2. If problem persists, delete and re-create a new system profile. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL09C7	A system profile named {0} already exists for this managed system in the Hardware Management Console save area. Choose a different name for the new system profile.	Every system profile created for an individual managed system must have a unique name. Choose a different name for the new System Profile. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL09C8	Could not open the Copy System Profile dialog. Try again.	1. Try the task again. 2. Log off the HMC, and log back on. 3. Try the task again. 4. If the problem persists, call your HMC software support.
HSCL09C9	Could not copy the system profile {0}. Try again.	1. Try the task again. 2. Log off the HMC, and log back on. 3. Try the task again. 4. If the problem persists, call for HMC software support.
HSCL09CA	Could not delete the system profile. Try again.	1. Try the task again. 2. Log off the HMC, and log back on. 3. Try the task again. 4. If the problem persists, call for HMC software support.

System Profile Error Codes	Message	Recovery Action
HSCL09CC	Cannot activate a Full System Partition profile when the managed system is powered on with Partition Standby.	Check the status of the Managed System from the properties panel and verify that the system was powered on as Full System Partition. If not in Full System Partition, switch the managed system from Partition Standby to Full System Partition. To switch these power-on options, turn off the power for the managed system. Then, turn on the power on and select Full System Partition during the power-on process.
HSCL09CD	Cannot activate user defined partition profiles when the managed system is powered on with Full System Partition.	Check the status of the Managed System from the properties panel and verify that the system was powered-on as Partition Standby. If not in Partition Standby, switch the managed system from Full System partition to Partition Standby. To switch these power-on options, turn off the power to the managed system. Then, turn on the power and select Partition Standby during the power-on process.
HSCL09CE	You cannot have LPAR and affinity LPAR profiles in the same System Profile.	Ensure the System Profile contains only profiles that belong to the same partition type. To determine the partition type, select the logical partition and view its properties.
HSCL09CF	Validation of system profile failed. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL09D0	Cannot validate system profile if the managed system is not in ready state.	Retry the operation with the managed system in the Ready state.
HSCL09D1	Cannot validate system when the managed system is powered-on with the Full System Partition	None

Operating System Reset Error Codes	Message	Recovery Action
HSCL0DAE	The Hardware Management Console was unable to successfully issue an Operating System Reset request to the managed system or Logical Partition	1. Try the task again. 2. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL0DAF	A Hard Operating System Reset can be issued only on a logical partition, not on the managed system.	None

Operating System Reset Error Codes	Message	Recovery Action
HSCL0DB0	A Soft Operating System Reset can be issued for the managed system when it is in the Ready state only if it was powered on in Full System Partition.	If the managed system was not powered on in Full System Partition, turn off the power to the managed system, and then turn on the power in Full System Partition. If the managed system is in the No-Power state, perform just the power-on operation. The managed system should transition to the Initializing state, then to the Ready state. If the managed system is in the Error state, or No-Communication state, refer to "Managed System States for the HMC" on page 259 and check the state of the managed system. Perform the appropriate actions to recover.
HSCL0DB1	A Soft Operating System Reset can be issued for the managed system only if it is in the Initializing or Ready state.	If the managed system is in the No-Power state, apply power to the system. The managed system should transition to the Initializing state then to the Ready state. If the managed system is in an Error state or No-Communication state, refer to "Managed System States for the HMC" on page 259 and check the state of the managed system. Perform the appropriate actions to recover.
HSCL0DB2	An Operating System Reset can be issued for a logical partition only if the partition is in the Running or Starting state.	1. Refresh the graphical user interface. 2. Try the task again. 3. Perform a Rebuild Managed System operation. Follow the procedures in "Rebuild is Indicated for Managed System" on page 257 to perform this action, then try the task again. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Virtual Terminal Error Codes	Message	Recovery Action
HSCL0FA1	The managed system's service processor could not open a virtual terminal session.	1. Verify that the managed system is connected and has power. 2. Try the task again. 3. Perform a Rebuild Managed System operation. Follow the procedures in "Rebuild is Indicated for Managed System" on page 257 to perform this action, then try the task again. 4. If the problem persists, call for HMC software support.

Virtual Terminal Error Codes	Message	Recovery Action
HSCL0FA2	All available virtual terminal sessions have been opened and are in use. To force a new open session, perform a Close Terminal Session operation which frees up the session.	No Virtual Terminal Sessions are available. Perform a Close Terminal Session to forcefully close an open session and free it up to be opened. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL0FA3	Unable to close the virtual terminal session. Issue a Close Virtual Terminal Connection operation.	An internal error occurred while attempting to close the Virtual Terminal Session. Issue a Close Virtual Connection; if this fails, call for HMC software support.
HSCL0FA4	There is no virtual terminal session with session number {0} open.	None

Backup and Restore Error Codes	Message	Recovery Action
HSCL1195	Unable to back up the profile data to the backup file. Try again.	1. Try the task again. 2. Reboot the HMC, and then try the task again. 3. Try the task with new media. 4. If the operation still fails, call for HMC software support.
HSCL1196	You do not have read access permission on the backup file, {0}. Try the operation again.	1. Try the task again. 2. If the operation still fails, call for HMC software support.
HSCL1197	Unable to read the profile data's backup file, {0}. Try the operation again.	1. Try the task again. 2. Reboot the HMC, and then try the task again. 3. If the operation still fails, call for HMC software support.
HSCL1198	Cannot find backup file, {0}, for profile data. Select a valid, existing backup file.	1. Try the task again. 2. If the operation still fails, call for HMC software support.
HSCL1199	A full restore is not permitted when there are logical partitions in the {0} state. A full restore can only be issued when the managed system was powered on with Partition Standby and there are no partitions running, booting, or in the open firmware state.	1. Verify the managed system was powered-on to run in Partition Standby. 2. Try the task again. 3. If the operation still fails, call for HMC software support.
HSCL119A	There was an I/O error while backing up the profile data. Try again.	1. Try the task again. 2. Reboot the HMC, and then try the task again. 3. If the operation still fails, call for HMC software support.
HSCL119B	The restore profile data operation failed. Try again.	1. Try the task again. 2. Reboot thehardware management console, and then try the task again. 3. If the operation still fails, call for HMC software support.

Backup and Restore Error Codes	Message	Recovery Action
HSCL119C	Cannot initialize profile data when a partition is in the {0} state and when the managed system is not powered on with Partition Standby, or when there are partitions running, booting, or in the open firmware state.	Cannot initialize the profile data when managed system is not running logical partitions and in the ready state. Also , there should be no partition in running, booting, or open firmware state. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL119D	Cannot restore the profile data if the managed system is in the {0} state.	1. Verify the managed system is in ready state and running logical partitions or Partition Standby. 2. Try the task again.
HSCL119E	Cannot initialize the profile data if the managed system is in the {0} state.	1. Verify the managed system is in ready state and running logical partitions or partition standby. 2. Try the task again.
HSCL119F	The backup file {0} used to restore the profile data is not valid. Its file size ({1}) is not correct. Select a valid backup file.	The backup file selected is not valid. The File may be corrupted. 1. Try the task again. 2. Select another backup file and try the task again. 3. If the problem persists, call for HMC software support
HSCL11A0	Cannot restore the profile data if the managed system is in the {0} state. The managed system must be in the Ready state and powered on with Partition Standby.	1. Verify the managed system is in ready state and running logical partitions or Partition Standby. 2. Try the task again.
HSCL11A1	Cannot initialize the profile data if the managed system is in the {0} state. The managed system must be in the Ready state and powered on with Partition Standby.	1. Verify the managed system is in ready state and running logical partitions or partition standby. 2. Try the task again.
HSCL11A2	Could not display the backup dialog for the managed system: {0}. Try again.	1. Try the task again. 2. Log off the HMC, then log back on. 3. Try the task again. 4. Call your software support.
HSCL11A3	Could not back up the profile data for the managed system: {0} to file: {1}.	1. Refresh the graphical user interface. 2. Try the task again. 3. Reboot the HMC, then try the task again. 4. If the problem persists, call for HMC software support.
HSCL11A4	Cannot back up profile data to the default backup file name: {0}.	Cannot back up the profile data to the default backup file. Choose a different backup file name. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Backup and Restore Error Codes	Message	Recovery Action
HSCL11A5	Could not display the remove backup dialog for the managed system: {0}. Try again.	1. Try the task again. 2. Log off the HMC, and log back on. 3. Try the task again. 4. Call for HMC software support.
HSCL11A6	Could not remove the backup file {0} from the managed system {1}.	1. Refresh the graphical user interface. 2. Try the task again. 3. Reboot the HMC, then try the task again. 4. If the problem persists, call for HMC software support.
HSCL11A7	No backup file has been selected for the operation. Select a backup file.	Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL11A8	Could not display the restore profile data dialog for the managed system: {0}. Try again.	1. Try the task again. 2. Log off the HMC, then log back on. 3. Try the task again. 4. If the problem persists, call for HMC software support.
HSCL11A9	Could not initialize the profile data task on the managed system {0}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	Refresh the graphical user interface. Check whether the operation has been performed and displays on the graphical user interface. If not, repeat the operation. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL11AA	Could not restore the profile data task on the managed system {0} with backup file {1} of {2} option. Refresh the interface and check whether the operation was performed. If not, try the operation again.	1. Refresh the graphical user interface. 2. Try the task again. 3. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 4. If the problem persists, call for HMC software support.
HSCL11AB	Could not display the recover partition data dialog for the managed system {0}.	1. Try the task again. 2. Log off the HMC, then log back on. 3. Try the task again. 4. If the problem persists, call for HMC software support.

Backup and Restore Error Codes	Message	Recovery Action
HSCL11AC	Could not perform the recover partition data task on the managed system {0}.	1. Refresh the graphical user interface. 2. Try the task again. 3. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 4. If the problem persists, call for HMC software support.
HSCL11AD	Could not display the Rebuild the Managed System dialog for the managed system {0}.	None
HSCL11AE	The backup profile data name must start with a numeric or alphabetic character.	Specify the name correctly.
HSCL11AF	The backup profile data name must not contain / \ ’ or ″ characters.	Specify the name correctly.

Utility Class Error Codes	Message	Recovery Action
HSCL138A	Unable to a get the socket connection to the managed system. Shut down and restart the Hardware Management Console.	Shut down and restart the HMC. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL138C	Unable to find the machine type, model, serial number of this HMC.	Reboot the HMC. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL138D	Could not release the management framework socket.	Reboot the HMC.Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL138F	Unable to get the Hardware Management Console host name. Check the network settings within the system configuration.	Check the network setting under system configuration, then try the task again. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL1390	The managed system is not registered in the management framework. Shut down and restart the Hardware Management Console.	Shut down and restart the HMC. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL1391	The management framework socket is not registered. Make sure to not attempt any operations while the delete, rebuild, or restore profile data tasks are being performed. Perform the Rebuild Managed System task.	1. Make sure not to perform any operation while the Delete, Rebuild and Restore Profile Data tasks are performed. 2. Perform the Rebuild Managed System task. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL1392	The management framework socket is either deleted or changed. Do not perform any operations while the delete, rebuild, or restore profile data tasks are being performed. Perform the Rebuild Managed System task.	Make sure not to perform any operation while the Delete, Rebuild, and Restore Profile Data tasks are performed. Follow the procedures in this guide. If the problem persists, call for HMC software support.

Utility Class Error Codes	Message	Recovery Action
HSCL1393	Unable to load the list of IBM PC product names.	1. Reboot the HMC. 2. If the problem persists, call for HMC software support.
HSCL1395	Unable to launch the confirmation dialog. Try again.	1. Refresh the graphical user interface. 2. Try the task again. 3. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 4. If the problem persists, call for HMC software support.
HSCL1396	Unable to initialize the HMC-CSP Version compatibility table.	Retry the operation. If it fails, contact HMC Software Support.
HSCL1397	Unable to determine what version of firmware is loaded on the service processor.	Try the operation again. If it fails, contact HMC Software Support.
HSCL1398	Unable to determine what versions of service processor firmware is compatible with this version of the Hardware Management Console.	Retry the operation. If the error persists, contact HMC software support.

CIMOM Error Codes	Message	Recovery Action
HSCL157F	Cannot find an instance of the object specified.	1. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 2. If the problem persists, call for HMC software support.
HSCL1584	You do not have the proper authorization or permission to perform this task. Log in as the proper user and try again.	Log in with appropriate permissions to perform the task. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL1585	There was an unknown error while querying the object manager database.	1. Try the task again. 2. Reboot the HMC. 3. If the problem persists, call for HMC software support.
HSCL1586	Cannot find an Instance with object manager of {0}.	1. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 2. If the problem persists, call for HMC software support.

HMC Console Error Codes	Message	Recovery Action
HSCL1771	Unable to create console information and set it with the managed system. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1772	Could not set Hardware Management Console information. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1773	Invocation of the Hardware Management Console information method failed. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1774	Unable to get the defined slot number for Hardware Management Console information slots. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1775	Could not get host Hardware Management Console information slot ID. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1776	Could not get the Hardware Management Console information. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL1777	Failed to construct the Hardware Management Console information string. Perform the Rebuild Managed System operation.	Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action.
HSCL177F	Could not delete the Hardware Management Console instance.	1. Perform a Rebuild Managed System operation. Follow the procedures in “Rebuild is Indicated for Managed System” on page 257 to perform this action, then try the task again. 2. Reboot the HMC and then try the task again. 3. If the problem persists, call for HMC software support.

WEBSM/AUIML Error Codes	Message	Recovery Action
HSCL1965	Unable to determine the Hardware Management Console server’s host name. Check the Hardware Management Console network settings under System Configuration and verify that they are correct.	Check the HMC Network Settings under System Configuration and verify the settings are correct, and that you have a valid host name for the HMC. Contact your System/Network Administrator for network settings help. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL1966	You must select one profile for powering on the Full System Partition or select Cancel.	Select a profile from the Power-on panel or select Cancel to close the panel.
HSCL1967	You must select one system profile to power on with or select Cancel.	Select a system profile from the panel or select Cancel to close the panel.

WEBSM/AUIML Error Codes	Message	Recovery Action
HSCL1968	You must select a power on option or select Cancel.	Select either Full System Partition or Partition Standby to turn on the power or select Cancel to close the panel.
HSCL1969	Could not retrieve information from the GUI server. Check your network configuration and connection.	Check the HMC network settings under System Configuration and verify the settings are correct. Follow the procedures in this guide. If the problem persists, contact the HMC support organization.
HSCL196A	Choose a new default profile from the list or select Cancel.	None
HSCL196B	The object is not found in the data area. Please refresh the interface.	1. Perform the refresh task. 2. If the problem persists, call for HMC software support.
HSCL196C	Problem obtaining object information. Please refresh the interface	1. Perform the refresh task. 2. If the same error occurs, perform the rebuild managed system operation. 3. If the problem persists, call for HMC software support.

User Management Error Codes	Message	Recovery Action
HSCL2329	The following characters cannot be used in the login name: space , : ( ) [ ] ” | & ; $ \ DOUBLE QUOTE.	Specify a login name using valid characters. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL232A	The user name already exists or may be a user name reserved by the Hardware Management Console. Choose another user name.	User names must be unique. Choose a different user name. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL232B	The user login name cannot be longer than 32 characters. Choose another login name with less than 32 characters.	Choose a new login name that uses less than 32 characters. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL232C	The user must have a role. Select a role from the list.	User must have a role assigned. Choose a role from the menu list. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL232D	Could not modify user’s property.	1. Try the task again. 2. If the problem persists, call for HMC software support.
HSCL232E	Could not create user.	Check to see the create command in debug print. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL232F	The Hardware Management Console user cannot be deleted.	None
HSCL2330	The new password and confirmation password do not match. Try again.	New password and confirmation password must match. Enter the new password again.

User Management Error Codes	Message	Recovery Action
HSCL2331	Change user password failed.	1. Try the task again. 2. If the problem persists, call for HMC software support.
HSCL2332	The Hardware Management Console user properties cannot be changed.	Cannot change the HMC special user properties. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL2333	Multiple roles are not allowed. Select only one role from the role list.	Select only one role from the role list. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL2334	Cannot create or modify the user due to the following reasons: 1. May not be able to locate the file 'rmcadduser' in /opt/hsc/bin directory. 2. May not be able to locate the file ''ctrmc.acls'' file in /var/ct/cfg directory. 3. Service Focal Point functionality may not be installed.	If the problem persists, call for HMC software support.
HSCL2336	The user name is not valid. The user name should not start with 0 1 2 3 4 5 6 7 8 9 ! @ # $ % ^ & * - + = / | { } [ ] : ; '' , < > . ? ~ ` _ \ DOUBLE QUOTE.	Specify a user name that contains valid characters. Follow the procedures in this guide. If the problem persists, call for HMC software support.
HSCL2337	Cannot delete the user due to the following reasons: 1. May not be able to locate the file 'rmcremoveuser' in /opt/hsc/bin directory. 2. May not be able to locate the file 'ctrmc.acls' in /var/ct/cfg directory. 3. Service Focal Point functionality may not be installed.	If the problem persists, call for HMC software support.
HSCL2338	User name is required.	Specify a user name and try the task again. If the problem persists, call for HMC software support.
HSCL2339	Password cannot be empty.	Specify a non-empty password and try the task again. If the problem persists, call for HMC software support.
HSCL233A	Could not find the file /usr/bin/expect.	Try the task again. If the problem persists, call for HMC software support.
HSCL233B	The old password specified for the user was incorrect.	Enter the old password correctly and try the task again. If the problem persists, call for HMC software support.
HSCL251E	Failed to set the 'enable remote virtual terminal' option	1. Retry the operation again. 2. If the problem persists, call for HMC software support.
HSCL251F	The following error was encountered: `\n{0}\n`. Retry the operation.	1. Wait 5-7 minutes. 2. Retry the operation again. 3. Reboot the HMC. 4. If the problem persists, call for HMC software support.

User Management Error Codes	Message	Recovery Action
HSCL2726	An affinity LPAR configuration already exists. You must remove this configuration before setting up a new affinity LPAR configuration.	1. Verify that affinity LPARs display on the graphical user interface. If no affinity LPARs can be seen, refresh the console. If the affinity LPARs do not display, rebuild the managed system. 2. Make sure that no affinity logical partitions are in the Running or Initializing state. 3. Remove the existing affinity LPAR configuration. 4. Retry the operation. 5. If problem persists, contact HMC software support.
HSCL2727	The operation failed. It is possible that another user is in the process of creating or updating affinity logical partitions. If this is not the case, restore profile data and retry the operation.	1. Make sure that another user is not in the process of creating or updating affinity LPARs. 2. If another user is not creating affinity LPARs, restore the profile data. Choose the Managed System Priority option, and restore from the file labeled **backupFile**. 3. Retry the operation.
HSCL2728	Your partition names are not all unique. No partitions have been created. Make sure that all partition names are different from each other and those of already created partitions.	Try setting up an affinity LPAR configuration again, using unique names for every partition, both LPAR and affinity LPAR.
HSCL2729	Affinity LPAR creation failed. Retry the operation.	1. Ensure affinity partitions do not already exist. 2. Retry the operation.
HSCL272A	An error occurred in partition creation. Default profiles and the system profile may have to be created manually. First, rebuild the managed system, and then create items if needed.	1. Rebuild the managed system. 2. You may have to manually create missing items (default profiles, system profile).
HSCL272B	An error occurred in default profile creation. Default profiles and the system profile will have to be created manually. First rebuild the managed system, and then create the needed items.	1. Rebuild the managed system. 2. Create the missing affinity LPAR default profiles manually. Create a system profile that includes each affinity partition's default profile.
HSCL272D	An error occurred in default profile creation. The system profile will have to be created manually. First rebuild the managed system, and then create the missing system profile.	1. Rebuild the managed system. 2. Create a system profile that includes each affinity partition's default profile.
HSCL272E	An unknown error occurred during partition creation.	1. Retry the operation 2. If the problem persists, contact HMC software support.
HSCL272F	An error occurred in partition creation. Affinity partitions have been created, but default profiles and the system profile may have to be created manually. First, recover partition data, and then create items if needed.	1. Recover partition data - choose the Restore option. 2. Manually create any missing affinity LPAR items

User Management Error Codes	Message	Recovery Action
HSCL2730	Unable to get the resources of the partition since it is not an affinity logical partition	1. Retry the task. 2. Rebuild the managed system.
HSCL2731	The addition of affinity logical partitions exceeds the maximum limit. Delete other partitions and retry the task.	Delete enough logical partitions and then retry the task.
HSCL2734	Cannot create only one affinity logical partition.	The user must create as many affinity LPAR partitions as resources will allow at the same time. To create an affinity LPAR configuration, use the **Affinity Partition** option.
HSCL2735	Cannot delete only one affinity logical partition.	The user must delete all affinity LPAR partitions at the same time. To delete an affinity LPAR configuration, use the **Affinity Partition** option.
HSCL2736	The update operation cannot be performed since there are no affinity logical partitions	1. Refresh the interface and check if affinity logical partitions exist. If so, retry the operation. 2. If the problem persists, call HMC software support.
HSCL2737	The operation failed since the update parameter is invalid.	1. Retry the task. 2. If the problem persists, call HMC software support.
HSCL2738	The operation failed since the cluster size parameter is invalid.	1. Retry the task. 2. If the problem persists, call HMC software support.
HSCL2739	The update operation failed since the hardware resources have not changed.	1. If the hardware resources (processor and memory) have changed, retry the task. 2. If the problem persists, call the HMC software support.
HSCL273A	The managed system is not affinity LPAR capable.	None. If you are certain that the managed system is or should be affinity LPAR-capable, contact software support.
HSCL273B	The managed system cannot handle the creation of partitions with the specified cluster size.	None. If you are certain that the managed system supports partitions of the specified cluster size, contact software support.
HSCL273C	Affinity LPAR deletion failed. Rebuild the managed system and retry the operation.	1. Rebuild the managed system. 2. Retry the operation. 3. If problem persists, contact software support.
HSCL273D	Deletion of affinity logical partitions failed. Recover partition data and retry the operation.	1. Recover partition data - choose the Restore option. 2. Retry the operation. 3. If problem persists, contact HMC software support.
HSCL273E	Deletion of partition {0} failed. The partition cannot be deleted in the Running or Initializing state. Stop the partition and retry the task.	1. Make sure that all partitions are stopped. 2. Retry the deletion operation.

User Management Error Codes	Message	Recovery Action
HSCL2901	This partition is not capable of adding, removing, or moving processors dynamically.	If you know that this partition is capable of processor DLPAR operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL2902	The destination partition is not capable of adding, removing, or moving processors dynamically.	If you know that this partition is capable of processor DLPAR operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL2903	Your processor request goes below the profile's Required processor limit. You can remove or move {0} or fewer processors. Retry the operation.	Retry the operation, entering a smaller number of processors.
HSCL2904	Your processor request exceeds the profile's Maximum processor limit. You can add or move up to {0} processors. Retry the operation.	Retry the operation, entering a smaller number of processors.
HSCL2905	This partition is not capable of adding, removing, or moving memory dynamically.	If you know that this partition is capable of DLPAR memory operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL2906	The destination partition is not capable of adding, removing, or moving memory dynamically.	If you know that this partition is capable of DLPAR memory operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL2907	Your memory request exceeds the profile's Maximum memory limit. You can add or move up to {0} MBs of memory. Retry the operation.	1. Retry the task and request a smaller memory amount. 2. Reset the partition, then reactivate the partition and then retry the operation. 3. If problem persists, contact your software support representative.
HSCL2908	Your memory request goes below the the profile's Minimum memory limit. You can remove or move up to {0} MB of memory. Retry the operation.	1. Retry the task and request a smaller memory amount. 2. Reset the partition, then reactivate the partition and then retry the operation. 3. If problem persists, contact your software support representative.

User Management Error Codes	Message	Recovery Action
HSCL2909	Your memory request exceeds the total available memory of the managed system. You can add up to {0} MB of memory. Retry the operation.	1. Check the available memory of the managed system, retry the task and request a smaller memory amount. 2. Reset the partition, then reactivate the partition and then retry the operation. 3. If problem persists, contact your software support representative.
HSCL290B	This partition is not capable of adding, removing, or moving I/O slots dynamically.	If you know that this partition is capable of DLPAR memory operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL290C	The destination partition is not capable of adding, removing, or moving I/O slots dynamically.	If you know that this partition is capable of DLPAR memory operations, make sure the managed system is powered on, wait and retry the task. If this does not work, rebuild the managed system, or reboot the HMC if necessary. Contact your local representative for more information about this feature.
HSCL290D	Since the managed system is not capable of dynamic logical partitioning, you cannot unassign resources.	None
HSCL290E	Since the managed system is not capable of dynamic logical partitioning, you cannot correct requested memory values.	None
HSCL290F	The partition cannot be activated because there are not enough free processors to satisfy the partition's requirements. However, there are stopped processors available which are still assigned to running partitions that you may unassign.	Attempt to restore lost processors. For more information, see "Restoring Processor Resources" on page 255. When you are finished, try to activate partition again.
HSCL2907	Your memory request exceeds the profile's Maximum memory limit. You can add or move up to {0} MB's of memory. Retry the operation.	1. Retry the task with the lesser memory. 2. Reset the partition and reactivate the partition and then retry the task. 3. If problem persists, call software support.
HSCL2908	Your memory request goes below the the profile's Minimum memory limit. You can remove or move up to {0} MB of memory. Retry the operation.	1. Retry the task with the lesser memory. 2. Reset the partition and reactivate the partition and then retry the task. 3. If problem persists, call software support.
HSCL2909	Your memory request exceeds the total available memory of the managed system. You can add up to {0} MB of memory. Retry the operation.	1. Check the available memory of the managed system and retry the task with lesser memory. 2. Reset the partition and reactivate the partition and then retry the task. 3. If problem persists, call software support.

User Management Error Codes	Message	Recovery Action
HSCL2910	The partition cannot be activated because there are not enough free adapters to satisfy the partition's requirements. However, there are stopped adapters available which are still assigned to running partitions that you may unassign.	Attempt to restore lost adapters. For more information, see "Restoring Adapter Resources" on page 256. When you are finished, activate partition again.
HSCL2911	The partition cannot be activated because there is not enough available system memory to satisfy the profile's required amount. However, there is some memory available which was requested by running partitions but is not being used that you may unassign.	Correct the requested memory value. For more information see "Restoring Memory Resources" on page 256. When you are finished, activate the partition again.
HSCL3001	LED operations are not supported with this CSP version. For LED operations, please upgrade to CSP version 3.0 or greater.	To upgrade to a higher version of CSP, contact your service representative.
HSCL3002	The LED operation failed.	Retry the operation. If the problem persists, contact hardware support.
HSCL3051	An error occurred during frame initialization. Not all I/O may have been powered on. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3052	An error occurred during frame initialization. Not all managed systems could be powered on. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support
HSCL3053	An unknown error occurred during frame initialization. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3054	An error occurred during frame initialization. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3055	An error occurred while deactivating CSPs. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3056	An error occurred during the pinhole reset. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3057	An error occurred while deactivating I/O drawers. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3058	Frame information retrieval failed. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3059	The refresh operation failed. Retry the operation.	Retry the operation. If the problem persists, contact HMC software support.
HSCL305A	The wrong number of cages was received. The I/O cages must be specified in pairs. Retry the operation.	Retry the operation, specifying the adapter drawers in pairs. There should be an even number of drawers specified. If the problem persists, contact HMC software support.
HSCL305B	The list of I/O drawers to deactivate was not sent correctly. Please send the cage numbers of the I/O drawers in pairs.	Retry the operation, sending the cage numbers of the adapter drawers in pairs.
HSCL3200	Unknown lock error.	Contact HMC software support.
HSCL3201	Invalid lock type.	Contact HMC software support.
HSCL3202	Failed to acquire lock because of timeout.	Retry the operation. If the problem persists, contact HMC software support.
HSCL3203	Illegal nested lock type requested.	Contact HMC software support.

User Management Error Codes	Message	Recovery Action
HSCL3204	Lock not held.	Contact HMC software support.

Platform Management Error Codes	Message	Recovery Action
HSCP0001	The Backup Critical Data request completed successfully.	None
HSCP0002	Ensure the media is inserted correctly into the drive and try the operation again.	Verify that the media is inserted correctly in the drive and try the operation again.
HSCP0003	The Backup Critical Data request failed.	Internal HMC Error. Call for HMC software support.
HSCP0004	The media is write protected. Remove the write protection and try the operation again.	Remove the write protection and try the operation again.
HSCP0005	The Backup Critical Data request is in progress. Please wait.	None
HSCP0010	The Format Removable Media request completed successfully.	None
HSCP0011	Ensure the media is inserted correctly into the drive and try the operation again.	None
HSCP0012	The media is write protected. Remove the write protection and try the operation again.	None
HSCP0013	An unknown error occurred. Replace the media and try the operation again.	Replace the media and try the operation again. If the error persists, call for HMC software support.
HSCP0014	The Format Removable Media request failed.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the error persists, call for HMC software support.
HSCP0015	Please wait while the media is being formatted.	None
HSCP0020	The Save Upgrade Data request completed successfully.	None
HSCP0021	The Save Upgrade Data request failed.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0022	The Save Upgrade Data request failed. Ensure the removable media is inserted correctly into the drive.	Verify the removable media is properly inserted in the drive and try the operation again. If the error persists, call for HMC software support.

Platform Management Error Codes	Message	Recovery Action
HSCP0023	The media is write protected. Remove the write protection and try the operation again.	None
HSCP0024	An error occurred while copying the upgrade data. Ensure the removable media is inserted correctly into the drive and retry the operation.	Verify the removable media is properly inserted in the drive and try the operation again. If the error persists, call for HMC software support.
HSCP0025	An error occurred while saving the upgrade data. Try the operation again. If the problem continues, contact your service representative.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0026	An error occurred while trying to mount the media. Ensure the removable media is inserted correctly and try the operation again.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0027	An error occurred while trying to unmount the media. Ensure the media is not being shared.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0028	An non-recoverable error occurred. Refer to the HMC console log for detailed information.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0029	An error occurred while instantiating the save upgrade data target class.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.

Platform Management Error Codes	Message	Recovery Action
HSCP0030	An error occurred creating the file that processes the save upgrade data on the next reboot. Try the operation again.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0040	The corrective service file was successfully downloaded to this system console. Press OK to continue and install this update.	None
HSCP0041	The corrective service file was successfully applied. Wait until all tasks complete and reboot the HMC for the changes to take effect.	None
HSCP0042	An unrecoverable error occurred during the corrective service file download. Try the operation again. If the problem continues, contact your service representative.	Try the operation again. If the error persists, call for HMC software support.
HSCP0043	An unrecoverable error occurred during the corrective service installation. Try the operation again. If the problem continues, contact your service representative.	Try the operation again. If the error persists, call for HMC software support.
HSCP0044	The removable media cannot be mounted. Ensure the media is inserted correctly into the drive and try the operation again.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the error persists, call software support.
HSCP0045	The corrective service data is corrupt. Ensure the media is inserted correctly into the drive and try the operation again.	Verify the removable media is properly inserted in the drive and try the operation again. If the error persists, call for HMC software support.
HSCP0046	An error occurred while attempting to remotely connect to the server. Try the operation again. If the problem continues, contact your service representative.	Verify that the remote site is operational and try the operation again. If the error persists, call for HMC software support.
HSCP0047	An unspecified error occurred while downloading the corrective service file. Try the operation again. If the problem continues, contact your service representative.	Verify that the remote site is operational and try the operation again. If the error persists, call for HMC software support.
HSCP0048	An unknown error occurred. Try the operation again. If the problem continues, contact your service representative.	Try the operation again. If the error persists, call for HMC software support.
HSCP0049	The Install Corrective Service request is in progress. Please wait.	None
HSCP0051	The corrective service file download was unsuccessful.	Read the text on the error message window.

Platform Management Error Codes	Message	Recovery Action
HSCP0052	Successfully downloaded file. Installing, please wait.	N/A
HSCP0053	Corrective service installation was successful.	N/A
HSCP0054	Corrective service installation has failed.	Read the text on the error message window.
HSCP0055	View the console log for details.	N/A
HSCP0056	Halting service installation.	N/A
HSCP0057	Corrective service file download in progress...	N/A
HSCP0058	The corrective service file downloaded successfully, continuing...	N/A
HSCP0060	The Customize Date/Time request completed successfully.	None
HSCP0061	The Customize Date/Time request failed.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0070	Enter an integer value between 1 and 99.	None
HSCP0071	You cannot schedule an event in the past. Set the date and time to schedule the event in the future.	Select a date and time that is after the present time.
HSCP0080	There are no system events.	None
HSCP0081	Unable to display the log data.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0082	Unable to retrieve log data.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.

Platform Management Error Codes	Message	Recovery Action
HSCP0083	An error occurred while processing the exit request.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCP0090	Cannot check both the 'Export default gateway' and 'Silent' options for 'routed'.	Select either 'Export default gateway' or 'Silent' for the Routed option.
HSCP0091	You may need to reboot for all Network Settings changes to take effect.	Restart the HMC.
HSCP0092	Unable to save your Network Settings updates to the system configuration files.	Try the operation again. Reboot the HMC If the error persists, call for HMC software support.
HSCP0093	Ethernet driver {1} cannot be set to {0}.	1. Select a valid speed for the adapter 2. Select **Auto-negotiate speed** 3. Reboot the HMC
HSCP0100	No CECs were detected that are attached to this system console.	1. If you have a managed system attached, reboot the HMC. 2. If the problem persists, contact your service service representative.
HSCP0101	No partitions have been defined for this CEC.	1. Check to ensure that Service Focal Point is communicating correctly with the managed system. 2. Reboot the HMC. 3. If the error persists, call for HMC software support.
HSCP0102	A blank or incorrect entry was entered in the partition password field.	Re-enter a valid password in the entry field and try the operation again.
HSCP0103	A blank or incorrect entry was entered in the listening port field.	Re-enter a valid listening port and try the operation again.
HSCP0104	A blank or incorrect entry was entered in the IP address field.	Re-enter the IP address and try the operation again.
HSCP0110	The Inventory Scout command completed successfully.	N/A
HSCP0111	The Inventory Scout command request failed.	Try the operation again. Reboot the HMC If the error persists, call for HMC software support.
HSCP0112	The removable media cannot be mounted. Ensure the media is inserted correctly into the drive and try the operation again.	1. Insert a properly formatted diskette into the drive. 2. Try using an alternate diskette 3. If the error persists, call for HMC software support.
HSCP0113	The media is write protected. Remove the write protection and try the operation again.	Remove write protection on the media and retry the operation.

Platform Management Error Codes	Message	Recovery Action
HSCP0114	The Inventory Scout request failed. Ensure the removable media is inserted correctly into the drive.	1. Insert the properly formatted diskette into the drive 2. Try using an alternate diskette 3. If the error persists, call for HMC software support.
HSCP0115	An error occurred while copying the Inventory Scout data. Verify that a blank formatted diskette is inserted correctly in the drive and retry the operation.	1. Ensure that there is enough free space on the media. 2. Try using an alternate diskette and retry the operation. 3. If the error persists, call for HMC software support.
HSCP0117	An error occurred while trying to unmount the media.	N/A
HSCP0118	The Inventory Scout daemon was restarted successfully.	N/A
HSCP0119	The Inventory Scout daemon cannot be restarted. Reboot the HMC and try the operation again.	Try the operation again. Reboot the HMC. If the error persists, call for HMC software support.
HSCP0120	The CEC name is malformed	Reboot the HMC. If the error persists, call for HMC software support.
HSCP0121	The Inventory Scout request failed. An error occurred while copying data to removable media.	1. Retry the operation. 2. Restart the **invscout** daemon 3. If the error persists, call for HMC software support.
HSCP0122	The system partition(s) did not respond to query attempts.	1. Check to ensure that Service Focal Point is communicating correctly with the managed system. 2. Reboot the HMC. 3. If the error persists, call for HMC software support.
HSCP0123	Unable to start the terminal session using available error data. Return to Service Management interface and attempt to start the TTY session from there.	1. Return to the Service Management interface and attempt to start the virtual terminal session. 2. If the problem persists, contact your service representative.
HSCP0124	Unrecoverable error attempting to start a TTY session. Return to Service Management interface and attempt to start the TTY session from there.	1. Return to the Service Management interface and attempt to start the virtual terminal session. 2. If the problem persists, contact your service representative.
HSCP0125	An incorrect user ID and password combination was entered. Specify a valid user ID and password and try the operation again.	1. Specify a valid user ID and password and retry the operation. 2. Ensure that the remote service (ftp) site is operational. 3. If the problem persists, contact your service representative.

Platform Management Error Codes	Message	Recovery Action
HSCP0126	The corrective service file was not found on the server. Ensure the correct fully qualified path and filename has been specified for the 'Patch file' field and retry the operation.	1. Specify a valid user ID and password and retry the operation. 2. Ensure that the remote service (ftp) site is operational. 3. If the problem persists, contact your service representative.
HSCP0127	An error occurred while unpacking the corrective service file. The file may be corrupt, or the HMC may have run out of disk space. Try the operation again. If the problem continues, contact your service representative.	Reboot the HMC. If the error persists, call for HMC software support.
HSCP0128	A required file is missing from the service package. Contact your service representative.	Contact your service representative.
HSCP0129	An attempt was made to apply incorrect service to this version of HMC software. Ensure the correct service filename has been specified and retry the operation.	1. Ensure that the correct service file name has been entered and try the operation again. 2. If the problem persists, contact your service representative.
HSCP0130	The target directory for service file extraction does not exist. Contact your service representative.	Reboot the HMC. If the error persists, call for HMC software support.
HSCP0131	A fatal error occurred during service file installation. The system may be unstable. Contact your service representative	Reboot the HMC. If the error persists, call for HMC software support.
HSCP0135	Error {0} processing data on removable media.	1. Attempt to download and apply the service file again. 2. Perform the Save Upgrade Data task to preserve configuration data and then reinstall the HMC from recovery CD as if an upgrade 3. If the problem persists, contact your service representative.
HSCP0136	The corrective service file was successfully copied to the HMC. Select the Frame 'Install Corrective Service' task to apply this update.	Select the Frame **Install Corrective Service** task to apply this update.
HSCP0137	The corrective service file was successfully downloaded to the HMC. Select the Frame 'Install Corrective Service' task to apply this update.	Select the Frame **Install Corrective Service** task to apply this update.
HSCP0138	An internal error occurred during Save Upgrade Data processing. Refer to the HMC console log for detailed information and recovery actions.	Refer to the HMC console log for detailed information and recovery actions.

Service Focal Point Error Codes	Message	Recovery Action
HSCS0001	Unable to access RMC to obtain Serviceable Events.	The HMC could not retrieve the Serviceable Events. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0002	Unable to process request.	The HMC could not process your request. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0003	Unable to update the attribute on the Serviceable Event.	The HMC could not process your request to make changes to the Serviceable Event. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0004	Unable to locate Serviceable Event to update.	The HMC could not locate the Serviceable Event you are trying to view or update. It may have expired or otherwise been closed. Exit the Select Serviceable Event dialog and retry.
HSCS0005	Function Failed: Error occurred attempting to display a Serviceable Event panel.	The HMC was unable to locate or launch a panel you have requested. This is an internal HMC error. 1. Perform Backup Critical Data task. 2. Call for HMC software support.
HSCS0006	This Serviceable Event may contain more information that this version of the HMC can display. You may wish to upgrade your HMC to the latest version.	In order to see Serviceable Event data made available in more recent HMC versions, upgrade this HMC to the most recent version or switch to an HMC that has already been upgraded.
HSCS0008	Function Failed: An error occurred when retrieving machine names.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0020	Function Failed: An error occurred when launching the Service Focal Point Settings panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0021	Function Failed: Error occurred getting information to display the Service Focal Point settings.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0022	Function Failed: An error occurred when updating Service Focal Point settings.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0023	Function Failed: Error occurred processing button for the Service Focal Point Settings Panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.

Service Focal Point Error Codes	Message	Recovery Action
HSCS0024	Function Failed: Error occurred processing sort for the Service Focal Point Settings Panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0025	Function Failed: Error occurred processing Double Click for the Service Focal Point Settings Panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0026	Service Focal Point settings have been saved successfully.	None.
HSCS0040	New FRU Location Code and Part Number must be entered.	Enter the requested Location Code and Part Number.
HSCS0041	A New FRU Part Number must be entered.	Enter the requested Part Number.
HSCS0042	There was nothing to apply.	There were no changes to the FRU list to be added to the Serviceable Event.
HSCS0043	The No FRUs to Update box was checked but there are updated FRUs in the in the pending table. If there are no FRUs to update, remove the ones from the pending table. If you want to update the FRUs from the pending table, uncheck the check box.	None
HSCS0044	The No FRUs to Update box was unchecked and there are no updated FRUs in the in the pending table. If there are no FRUs to update, check the check box to indicate this.	None
HSCS0045	Function Failed: An error occurred when updating FRU information for the Serviceable Event.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0046	Function Failed: An error occurred when attempting to remove an item from the list.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0047	Function Failed: An error occurred when attempting to Close the Serviceable Event	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0048	Function Failed: An error occurred when adding FRU information for the Serviceable Event.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0049	Function Failed: An error occurred when processing the panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0050	Function Failed: An error occurred when launching panel.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.

Service Focal Point Error Codes	Message	Recovery Action
HSCS0060	Cannot change state from Unknown for machine	The requested machine state is not allowed at this time. Close and then restart the Enable/Disable panels for updated machine information.
HSCS0061	Insert scratch diskette number {0} of {1}.	Insert a scratch diskette and select the appropriate button.
HSCS0062	Insert DVD cartridge and press the {0} button.	Insert a formatted DVD cartridge and push the appropriate button.
HSCS0064	No extended error data available.	Select a serviceable event that has extended error data associated with it.
HSCS0065	Error writing to diskette: {0}	Make sure there is a diskette in the diskette drive. Try the operation again.
HSCS0066	Error writing to DVD cartridge: {0}	Make sure there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0067	Error reading extended error data: {0}	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0068	Error creating temporary file: {0}	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCS0069	Error writing to temporary file: {0}	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCS0070	Error formatting diskette: {0}	Make sure there is a diskette in the diskette drive. Try the operation again.
HSCS0071	Extended error data has been saved successfully.	None
HSCS0072	The saving of extended error data has been cancelled.	No action. The operation was cancelled as a result of your request.
HSCS0080	Error encountered while getting the partition information.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0081	Error encountered while reading the partition information.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.

Service Focal Point Error Codes	Message	Recovery Action
HSCS0082	Error encountered while getting the extended error data.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0083	Unexpected error encountered while saving the extended error data.	1. Verify that the removable media is properly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, call for HMC software support.
HSCS0084	Error encountered while attempting to call home with the extended error information.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0085	Error encountered while attempting to call home with the extended error information. The call program returned a value of {0}.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0086	Request to call home the extended error information has been successfully submitted. See the Service Agent application to monitor the progress of the request.	The operation was successful. Use the Service Agent application to monitor the progress of the request.
HSCS0087	Error encountered while attempting to call home the Serviceable Event.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0088	Error encountered while attempting to call home the Serviceable Event. The callsa program returned a value of {0}.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0089	Request to call home the Serviceable Event has been successfully submitted. See the Service Agent application to monitor the progress of the request.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0090	Unexpected return code encountered while creating a temporary packaging file: {0}	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0096	No items selected when button was pressed.	Not all functions may be operating. Wait and try the previous function again. If error continues, shut down and restart the HMC. If error persists, call for HMC software support.
HSCS0100	Please wait while the extended error data is being saved.	The extended error data is being saved to the appropriate removable media.
HSCS0101	Error writing to DVD cartridge.	Ensure there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0102	Error unmounting DVD cartridge after writing data successfully.	Ensure there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0103	DVD drive is already mounted.	None

Service Focal Point Error Codes	Message	Recovery Action
HSCS0104	The LED request did not complete successfully.	1. Retry the task. 2. Log out and then back in to the HMC interface. 3. Reboot the HMC. 4. If the problem persists, call HMC software support.
HSCS0105	The LED request completed successfully.	None.
HSCS0106	Function failed: An error occurred attempting to display the LED Management panel.	1. Retry the task. 2. Log out and then back in to the HMC interface. 3. Reboot the HMC. 4. If the problem persists, call HMC software support.
HSCS0122	Function failed: An error occurred attempting to display the Hardware Services panel.	1. Retry the task. 2. Log out and then back in to the HMC interface. 3. Reboot the HMC. 4. If the problem persists, call HMC software support.
HSCS0123	The System Attention LED for the selected machine is not supported. The system LED will not be activated	None.
HSCS0124	The Identify LED for the selected FRU is not supported. The FRU LED will not be activated.	None.

Virtual Terminal Errors

When using a virtual terminal (VTERM), you might see an error code displayed in the bottom-left corner of the VTERM window. The following table lists the error codes and the recovery actions for each.

Virtual Terminal (VTERM) Error Codes	Message	Recovery Action
Comm 654	The virtual terminal server is unable to process this type of request. An unknown error occurred during virtual terminal device-type negotiations.	If the error persists, contact the system administrator for help.
Comm 655	The socket connection to the Virtual Terminal server has been established and the session is waiting for negotiation to finish.	If the error persists, contact the system administrator for help.
Comm 657	The session is in the process of establishing the TCP/IP connection to the virtual terminal server. When you close a session that displays COMM 657, there may be some delay before it closes.	The delay varies. You can close the browser.

Virtual Terminal (VTERM) Error Codes	Message	Recovery Action
Comm 658	The session is initializing the TCP/IP connection to the HMC.	If the error persists, contact the system administrator for help.
Comm 659	The Virtual Terminal TCP connection to the session has not succeeded or has failed.	• The TCP/IP connection to the virtual terminal server could not be established. • You clicked Disconnect on the Communication menu. • The virtual terminal server closed the TCP/IP connection either by application control or because it detected an error.

Operating States

In the Contents area, an operating state is listed next to your managed system. Read the next section to learn more about what each of these states mean, and the actions you should take to recover.

Managed System Operating States

The following operating states apply to the managed system itself.

State	Description	Recovery Action
Initializing	The managed system is powered on and is initializing.	Wait for initialization to complete. Initialization can take up to an hour, depending on the managed system's hardware and boot configuration.
Ready	The managed system is powered on and functioning normally.	None
No Power	The managed system is powered off.	None
Error	The managed system's operating system or hardware is experiencing errors.	If the managed system is set up to run as a Full System Partition, the system will also indicate an Error state. Read the managed system operator panel.
Incomplete	The HMC cannot gather complete partition, profile, and resource information from the managed system.	In the Contents area, highlight the managed system icon and select **Rebuild the Managed System** from the menu.
No Connection	HMC cannot contact the managed system.	1. Delete the managed system from the Navigation area by highlighting the managed system icon and selecting **Delete** from the menu. 2. Follow the instructions to delete the managed system from the Navigation area. 3. Reconnect to the managed system by checking that the cable connections are secure.

State	Description	Recovery Action
Recovery	The partition and profile data stored in the managed system is corrupted.	In the Contents area, select the managed system icon and choose **Recover Partition Data** from the menu. • For the data to be restored, the managed system must be powered on using the Partition Standby power on option. If your system is not currently powered on in Partition Standby, it will be powered off first before powering on to Partition Standby mode. In this case, restoring data can take up to an hour. OR • If you do not want to restore data from a backup source, select **Initialize** from the menu. **Note:** Powering on using the Partition Standby option will require that you power off the managed system if the system is currently using the Full System Partition.
Version Mismatch	Your managed system's service processor level is higher than your HMC's code level.	Contact your service representative to upgrade your HMC's level so that the levels match.
CUoD CTA	You must accept the CUoD license.	To accept the license, do any of the following: • When you boot the HMC and managed system, click the **Accept** button on the **License Agreement** panel. • If you have already booted the HMC and managed system, select the managed system in the Contents area. Select **CUoD —> Accept License**. Click the **Accept** button. • Power off the managed system, remove all CUoD resources from the managed system, and then power your managed system back on again.

Partition Operating States

The following operating states describe the logical partition you have created.

State	Description	Recovery Action
Ready	The partition is not yet active but is ready for activation.	None
Starting	The partition is activated and is going through its booting routines.	None
Running	The partition has finished its booting routines. The operating system can be performing its booting routines or is in its normal running state.	None

State	Description	Recovery Action
Error	Activation of this partition failed due to a hardware or operating system error.	Select the partition and choose the **Read Boot Error Value** task from the menu to see the reasons for the activation failure.“Boot Error Values” on page 260 You can also try to activate the partition again.
Not Available	This partition is not available for use. Reasons can include: • The managed system is powered off. • The Full System Partition is not available when the managed system is powered on with the Partition Standby power-on option. • Logical partitions are not available when the managed system is powered on with the Full System Partition power-on option. • Affinity partitions are not available when the managed system is powered on and non-affinity partitions are activated first. • Non-affinity partitions are not available when the managed system is powered on and affinity partitions are powered on first.	Turn on the power to the managed system and select either Full System Partition or Partition Standby during the power-on process.
Open Firmware	The partition was activated by a profile that specified an OPEN_FIRMWARE boot mode.	None

Restoring Partition Resources

The following section has procedures to help you restore partition resources that are stopped but are still assigned to a partition as a result of a failed dynamic logical partitioning operation. These resources are lost, or are unusable by any other partition until they have been unassigned.

Restoring Processor Resources

When you are dynamically adding processor resources to a partition, the HMC determines if there are any stopped processors in a running partition. If the HMC finds stopped, unused processors, a **Processor Information** button appears on the panel. When you click this button, the **Processor Recovery** window opens. This window displays each stopped processor’s states, statuses, and the partitions to which they are currently assigned.

If no partition is performing a dynamic logical partitioning processor operations, you can unassign stopped processors from their partitions and free them for system use.

Note: If another user is in the middle of performing a dynamic logical partitioning processor operation on any partition, and you unassign stopped processors from that partition, you will cause the user’s dynamic logical partitioning operation to fail.

To unassign stopped processors, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console’s icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system’s icon to expand the tree.
6. Select the partition to which you want to add the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.

8. Select **Processors**.
9. The **Dynamic Logical Partitioning** window opens. Click **Add resources to this partition**.
10. If the **Processor Information** button appears underneath the **Number of CPUs to add** field, the HMC has discovered stopped processors on running partitions that you might be able to unassign, or free for system use. If the **Processor Information** button appears, click it. If it does not, you do not have processor resources to restore.
11. The **Restore Processors** window opens. This window displays each lost processor, along with the processor's state, status, and partition assignment. Select the processor you want to free and click **Unassign**. The processors you selected are then unassigned and freed for other partitions to use.

Restoring Adapter Resources

When you are dynamically adding adapter resources to a partition, the HMC determines if there are any stopped adapters in any running partition. If the HMC finds stopped, unused adapters, an **Adapter Information** button appears on the panel. When you click this button, the **Restore Adapters** window opens. This window displays each stopped adapter's state, status, and the partition to which it is assigned. If another user is not performing a dynamic logical partition operation, you can unassign stopped adapters from their partitions and free them for system use.

Note: If another user is in the middle of performing a dynamic logical partitioning adapter operation on any partition, and you unassign stopped adapters from that partition, you will cause the user's dynamic logical partitioning operation to fail.

To unassign stopped adapters from a running partition, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition to which you want to add the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Adapters**.
9. The **Dynamic Logical Partitioning** window opens. Click **Add resources to this partition**.
10. If the **Adapter Information** button appears underneath the **Adapters to add** field, the HMC has discovered stopped processors on running partitions that you might be able to unassign, or free for system use. If the **Adapter Information** button appears, click it. If it does not, you do not have adapter resources to restore.
11. The **Adapter Recovery** window opens. This window displays each lost adapter, along with the adapter's drawer, slot, type, state, and partition assignment. If you are sure that another user is not currently performing a dynamic logical partitioning operation, select the adapter you want to free and click **Unassign**. The adapters you selected are then unassigned and freed for system use.

Restoring Memory Resources

When you are dynamically adding, removing, or moving memory resources to a partition, the HMC determines if there is an inconsistency between the amount of memory being used by the partition and the amount of memory requested by the partition for pending memory changes.

If these amounts are not equal, a **Memory Information** button appears on the window. When you click this button, the **Restore Memory** window opens. This window displays each running partition's amount of memory in use, requested memory amount, the maximum and minimum profile memory values, and the total available system memory. If another user is not performing any dynamic logical partitioning memory operations, you can correct a partition's requested memory value amount so that it is equal to the memory

amount currently in use. If the requested memory value is greater than the amount of memory actually in use, a correction of the requested memory amount will result in some memory being freed for other partitions to use. If another user is in the middle of performing a dynamic logical partitioning memory operation on a partition, and you correct the requested memory amount for that partition, you will cause the other user's dynamic logical partitioning operation to fail.

To correct requested memory amounts, do the following:

1. Log in to the HMC using either the System Administrator or Advanced Operator roles.
2. In the Navigation area, click the console's icon to expand the tree.
3. In the Navigation area, click the **Server and Partition** folder.
4. In the Contents area, click the **Server Management** icon.
5. In the Contents area, click the managed system's icon to expand the tree.
6. Select the partition to which you want to add the processors.
7. From the Selected menu, select **Dynamic Logical Partitioning**.
8. Select **Memory**.
9. The **Dynamic Logical Partitioning** window opens. Click **Add resources to this partition**.
10. If the **Memory Information** button appears underneath the **Destination Partition Details** field, the HMC has discovered memory inconsistencies. If the **Memory Information** button appears, click it. If it does not appear, you do not have memory resources to restore.
11. The **Restore Memory** window opens. This window displays the name of the partition that has the inconsistency, the amount of memory in use by this partition, the requested memory amount, this partition's minimum and maximum memory amounts, and the amount of free (system available) memory. Select the partition or partitions you want to correct, and click **Correct Requested Value**. The memory amount is then corrected and the **Dynamic Memory Configuration** window is updated with the new values.

Error Recovery Actions

The recovery action for many error messages is to perform a rebuild managed system operation. This section has procedures to help rebuild a managed system. References to this procedure are indicated throughout the error message tables as appropriate.

Rebuild is Indicated for Managed System

For messages that indicate that a rebuild managed system operation is needed, do the following to be sure that the operation is necessary:

1. Verify you have the correct authority to perform the task.
   - If you do not, log in with the correct user authority and try the task again.
   - If you do have the correct authority, retry the task. If it still fails, continue with step 2.
2. Perform the Rebuild Managed System task (see "Steps to Rebuild a Managed System") then retry the failing task. If the task still fails, continue with step 3.
3. Reboot the HMC, then verify that the managed system is in *Ready* state.
   - If the managed system is in *Ready* state, retry the failing task. If the task still fails, call for HMC software support.
   - If the managed system is in any state other than *Ready*, (for example, not in *Connection* state, *Error* state, or another state) refer to "Managed System States for the HMC" on page 259 for the recovery procedure for the current state.

Steps to Rebuild a Managed System

To rebuild a managed system, do the following:

1. In the HMC contents area, select the managed system that you want to rebuild.

2. Select **Rebuild Managed System** from the Select menu or by clicking the right mouse button in the content area.
3. A confirmation window displays a message asking you to confirm whether you want to perform this task.

   While this task is running, you cannot perform any other HMC functions. This task can take up to several minutes to complete.

Steps for Rebooting the HMC

To reboot the HMC, do the following:

1. From the Select menu, select **Console**.
2. Select **Exit**.
3. When you exit from your HMC session, you can choose to shut down, reboot, or log off from your session. Using the pull-down bar, select **reboot**.
4. Select **Exit**. The HMC reboots.

Performing a File System Check on HMC Reboot

In the event of an unexpected power loss or if the white reset button on the HMC is pressed, the system runs a file system check (`fsck`) on the next system reboot. If the automatic file system check fails, the HMC prompts the user to enter the HMC's root password so that it can perform a file system maintenance manually. If the following message displays: `Enter the root password or hit Control-D to reboot.`, do the following to recover the HMC:

1. Type the following root password: `passw0rd`
2. To run a file-system check, type `fsck` *file system* where *file system* is the name of the file system that fails the file system check, such as **/** and **/var** in the field. When the checking is completed, a prompt window opens.
3. Type `reboot`.

   OR

   Press Ctrl-D to reboot the HMC interface.

Changing a Partition Host Name Manually

If you need to change the host name of the partition manually, before changing the host name of the partition, do the following:

1. Run the following command (Skip this step if the AIX level is earlier than AIX 5.1 with 5100-02 Recommended Maintenance Package.):

   ```
   /usr/sbin/rsct/bin/runact -c IBM.ManagementServer SetRTASPollingInterval Seconds=0
   ```

2. Run the following command:

   ```
   /usr/sbin/rsct/bin/lsrsrc IBM.ManagementServer Hostname
   ```

   The output displayed will be similar to the following: (If the partition is managed by multiple HMCs, there may be multiple entries, because each HMC has its own entry.)

   ```
   resource 1: Hostname = "hmc1.mydomain.mycompany.com"
   ```

3. For each entry, remove the resource using the host name shown. For example, type the following:

   ```
   /usr/sbin/rsct/bin/rmrsrc -s'Hostname = "hmc1.mydomain.mycompany.com"' IBM.ManagementServer
   ```

   . You can verify that all entries have been removed by performing Step 2 again.

4. Run the following command:

   ```
   /usr/sbin/rsct/bin/rmcctrl -z
   ```

5. Change the host name of the partition.
6. Once the host name has been changed, run the following command: **/usr/sbin/rsct/bin/rmcctrl -A**

Managed System States for the HMC

This section describes the states for a managed system that display on the HMC. Follow the procedures in this section to attempt to restore management of a system in one of the listed states.

No Connection State

In the *No Connection* state, the HMC has lost contact with the managed system, or power to the service processor has been removed. Do the following:

1. Check the operator panel on the managed system to verify that the power is on.
   a. If the power light indicates that there is no power on the managed system operator panel, refer your system's user's guide for problem-determination procedures.
   b. After power is restored, wait 5 minutes for the service processor to re-IPL and the HMC to re-establish contact. If the HMC can access partitions using a virtual terminal (VTERM) but the state is still *No Connection*, call for HMC support.
2. If the power indicator is on, wait 5 minutes for the HMC to attempt to reestablish contact. The service processor in the managed system may be in the process of turning power on. If partitions no longer respond, the system power is off.
3. From a telnet session from another system, attempt to ping or contact active partitions on this managed system.

   If the partitions are active, do the following:
   a. Verify that the serial cable on the HMC is firmly connected and that it is not damaged.
   b. Reboot the HMC.
   c. Reset the Service Processor.
4. If the managed system is running and restarting the HMC did not resolve the problem, call for HMC software support.

Incomplete State

In the *Incomplete* state, the HMC is unable to collect information required to build a complete representation of the managed system. Do the following:

1. Select **Rebuild Managed System** from the Managed System Task list. If the state goes to *Recovery*, see "Recovery State." If the state does not go to *Recovery*, continue with the next step.

   Note: This operation performed in the next step may take up to ten minutes to complete.
2. Reboot the HMC. If the state goes to *Recovery*, see "Recovery State."

   If the state remains *Incomplete*, verify whether there is a redundant HMC and verify that no one is entering commands from the alternate HMC.

   Repeat step 1. If it still fails, go to the next step.
3. Restore the profile data (see task list). The profile-data restore task is a full restore from a backup copy.
4. Verify that the HMC serial cable is securely attached to the HMC and that it is not damaged.
5. Reset the service processor.
6. If the problem persists, call for service.

Recovery State

In the *Recovery* state, profile data stored in the managed system has been cleared or corrupted. Do the following:

1. Select **Recover partition data** from the managed system task list to restore or initialize profile data.
2. If the state changes to *Incomplete*, see "Incomplete State" for recovery procedures.
3. If the state changes to *No Connection*, see "No Connection State" for recovery procedures.

4. If the restore fails, reset the service processor.
5. Clear NVRAM (nonvolatile memory), and repeat steps 1 through 4.
6. If the problem persists, call for HMC software support.

Error State

The *Error* state automatically generates a call to the service support center if the function is enabled. If the function is not enabled, call for HMC software support.

Open Firmware State

In the *Open Firmware* state, the partition has been activated. You can open a virtual terminal window to the partition and enter open firmware commands.

Boot Error Values

If a problem occurs during the boot process and initial loading of the console software, the following table contains the boot error values and messages that might display on the HMC.

Boot Error Values	Message
0x0A	NOT_ENOUGH_PARTITION_LICENSED_MEMORY
0x00	NO_ERROR
0x01	NO_GLOBAL_SERVER
0x02	NO_CONTIGUOUS_PAGE_TABLE_MEMORY
0x03	NO_CONTIGUOUS_REAL_MODE_MEMORY
0x04	NOT_ENOUGH_PARTITION_LOGICAL_MEMORY
0x05	ALL_ASSIGNED_PROCESORS_ARE_NOT_WORKING
0x06	NO_PROCESSORS_ASSIGNED
0x07	INVALID_PROCESSOR_ASSIGNED_FOR_ALPAR_PARTITION
0x08	NO_MEMORY_AVAILABLE_FOR_ALPAR_PARTITIONS
0x60	ANOTHER_SERVICE_AUTHORITY_PARTITION_IS_ACTIVE
0x7F	FAIL_TO_BOOT
0x80	I/O_SLOT_ASSIGNMENT_ERROR
0xAC	AIX_OS_TERM_WITH_CRASH_CODE

Releasing an HMC Lock on the Managed System

If you have two HMCs connected to your managed system, one HMC temporarily locks the other out while it is performing operations. This action prevents the other HMC from operating on the managed system because simultaneous operations could cause conflicting results. If the interface is locked, most console operations automatically wait for the lock to release.

However, in the rare event that an HMC has a problem that prevents the lock from being properly released, you may need to manually unlock the connection to the managed system. Typically, if one HMC has locked the connection, you must unlock it from the other HMC, which then allows other HMCs to communicate with the managed system and run further commands.

To release a lock on a managed system, you must be a member of one of the following roles:

- System Administrator
- Advanced Operator

To release an HMC lock, do the following:

1. In the Contents area, select the managed system.
2. In the menu, click **Selected**.
3. Select **Release Console Lock**.

Index

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

Hardware Management Console for pSeries
Installation and Operations Guide

Publication No. SA38-0590-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SA38-0590-07

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department H6DS-905-6C006
11501 Burnet Road
Austin, TX 78758-3493

Fold and Tape | **Please do not staple** | Fold and Tape

SA38-0590-07

Cut or Fold
Along Line

Part Number: 80P3842

Printed in USA

November 2003

(1P) P/N: 80P3842

SA38-0590-07

Spine information:

Hardware Management Console for pSeries
Installation and Operations Guide

SA38-0590-07