

# ESCALA Power7



T æ æ ã \* Á@Á  
Pæå, æ^Á æ æ^ { ^} oÁ [ ] • [ | ^



# ESCALA Models Reference

The ESCALA Power7 publications concern the following models:

Bull Escala E1-700 / E3-700	(31E/2B ,8231-E2B)
Bull Escala E1-705	(31E/1C, 8231-E1C)
Bull Escala E1-715	(31E/1D, 8231-E1D)
Bull Escala E3-705	(31E/2C, 8231-E2C)
Bull Escala E3-715	(31E/2D, 8231-E2D)
Bull Escala E2-700 / E2-700T	(02E/4B, 8202-E4B)
Bull Escala E2-705 / E2-705T	(02E/4C, 8202-E4C)
Bull Escala E2-715 / E2-715T	(02E/4D, 8202-E4D)
Bull Escala E4-700 / E4-700T	(05F/6B, 8205-E6B)
Bull Escala E4-705	(05E/6C, 8205-E6C)
Bull Escala E4-715	(05E/6D, 8205-E6D)
Bull Escala E5-700	(33E/8B, 8233-E8B)
Bull Escala E5-715	(08E/8D, 8408-E8D)
Bull Escala M5-715	(09R/MD, 9109-RMD)
Bull Escala M6-700	(17M/MB, 9117-MMB)
Bull Escala M6-705	(17M/MC, 9117-MMC)
Bull Escala M6-715	(17M/MD, 9117-MMD)
Bull Escala M7-700	(79M/HB, 9179-MHB)
Bull Escala M7-705	(79M/HC, 9179-MHC)
Bull Escala M7-715	(79M/HD, 9179-MHD)
Bull Escala H9-700	(19F/HB, 9119-FHB)

References to 8236-E8C models are irrelevant.

## Hardware

February 2013

BULL CEDOC  
357 AVENUE PATTON  
B.P.20845  
49008 ANGERS CEDEX 01  
FRANCE

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 2013

Printed in France

## **Trademarks and Acknowledgements**

We acknowledge the rights of the proprietors of the trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

*The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.*

---

# Contents

<b>Managing the HMC</b> . . . . .	<b>1</b>
What's new in Managing the HMC . . . . .	1
Introduction to the HMC . . . . .	2
User interface style for the HMC . . . . .	2
Predefined user IDs and passwords. . . . .	3
Tasks and roles . . . . .	3
Starting the HMC. . . . .	4
Using the web-based user interface . . . . .	5
Task bar . . . . .	5
Navigation pane . . . . .	5
Welcome. . . . .	5
Systems Management . . . . .	6
Servers . . . . .	6
Frames . . . . .	10
Custom Groups . . . . .	10
System Plans . . . . .	11
HMC Management . . . . .	12
Service Management . . . . .	12
Updates . . . . .	12
Work pane. . . . .	13
Working with Tables . . . . .	13
Selecting Rows . . . . .	13
Filtering . . . . .	13
Sorting . . . . .	13
Column configuration . . . . .	14
Views menu . . . . .	14
Status bar . . . . .	14
Status: Unacceptable . . . . .	14
Status: Attention LEDs. . . . .	14
Status: Serviceable Events . . . . .	14
Status Overview. . . . .	15
HMC tasks, user roles, IDs, and associated commands . . . . .	15
Systems Management for Servers . . . . .	39
Properties . . . . .	39
Update Password . . . . .	40
Operations . . . . .	41
Power On . . . . .	41
Power Off . . . . .	41
Power Management . . . . .	42
LED Status . . . . .	42
Schedule Operations . . . . .	43
Advanced System Management . . . . .	44
Utilization Data . . . . .	45
Rebuild. . . . .	45
Change Password . . . . .	45
Configuration . . . . .	45
Create Logical Partition . . . . .	45
System Plans . . . . .	46
Partition Availability Priority . . . . .	46
View Workload Management Groups. . . . .	46
Manage Custom Groups . . . . .	46
Manage Partition Data. . . . .	46
Manage System Profiles . . . . .	48
Virtual Resources . . . . .	48
Shared processor pool management . . . . .	48
Shared Memory Pool Management . . . . .	49

Virtual Storage Management . . . . .	49
Virtual Network Management . . . . .	49
Connections . . . . .	50
View service processor connection status . . . . .	50
Resetting or removing connections . . . . .	50
Disconnecting another HMC. . . . .	50
Adding a managed system . . . . .	51
Correcting a connection problem . . . . .	51
Correcting a No connection state for a managed system . . . . .	51
Correcting an Incomplete state for a managed system . . . . .	53
Correcting a Recovery state for a managed system . . . . .	53
Correcting an Error state for a managed system . . . . .	53
Correcting a Failed Authentication state for a managed system . . . . .	53
Correcting a new connection problem between the HMC and a managed system . . . . .	54
Hardware Information. . . . .	55
Adapters . . . . .	55
Host Channel Adapter (HCA) . . . . .	55
Host Ethernet Adapter (HEA) . . . . .	55
View Hardware Topology . . . . .	55
PCIe Hardware Topology. . . . .	56
Updates . . . . .	56
Serviceability . . . . .	56
Manage Serviceable Events . . . . .	56
Create Serviceable Event . . . . .	57
Reference Code History . . . . .	58
Control Panel Functions . . . . .	58
Hardware . . . . .	58
Add FRU . . . . .	58
Add Enclosure . . . . .	58
Exchange FRU . . . . .	58
Exchange Enclosure . . . . .	59
Remove FRU . . . . .	59
Remove Enclosure . . . . .	59
Power On/Off IO Unit . . . . .	59
Manage Dumps . . . . .	59
Collect VPD . . . . .	60
Edit MTMS . . . . .	60
FSP Failover . . . . .	60
Capacity on Demand . . . . .	61
Systems Management for Partitions . . . . .	61
Properties . . . . .	61
Change Default Profile . . . . .	62
Operations . . . . .	62
Activate . . . . .	62
Restart . . . . .	62
Shut Down . . . . .	63
Manage Attention LED . . . . .	63
Schedule Operations . . . . .	63
viosrcmd . . . . .	65
Delete . . . . .	65
Mobility . . . . .	65
Migrate. . . . .	65
Validate . . . . .	66
Recover. . . . .	66
Suspend operations. . . . .	66
Validate . . . . .	66
Suspend . . . . .	67
Resume. . . . .	67
Configuration . . . . .	67
Manage Profiles . . . . .	67
Manage Custom Groups . . . . .	68

Save Current Configuration . . . . .	68
Hardware Information . . . . .	68
Adapters . . . . .	68
Host Ethernet Adapter (HEA) . . . . .	68
Host Channel Adapter (HCA) . . . . .	68
Switch Network Interface . . . . .	69
Virtual IO Adapters . . . . .	69
Dynamic Logical Partitioning . . . . .	69
Processor . . . . .	69
Memory . . . . .	70
Physical Adapters . . . . .	70
Virtual Adapter . . . . .	70
Host Ethernet . . . . .	70
Console window . . . . .	71
Serviceability . . . . .	71
Manage Serviceable Events . . . . .	71
Reference Code History . . . . .	72
Control Panel Functions . . . . .	72
Systems Management for Frames . . . . .	72
Properties . . . . .	73
Update Password . . . . .	73
Operations . . . . .	73
Initialize Frames . . . . .	73
Initialize All Frames . . . . .	74
Rebuild . . . . .	74
Change Password . . . . .	74
Power On/Off IO Unit . . . . .	74
Configuration . . . . .	74
Manage Custom Groups . . . . .	74
Connections . . . . .	75
Bulk Power Assembly (BPA) Status . . . . .	75
Reset . . . . .	75
Hardware Information . . . . .	75
View RIO Topology . . . . .	76
Serviceability . . . . .	76
Manage Serviceable Events . . . . .	76
Hardware . . . . .	77
Add FRU . . . . .	77
Add Enclosure . . . . .	77
Exchange FRU . . . . .	77
Exchange Enclosure . . . . .	77
Remove FRU . . . . .	78
Remove Enclosure . . . . .	78
System Plans . . . . .	78
View System Plan . . . . .	78
Create System Plan . . . . .	79
Deploy System Plan . . . . .	79
Export System Plan . . . . .	79
Import System Plan . . . . .	80
Remove System Plan . . . . .	80
HMC Management tasks . . . . .	80
HMC Management - Operations . . . . .	80
View HMC Events . . . . .	81
Shut Down or Restart . . . . .	81
Schedule Operations . . . . .	81
Format Media . . . . .	82
Back up HMC Data . . . . .	83
Restore HMC Data . . . . .	83
Save Upgrade Data . . . . .	83
Change Network Settings . . . . .	83
Test Network Connectivity . . . . .	84

View Network Topology . . . . .	85
Tip of the Day . . . . .	85
View Licenses . . . . .	85
Change User Interface Settings . . . . .	86
Change Date and Time . . . . .	86
Launch Guided Setup Wizard . . . . .	86
HMC Management - Administration . . . . .	87
Change User Password . . . . .	87
Manage User Profiles and Access . . . . .	87
Manage Task and Resource Roles . . . . .	88
Manage Users and Tasks . . . . .	89
Manage Certificates. . . . .	89
KDC Configuration. . . . .	90
View KDC Server . . . . .	91
Modify KDC Server . . . . .	91
Add KDC server . . . . .	92
Remove KDC server . . . . .	92
Import Service Key . . . . .	92
Remove Service Key . . . . .	93
Configuring the HMC so that it uses LDAP authentication . . . . .	93
Remote Command Execution . . . . .	94
Remote Virtual Terminal . . . . .	94
Open Restricted Shell Terminal . . . . .	94
Change Language and Locale . . . . .	94
Create Welcome Text . . . . .	95
Manage Data Replication . . . . .	95
Managing Install Resources . . . . .	95
Enhanced password policy . . . . .	97
Managing the Virtual I/O Server image repository . . . . .	98
Service Management tasks . . . . .	98
Create Serviceable Event . . . . .	98
Manage Serviceable Events . . . . .	99
Load Serviceable Events . . . . .	99
Manage Remote Connections . . . . .	99
Manage Remote Support Requests . . . . .	100
Format Media . . . . .	100
Manage Dumps . . . . .	101
Transmit Service Information . . . . .	101
Manage Systems Call-Home . . . . .	101
Manage Outbound Connectivity . . . . .	102
Manage Inbound Connectivity. . . . .	103
Manage Customer Information . . . . .	103
Manage Serviceable Event Notification . . . . .	103
Manage Connection Monitoring . . . . .	104
Call-Home Setup Wizard . . . . .	104
Updates . . . . .	104
Update HMC . . . . .	105
Managed system updates . . . . .	105
Change Licensed Internal Code for the current release. . . . .	106
Upgrade Licensed Internal Code to a new release . . . . .	107
Flash Side Selection . . . . .	108
Check system readiness . . . . .	108
View system information . . . . .	108
Remote operations. . . . .	109
Using a remote HMC. . . . .	109
Using a web browser . . . . .	110
Using the HMC remote command line . . . . .	111
Setting up secure script execution between SSH clients and the HMC. . . . .	111
Enabling and disabling HMC remote commands . . . . .	112
Web browser requirements . . . . .	112
Preparing to use the web browser . . . . .	113



Logging in to the HMC from a LAN-connected web browser . . . . .	113
Customizable data replication . . . . .	113
Peer-to-peer replication . . . . .	114
Master-to-slave replication . . . . .	115
Data replication . . . . .	116
<b>Notices . . . . .</b>	<b>117</b>
Programming interface information . . . . .	118
Trademarks . . . . .	118
Terms and conditions. . . . .	119



---

## Managing the HMC

This topic helps users to understand how to use the Hardware Management Console (HMC), describes the tasks you can use on the console, and describes how to navigate using the web-based user interface.

---

### What's new in Managing the HMC

Read about new or significantly changed information in Managing the HMC since the previous update of this topic collection.

This topic highlights some of the new features and functions on the HMC. For more information, click **HMC Readme** from the HMC workplace Welcome pane.

#### March 2013

The following updates have been made to the content:

- As of Version 7.7, or later, you can install a Virtual I/O Server (VIOS) on a logical partition from an HMC by using a DVD, a saved image, or a Network Installation Management (NIM) server. See the updated Activate topic.
- As of Version 7.7, or later, you can store the VIOS images from a DVD, a saved image, or a Network Installation Management (NIM) server on the HMC. See the new “Managing the Virtual I/O Server image repository” on page 98 topic.
- As of Version 7.7, or later, you can enable the Virtual Server Network (VSN) on POWER7<sup>®</sup> processor-based servers. See the updated “Properties” on page 39 topic.
- The following topics were updated for upgrading the Licensed Internal Code (LIC) by using the HMC:
  - “Change Licensed Internal Code for the current release” on page 106
  - “Upgrade Licensed Internal Code to a new release” on page 107

#### October 2012

The following updates have been made to the content:

- With HMC Version 7.6, or later, you can view the Peripheral Component Interconnect Express (PCIe) hardware topology for the selected POWER7 processor-based servers. The “PCIe Hardware Topology” on page 56 topic was added.
- With HMC Version 7.6, or later, you can set the processing units to the lowest supported value of 0.05 processor per virtual processor. See the updated “Properties” on page 61 topic.
- With HMC Version 7.6, or later, you can restore critical backup data by using a Secure Shell File Transfer Protocol (SFTP) server. See the updated “Restore HMC Data” on page 83 topic.
- HMC Version 7.6 supports Microsoft Internet Explorer 6.0 - Microsoft Internet Explorer 9.0, and Mozilla Firefox Version 4 - Mozilla Firefox Version 10. See the updated “Web browser requirements” on page 112 topic.

#### October 2011

The following updates have been made to the content:

- With HMC Version 7.4, or later, you can enable the Virtual Trusted Platform Module (VTPM) on POWER7 processor-based servers. The “Properties” on page 39 topic was updated for the VTPM feature.

## May 2011

The following updates have been made to the content:

- With the HMC Version 7.2, or later, you can suspend a logical partition with its operating system and applications, and store the virtual server state to persistent storage. You can resume the operation of the logical partition on the same system. The “Suspend operations” on page 66 topic is new for logical partitions with the partition suspend and resume capability.
- With the HMC Version 7.2, or later, the system administrators can set password restrictions by activating the enhanced password policy. You can also create and activate the user-defined policy to set password restrictions. For more information, see “Enhanced password policy” on page 97.

## September 2010

- Added information for the IBM® Power® 710 Express and IBM Power 730 Express (8231-E2B), IBM Power 720 Express (8202-E4B), IBM Power 740 Express (8205-E6B), and IBM Power 795 (9119-FHB) servers.

## February 2010

- Added information for systems servers that contain the POWER7 processor.

---

## Introduction to the HMC

This section briefly describes some of the concepts and functions of the Hardware Management Console (HMC) and introduces the user interface that is used for accessing those functions.

The HMC allows you to configure and manage servers. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To ensure consistent function, each HMC is shipped preinstalled with the HMC Licensed Machine Code Version 7.

To provide flexibility and availability, you can implement HMCs in several configurations.

### HMC as the DHCP server

An HMC that is connected by either a private network to the systems it manages might be a DHCP server for the service processors of the systems. An HMC might also manage a system over an open network, where the managed system's service processor IP address has been assigned by a customer-supplied DHCP server or manually assigned using the Advanced System Management Interface (ASMI).

### Physical proximity

Prior to HMC version 7, at least one local HMC was required to be physically located near the managed systems. This is not a requirement with the Version 7 and the HMC's web browser interface.

### Redundant or Dual HMCs

A server might be managed by either one or two HMCs. When two HMCs manage one system, they are peers, and each can HMC be used to control the managed system. The best practice is to attach one HMC to the service networks or HMC ports of the managed systems. The networks are intended to be independent. Each HMC might be the DHCP server for a service network. Because the networks are independent, the DHCP servers must be set up to provide IP addresses on two unique and nonroutable IP ranges.

## User interface style for the HMC

This HMC uses a web-based user interface. This interface uses a tree style navigation model providing hierarchical views of system resources and tasks to enable direct access to hardware resources and task management capabilities. It provides views of system resources and provides tasks for system administration.

See “Using the web-based user interface” on page 5 for detailed information on how to use this HMC interface.

## Predefined user IDs and passwords

Predefined user IDs and passwords are included with the HMC. It is imperative to your system’s security that you change the hscroot predefined password immediately.

The following predefined user IDs and passwords are included with the HMC:

*Table 1. Predefined HMC user IDs and passwords*

User ID	Password	Purpose
hscroot	abc123	The hscroot user ID and password are used to log in to the HMC for the first time. They are case-sensitive and can only be used by a member of the super administrator role.
root	passw0rd	The root user ID and password are used by the service provider to perform maintenance procedures. They cannot be used to log in to the HMC.

## Tasks and roles

Each HMC user can be a member of a different role. Each of these roles allows the user to access different parts of the HMC and perform different tasks on the managed system. HMC roles are either predefined or customized.

The roles discussed in this section refer to HMC users; operating systems running on logical partitions have their own set of users and roles. When you create an HMC user, you must assign that user a task role. Each task role allows the user varying levels of access to tasks available on the HMC interface. For more information about the tasks each HMC user role can perform, see “HMC tasks, user roles, IDs, and associated commands” on page 15.

You can assign managed systems and logical partitions to individual HMC users. This allows you to create a user that has access to managed system A but not to managed system B. Each grouping of managed resource access is called a managed resource role. To learn more about managed resource roles and how to create them, see “Manage Task and Resource Roles” on page 88.

The **predefined** HMC roles, which are the default on the HMC, are as follows:

*Table 2. Predefined HMC Roles*

Role	Description	HMC User ID
Operator	The operator is responsible for daily system operation.	<b>hmcoperator</b>
Super Administrator	The super administrator acts as the root user, or manager, of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.	<b>hmcsuperadmin</b>

Table 2. Predefined HMC Roles (continued)

Role	Description	HMC User ID
Product Engineer	A product engineer assists in support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.	<b>hmcpe</b>
Service Representative	A service representative is an employee who is at your location to install, configure, or repair the system.	<b>hmcservicerep</b>
Viewer	A viewer can view HMC information, but cannot change any configuration information.	<b>hmcviewer</b>

You can create **customized** HMC roles by modifying predefined HMC roles. Creating customized HMC roles is useful for restricting or granting specific task privileges to a certain user. For more information about creating customized HMC roles, see “Manage Task and Resource Roles” on page 88.

## Starting the HMC

Turn on the HMC by setting both the display and system unit to the *On* position. The initialization window, which includes the copyright information, is displayed. Learn about how to log in to the HMC interface.

When initialization is complete, the pre-login window is displayed.

**Note:** The pre-login window contains the link to log in to the HMC application, the ability to view the online help information, and the summarized status information for the HMC. You will need to log in to view the status information.

To log in to the HMC do the following:

1. In the pre-login window, click **Log on and launch the Hardware Management Console web application**.
2. Enter the user ID and password combination assigned to you.
3. Click **Logon**.

**Note:** If you previously disconnected from your session, the Choose a Disconnected Session window opens. Select the session you want to reconnect to and click **Reconnect**.

After you log in, the HMC workplace window opens and, if enabled, the **Tip of the Day** window appears. For more information about how to enable this feature, see “Tip of the Day” on page 85.

The HMC workplace window allows you to work with tasks for your console and managed systems. Not all tasks are available for each user ID. The user role assigned to your user ID determines what tasks you are able to perform. For example, if you are assigned a user ID with the operator role, you will have access to all the tasks that have *operator* access. See “HMC tasks, user roles, IDs, and associated commands” on page 15 for a listing of all tasks and the user roles for which the tasks are available.

If at any time you do not know or remember what user ID you are currently logged in to the HMC, look at the task bar on the top of the Welcome page or you can click **HMC Management** in the navigation pane. Then click **Manage Users and Tasks** from the work pane (see “Manage Users and Tasks” on page 89 for more information).

---

## Using the web-based user interface

You can use the web-based user interface to perform tasks on the Hardware Management Console (HMC) or on your managed resources.

This user interface comprises several major components: the banner, the taskbar, the navigation pane, the work pane, and the status bar.

The *banner*, across the top of the workplace window, identifies the product and logo. It is optionally displayed. Use the **Change User Interface Settings** task to change the setting.

The *taskbar*, located below the banner, displays the names of any tasks that are running, the user ID you are logged in as, online help information, and the ability to logoff or disconnect from the console.

The *navigation pane*, in the left portion of the window, contains the primary navigation links for managing your system resources and the HMC. The items are referred to as nodes.

The *work pane*, in the right portion of the window, displays information based on the current selection from the navigation pane. For example, when **Welcome** is selected in the navigation pane, the Welcome window content is displayed in the work pane.

The *status bar*, in the bottom left portion of the window, provides visual indicators of current overall system status. It also contains a status overview icon which may be selected to display more detailed status information in the work pane.

You can resize the panes of the HMC workplace by moving the mouse pointer over the border that separates the navigation pane from the work pane until the mouse pointer changes to a double-pointed arrow. When the pointer changes shape, press and hold the left mouse button while dragging the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size. You can also do this within the work pane border that separates the resources table from the taskpad.

## Task bar

The Task bar contains the Help and Logoff tasks and a button that represents each currently running task.

## Navigation pane

The navigation pane contains the primary navigation links for managing your system resources and the HMC.

- “Welcome”
- “Systems Management” on page 6
- “System Plans” on page 11
- “HMC Management” on page 12
- “Service Management” on page 12
- “Updates” on page 12

## Welcome

Welcome is the initial window that is displayed when you log on to the HMC.

The Welcome work pane lists the nodes of the navigation pane and their descriptions. It also includes the following Additional Resources:

## Guided Setup Wizard

Provides a step-by-step process to configure your HMC.

## HMC Operations Guide

Provides an online version of the *Managing the HMC* for system administrators and system operators using the HMC.

If you are accessing the HMC remotely, you can view the publication in PDF format or in HTML format (click **View as HTML**). If you are accessing the HMC locally, you can view the publication in HTML format.

## HMC Readme

Provides hints and errata information about the HMC.

## Online Information

Provides information about the HMC.

**Note:** The following information is only available when you are accessing the HMC remotely.

### IBM System Support

supplies support and technical information for IBM Systems

### HMC Support

supplies support and technical information for the HMC

### Education and Tutorials

supplies course materials for training and updating HMC skills

To see what level of the HMC you are currently using, point your mouse over **HMC Version** at the top of the work pane.

## Systems Management

Systems Management contains a tree view of managed resources.

### Servers:

Servers represents the servers that are managed by this HMC.

To add servers, you can use the **Add Managed System** task under the **Connections** category in the taskpad.

When you click **Servers** from the navigation pane a listing of individually defined servers is displayed in table form in the work pane, and under the **Servers** node in the navigation pane.

*Selecting a server:*

Learn about the information displayed when you select a server.

To perform tasks on a server, click in the **Select** column next to the server name in the work pane table.

To perform tasks on a server's partitions, you can perform one of the following actions:

- Select a server under the **Servers** node from the navigation pane.
- Click on a server name from the work pane table.

When the work pane displays a list of servers, it displays the following attributes by default.

**Name** Specifies the user-defined name of the managed system.

**Status** Displays the current status of the managed system (for example, Operating, Power off, Initializing) and, in addition, displays icons representing an unacceptable state or an active Attention LED. See "Status: Unacceptable" on page 14 or "Status: Attention LEDs" on page 14 for more information.



### **Available Processing Units**

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

### **Available Memory**

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

### **Reference Code**

Displays the system reference codes for the server. Click the reference code in the table for a detailed description.

The Servers work pane table can also display the following optional attributes in the table.

### **Configurable Processing Units**

Displays the number of processors of the managed system.

### **Configurable Memory**

Displays the configurable memory of the managed system.

To show optional attributes, select the **Column configuration** icon on the table toolbar. This function allows you to select additional attributes that you want displayed as columns in the table. It also allows you to reorder the columns, see “Column configuration” on page 14 for more information.

You can also use **Views** from the table toolbar to display the **Default** server attributes in the table or to display the **Capacity On Demand** server attributes in the table. See “Views menu” on page 14 for more information.

### *Displaying server details:*

Display a server's properties.

To display details (properties) about a server, you can select the server by clicking in the **Select** column in the work pane table. Then you can either click **Properties** from the taskpad or click on the double-arrow icon next to the server name and click **Properties** from the context menu. In both cases, the Properties window opens.

### *Launching tasks for managed objects:*

After you have chosen the objects to work with, you are ready to perform the appropriate tasks on them. Learn about how to launch a task for your selected managed objects.

Appropriate tasks for a selected object are listed in the taskpad, in context menus, and in the **Tasks** menu. If a particular task cannot be performed on an object, the task will not display.

## Taskpad

This view contains available tasks for selected managed objects.

The **taskpad** is displayed below the work pane when you have selected an object you want to work with.

### Note:

1. Resize the taskpad by moving the mouse pointer over the border that separates the work pane from the taskpad.
2. Optionally display the taskpad by using the **Change User Interface Settings** task. For more information, see “Change User Interface Settings” on page 86.
3. Expand or collapse all the task categories in the taskpad by selecting **Expand All** or **Collapse All** from the taskpad heading.

The tasks contained in this view meet the following characteristics:

- Tasks are available for the currently selected target objects in the navigation pane or the work pane table view. If multiple objects are selected in the work pane table, the intersection of the selected objects' tasks is displayed. If there are no selections in the table, tasks are displayed for the object selected in the navigation pane.
- Tasks available are limited by the role of the user who is currently logged in.

The following is an example of using the *taskpad* method:

1. Select a server in the work pane table (click the **Select** column).
2. Select a task group from the taskpad (click the expand button or click the group name).

**Note:** After you have expanded the task groups, those groups remain open so that you can repeatedly open other tasks without having to reopen the task groups again.

3. Select a task that is displayed under the task group that you want to perform on that server. The task window opens.

## Context Menu

The **Context menu** lists the task groups appropriate for the selected object. Context menus are available only for table selections. For example, in the **Select** column of the Servers Work pane table, select the object you want to work with. The Context menu button (double right arrows) appears next to the object name you have selected. Click the button and the task groups menu appears for that particular object. Then select a task. If more than one object is selected, the tasks that appear in the Context menu(s) apply to all selections.

## Tasks menu

The tasks menu is displayed on the table toolbar.

The tasks menu is available only for table selections. For example, in the **Select** column of the Servers work pane table, select the object you want to work with. Click **Tasks** for the list of the applicable task groups for the selected objects in the table. Select a task group, then select a task to open for the object. If more than one object is selected, the tasks that are displayed in the tasks menu apply to all selections.

### Partitions:

When you select a managed server in the navigation pane, the work pane displays the list of partitions defined on the server.

The Partitions work pane table displays the following attributes by default:

- Name** Specifies the user-defined name of the logical partition.
- ID** Specifies the ID of the partition
- Status** Displays the current status of the partition (for example, running, not activated) and, in addition, displays icons representing an unacceptable state or active Attention LED. See “Status: Unacceptable” on page 14 or “Status: Attention LEDs” on page 14 for more information.

**Processing Units**

Displays the unit of measure for shared processing power across one or more virtual processors. Processing power can be specified in fractions of a processor.

**Memory**

Specifies the amount of memory allocated to the partition currently. The memory amount can be shown in MB or GB. Click **MB** or **GB** in the Memory column title.

**Active Profile**

Specifies the profile that was used to activate the partition last.

**Environment**

Specifies the type of object, logical partition, server, frame.

**Reference Code**

Displays the system reference codes for the partition. For POWER6® systems, click the reference code in the table for a detailed description.

The Partitions work pane table can also display the following optional attributes in the table.

**Processor**

If the partition is using dedicated processors, this value indicates the number of processors currently allocated to the partition. If the partition is using shared processors, this value represents the virtual processors currently allocated to the partition.

**Service Partition**

Specifies whether the partition has service authority.

**Configured**

Specifies whether a partition is configured with all the required resources to power on.

**Default Profile**

Specifies the profile that is configured as the default profile. When users perform the **Activate** task from the partition, this profile is selected by default.

**OS Version**

Displays the OS version of the managed system.

**Processor Mode**

Specifies whether the partition is using dedicated or shared processors.

**Memory Mode**

Specifies whether the partition is using dedicated or shared memory.

**IPL Source**

Displays the IPL source of the managed system.

Optional attributes can be displayed when you select the **Column configuration** icon on the table toolbar. This function allows you to select additional attributes that you want displayed as columns in the table. It also allows you to reorder the columns, see “Column configuration” on page 14 for more information.

*Displaying partition details:*

Display a partition's properties.

To display details (properties) about a partition you can select the partition by clicking in the **Select** column in the work pane table. Then you can either click **Properties** from the taskpad or click on the double-arrow icon next to the partition name and click **Properties** from the context menu. You can also click on the partition name. In all cases the **Properties** window is displayed.

#### **Frames:**

The **Frames** node identifies the frames managed by this HMC.

Frames typically have dual Bulk Power Controllers (BPCs), however only one BPC is displayed as both BPCs share the same machine type, model, and serial number and function as redundant peers.

The Frames work pane table includes the following attributes:

**Name** Displays the defined name of the Frame.

**Status** Displays the status of the frame object. A frame is in an unacceptable state when it is in **No Connection** or **Incomplete** state. When either of these conditions occurs, a red X is displayed in the status cells next to the status text which identifies the state. Clicking on either the X or the status text opens information describing the unacceptable state and potential remedies.

#### **Frame Number**

Displays the number of the managed frame. You can modify the number.

**Note:** CEC must be powered off to change the frame number.

#### **Connection Status**

Displays connection status of the frame (side A and B).

#### **Custom Groups:**

The **Custom Groups** node provides a mechanism for you to group system resources together in a single view.

Groups may be nested to create custom "topologies" of system resources.

Custom groups include the predefined groups **All Partitions** and **All Objects** and any user-defined groups that you created using the **Manage Custom Groups** task under the **Configuration** category in the taskpad. The **All Partitions** group includes all the partitions defined to all servers managed by the HMC. The **All Objects** group is a collection of all the managed servers, partitions, and frames.

These system-defined groups (All Partitions and All Objects) cannot be deleted. However, if you do not want **All Partitions** or **All Objects** displayed under **Custom Groups**, do the following:

1. Open the **Change User Interface Settings** task from the HMC Management work pane.
2. Deselect **All Partitions node** and **All Objects node** in the **User Interface Settings** window.
3. Click **OK** to save the changes and close the window. Those groups are no longer displayed under **Custom Groups** in the navigation pane.

You can use the **Views** menu on the table toolbar to display your preferred table column configuration. For more information, see "Views menu" on page 14.

#### *User-defined groups:*

Create new groups and manage existing ones.

Click **Manage Custom Groups** task under the Configuration category from the taskpad to create your own group that you want to work with.

To create a group, do the following:

1. Select one or more resources (for example: servers, partitions, frames) that you want to include in the group you want to work with.
2. Click **Manage Custom Groups**.
3. Select **Create a new group**, specify a group name and description, and then click **OK**. The new user-defined group is displayed in the navigation pane under **Custom Groups**.

You can also create a group by using the pattern match method. To use the pattern match method, do the following:

1. Without selecting an object, click **Manage Custom Groups** from the Custom Groups or Systems Management taskpad.
2. From the Create Pattern Match Group window, select one or more group types that you want to create, specify a group name, description, and the pattern used to determine if an object should be part of the group. Click **OK** to complete. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

**Note:** Patterns specified in the **Managed Resource Pattern** input field are regular expressions. For example, if you specified **abc.\***, all the resources that begin with **abc** will be included in that group.

For more information, see “Manage Custom Groups” on page 46.

## System Plans

You can display the plans and the tasks used to deploy system plans to managed systems.

A *system plan* contains a specification of the logical partition configuration of a single managed system. You can also use this node to import, export, and manage the files containing these system plans.

To display the plans and tasks:

1. In the navigation pane, select **System Plans**.
2. In the work pane, select a plan you want to work with by clicking in the **Select** column.
3. From the taskpad, click one of the following tasks:
  - Create System Plan
  - Deploy System Plan
  - Export System Plan
  - Import System Plan
  - Remove System Plan
  - View System Plan

These tasks are described in further detail in “System Plans” on page 46. The table in the work pane displays the system plans that the HMC manages and attributes related to the system plans.

The following attributes are set as the defaults. However, you can select or deselect the attributes that you want displayed in the table by clicking the **Column configuration** icon on the table toolbar. You can also reorder the columns. For more information, see “Column configuration” on page 14.

**Name** Displays the system plan file name.

**Description**  
Specifies a description of the system plan.

**Source**  
Displays how the system plan was created.

**Version**  
Displays version information about the system plan.

### **Last Modified Date**

Specifies the date when the system plan was last modified.

The create and deploy System Plans tasks are also displayed for a server under the **Configuration** task group.

If there are no system plans available when you select **System Plans**, you can create or import a plan from the tasks listed in the taskpad.

### **Related concepts:**

“Managing Install Resources” on page 95

Add or remove operating environment installation resources for your HMC.

## **HMC Management**

HMC Management contains a categorized view of HMC management tasks and their descriptions.

These tasks are used for setting up the HMC, maintaining its internal code, and securing the HMC.

To display the tasks in the work pane, do the following:

1. In the Navigation pane, select **HMC Management**.
2. In the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks is displayed. The categories include:
  - Operations
  - Administration

To see the HMC level you are using, point your mouse over **HMC Version** at the top of the work pane.

If you want an alphabetic listing of the tasks, click **Alphabetical List** in the upper right corner of the work pane. Click **Categorized List** to go back to the task categories.

**Note:** If you are accessing the HMC remotely, some tasks do not display.

HMC Management tasks are described in further detail in “HMC Management tasks” on page 80 and a listing of the tasks and the default user roles that can use them are shown in Table 4 on page 15.

## **Service Management**

Service Management contains a categorized or alphabetic view of tasks and their descriptions used to service the HMC.

To display the tasks in the work pane, do the following:

1. In the Navigation pane, select **Service Management**.
2. In the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks appear. The category is Connectivity.

To see the HMC level you are using, point your mouse over **HMC Version** at the top of the work pane.

If you want an alphabetical listing of the tasks, click **Alphabetical List** in the upper right corner of the work pane. Click **Categorized List** to go back to the task categories.

Service Management tasks are described in further detail in “Service Management tasks” on page 98 and a listing of the tasks and the default user roles that can use them are shown in Table 4 on page 15.

## **Updates**

Updates provides a way for you to access information on both HMC and system firmware code levels at the same time without performing a task.

The **Updates** work pane displays the HMC code level, and system code levels. You can also install corrective service by clicking **Update HMC**.

**Note:** Before performing HMC updates, see “Update HMC” on page 105.

To display the tasks, do the following:

1. In the navigation pane, select **Updates**.
2. Select a managed object.
3. In the taskpad, click the task you want to perform.

These tasks can also be viewed under the **Updates** task group when you are working with managed objects displayed in **Systems Management**.

## Work pane

The work pane displays a table of information based on the current selection in the navigation pane or status bar.

Selecting an object displays a configurable table in the work pane.

## Working with Tables

The tool bar at the top of the table contains buttons used to select, filter, sort, and arrange the entries in the table.

Hovering over the toolbar buttons displays their functions. The toolbar also includes menus that are used with the information displayed in the tables. For more information, see “Tasks menu” on page 8 and “Views menu” on page 14.

### Selecting Rows:

You can select more than one table row at a time.

Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. The **Select All** or **Deselect All** buttons can be used to select or deselect all objects in the table. The table summary at the bottom of the table includes the total number of items that are selected.

### Filtering:

Learn more about how to define a filter for a column to limit the entries displayed in a table.

If you select the **Filter Row** button a row appears under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. Select the **Clear All Filters** button to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

### Sorting:

The Edit Sort and Clear All Sorts buttons are used to perform multi-column sorts of objects in the table in ascending or descending order.

Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order. Click **Clear All Sorts** to return to the default ordering.



## Column configuration:

The column configuration buttons give you the ability to select which columns to display for folders in the Systems Management tree view.

Click the **Configure Columns** button to arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the Columns list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the box next to the column names. The column order is manipulated by clicking on a column name from the list box and using the arrow buttons to the right of the list to change the order of the selected column. When you have completed the configuration of the columns, click **OK**. The columns appear in the table as you specified. If you want to go back to the original layout of the table, click the **Reset Column Order, Visibility, and Widths** button from the table toolbar. Select one or more of the properties you want to reset. Click **OK** to save this setting.

## Views menu:

The Views menu is displayed on the toolbar and is only available for table selections when working with servers, custom groups, exceptions view, or attention LEDs view.

This table option allows you to display different sets of attributes (columns) in the table. You can also change the attributes for each view.

## Status bar

The status bar in the bottom left pane provides a view of overall system status, including managed system resources and the HMC.

A status-sensitive title, background color, and indicator icons are part of the status bar. The status indicators appear in color when one or more objects go into unacceptable status, have attention LEDs, or have open serviceable events. Otherwise, the status icon is not available.

Click any of the individual icons in the status bar to view a listing of resources with specific status. For example, select the Unacceptable icon to view all resources in an unacceptable state. The results are displayed in a table in the work pane.

### Status: Unacceptable

If any managed object is in unacceptable state, the Unacceptable indicator displays on the status bar.

When you select the **Unacceptable** indicator, it displays a table in the work pane of only the objects in an unacceptable state. By clicking on the icon, help information is opened describing the status of the server or partition. You can also use the **Views** menu to display your preferred table column configuration for these objects.

### Status: Attention LEDs

If any managed object's Attention LED is activated, the Attention LED icon displays in the status bar.

When you select the Attention LED icon it displays a table in the work pane of only the objects in Attention LED. A help window opens when you click on the icon. You can also use the **Views** menu to display your preferred table column configuration for these objects.

### Status: Serviceable Events

If at least one serviceable event for the HMC or a managed object is in an open state, the serviceable event icon displays in the status bar.

When you click the icon the **Manage Serviceable Events** window opens. This window displays all open events.



## Status Overview

The Status Overview icon displays a detailed summary of system status in the work pane.

The **Status Overview** icon displays details about any errors, attention LEDs active, or open serviceable events found for the HMC or managed objects. It also summarizes the total number of errors, attention LEDs, and open serviceable events by object type. Object types include the server, partition, frames, and the HMC. When any of these conditions are present, links are available to display all objects with the particular state in the work pane.

---

## HMC tasks, user roles, IDs, and associated commands

The roles discussed in this section refer to HMC users; operating systems running on logical partitions has its own set of users and roles.

Each HMC user has an associated task role and a resource role. The task role defines the operations the user can perform. The resource role defines the systems and partitions for performing the tasks. The users may share task or resource roles. The HMC is installed with five predefined task roles. The single predefined resource role allows access to all resources. The operator can add customized task roles, customized resource roles, and customized user IDs.

Some tasks have an associated command. For more information about accessing the HMC command line, see “Using the HMC remote command line” on page 111.

Some tasks can only be performed using the command line. For a listing of those tasks, see Table 9 on page 37.

For more information about where to find task information, see the following table:

*Table 3. HMC task groupings*

HMC tasks and the corresponding user roles, IDs, and commands	Associated table
HMC Management	Table 4
Service Management	Table 5 on page 19
Systems Management	Table 6 on page 21
Frame Management	Table 7 on page 35
Control Panel Functions	Table 8 on page 36

This table describes the HMC management tasks, commands, and default user roles associated with each HMC Management task.

*Table 4. HMC Management tasks, commands, and default user roles*

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Back up HMC Data “Back up HMC Data” on page 83 bkconsdata	X	X		X

Table 4. HMC Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Change Date and Time “Change Date and Time” on page 86 chhmc lshmc	X	X		X
Change Language and Locale “Change Language and Locale” on page 94 chhmc lshmc	X	X	X	X
Change Network Settings “Change Network Settings” on page 83 chhmc lshmc	X	X		X
Change User Interface Settings “Change User Interface Settings” on page 86	X	X	X	X
Change User Password “Change User Password” on page 87 chhmcusr	X	X	X	X
Configure KDC “KDC Configuration” on page 90 chhmc lshmc getfile rmfile		X		
Configure LDAP “Configuring the HMC so that it uses LDAP authentication” on page 93 lshmcldap chhmcldap		X		

Table 4. HMC Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Create Welcome Text “Create Welcome Text” on page 95 chusrta lsusrta	X	X		
Launch Guided Setup Wizard “Launch Guided Setup Wizard” on page 86		X		
Launch Remote Hardware Management Console	X	X	X	X
Lock HMC Screen	X	X	X	X
Logoff or Disconnect	X	X	X	X
Manage Certificates “Manage Certificates” on page 89		X		
Manage Data Replication “Manage Data Replication” on page 95	X	X		
Manage Install Resources “Managing Install Resources” on page 95	X	X		
Manage Task and Resource Roles “Manage Task and Resource Roles” on page 88 chaccfg lsaccfg mkaccfg rmaccfg		X		
Manage User Profiles and Access “Manage User Profiles and Access” on page 87 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		

Table 4. HMC Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Manage Users and Tasks “Manage Users and Tasks” on page 89 lslogon termtask	X	X	X	X
Open 5250 Console	X	X		X
Open Restricted Shell Terminal “Open Restricted Shell Terminal” on page 94	X	X	X	X
Remote Command Execution “Remote Command Execution” on page 94 chhmc lshmc	X	X		X
Remote Operation “Remote operations” on page 109 chhmc lshmc	X	X	X	X
Remote Virtual Terminal “Remote Virtual Terminal” on page 94	X	X		X
Restore HMC Data “Restore HMC Data” on page 83	X	X		X
Save Upgrade Data “Save Upgrade Data” on page 83 saveupgdata	X	X		X
Schedule Operations “Schedule Operations” on page 81	X	X		
Shut Down or Restart “Shut Down or Restart” on page 81 hmcshutdown	X	X		X

Table 4. HMC Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Test Network Connectivity “Test Network Connectivity” on page 84 ping	X	X	X	X
Tip of the Day “Tip of the Day” on page 85	X	X	X	X
View HMC Events “View HMC Events” on page 81 lssvcevents	X	X		X
View Licenses “View Licenses” on page 85	X	X	X	X
View Network Topology “View Network Topology” on page 85	X	X	X	X
Change Default User Interface Settings	X	X	X	X

This table describes the Service Management tasks, commands, and default user roles.

Table 5. Service Management tasks, commands, and default user roles

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Create Serviceable Event “Create Serviceable Event” on page 98		X		X
Manage Serviceable Events “Manage Serviceable Events” on page 99 chsvcevent lssvcevents		X		X
Manage Remote Connections “Manage Remote Connections” on page 99	X	X		X
Manage Remote Support Requests “Manage Remote Support Requests” on page 100	X	X	X	X

Table 5. Service Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Format Media "Format Media" on page 82	X	X		X
Manage Dumps "Manage Dumps" on page 101 dump cpdump getdump lsdump startdump lsfru	X	X		X
Transmit Service Information "Transmit Service Information" on page 101 chsacfg lssacfg	X	X		
Enable Electronic Service Agent "Manage Systems Call-Home" on page 101	X	X		X
Manage Outbound Connectivity "Manage Outbound Connectivity" on page 102	X	X		X
Manage Inbound Connectivity "Manage Inbound Connectivity" on page 103	X	X		X
Manage Customer Information "Manage Customer Information" on page 103	X	X		X
Authorize User		X		
Manage Serviceable Event Notification "Manage Serviceable Event Notification" on page 103 chsacfg lssacfg	X	X		X

Table 5. Service Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles and IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Manage Connection Monitoring “Manage Connection Monitoring” on page 104	X	X	X	X
Electronic Service Agent™ Setup Wizard “Call-Home Setup Wizard” on page 104		X		X

This table describes the Systems Management tasks, commands, and default user roles.

Table 6. Systems Management tasks, commands, and default user roles

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Managed System Properties “Properties” on page 39 lshwres	X	X	X	X
lsled	X	X	X	X
lslparmigr	X	X	X	X
lssyscfg	X	X	X	X
chhwres	X	X	X	X
chsyscfg	X	X	X	X
migrpar	X	X	X	X
optmem	X	X		X
lsmemopt	X	X	X	X
Update Password “Update Password” on page 40 chsyspwd		X		
Change Default Profile “Change Default Profile” on page 62 chsyscfg lssyscfg	X	X		
Change Default User Interface Settings	X	X	X	X
<b>Operations</b>				

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Power On "Power On" on page 41 chsysstate	X	X		X
Power Off "Power Off" on page 41 chsysstate	X	X		X
Activate: Profile "Activate" on page 62 chsysstate	X	X		X
Activate: Current Configuration "Activate" on page 62 chsysstate	X	X		X
Restart "Restart" on page 62 chsysstate	X	X		X
chlpstate	X	X		X
Shut Down "Shut Down" on page 63 chsysstate	X	X		X
chlpstate	X	X		X
Suspend Operations "Suspend operations" on page 66 chlpstate	X	X		
LED Status: Deactivate Attention LED "Manage Attention LED" on page 63 chled	X	X		
LED Status: Identify LED "Manage Attention LED" on page 63	X	X	X	X
LED Status: Test LED "Manage Attention LED" on page 63	X	X	X	X
Schedule Operations "Schedule Operations" on page 63	X	X		



Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Launch Advanced System Management (ASM) “Advanced System Management” on page 44 asmmenu	X	X		X
Utilization Data: Change Sampling Rate “Utilization Data” on page 45 chlpoutil lslpoutil	X	X		X
Utilization Data: View “Utilization Data” on page 45 lslpoutil	X	X	X	X
Rebuild “Rebuild” on page 45 chsysstate	X	X		
Change Password “Change Password” on page 45 chsyspwd		X		
Power Management “Power Management” on page 42 chpwrmgmt lspwrmgmt		X		
Perform VIOS Command “viosrcmd” on page 65 viosrcmd	X	X		X
Delete “Delete” on page 65 rmsyscfg	X	X		X
Mobility: Migrate “Migrate” on page 65 lslparmigr migrlpar	X	X		X

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Mobility: Validate "Validate" on page 66 lsiparmigr migrlpar	X	X		X
Mobility: Recover "Recover" on page 66 lsiparmigr migrlpar	X	X		X
Manage profiles "Manage Profiles" on page 67 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
Launch OS Management "Operations" on page 62	X	X	X	X
<b>Configuration</b>				
Create Logical Partition: AIX® or Linux "Create Logical Partition" on page 45 mksyscfg	X	X		
Create Logical Partition: VIO Server "Create Logical Partition" on page 45 mksyscfg	X	X		
Create Logical Partition: IBM i "Create Logical Partition" on page 45 mksyscfg	X	X		
System Plans: Create "System Plans" on page 46 mksysplan		X		

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
System Plans: Deploy "System Plans" on page 46 deploysysplan		X		
System Plans: Import "System Plans" on page 46 cpsysplan		X		
System Plans: Export "System Plans" on page 46 cpsysplan		X		
System Plans: Remove "System Plans" on page 46 rmsysplan		X		
System Plans: View "System Plans" on page 46		X		
Manage Custom Groups "Manage Custom Groups" on page 46	X	X		X
View Workload Management Groups "View Workload Management Groups" on page 46 lshwres lssyscfg	X	X	X	X
Partition Availability Priority "Partition Availability Priority" on page 46 chsyscfg lssyscfg mksyscfg	X	X		

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcooperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Manage System Profiles “Manage System Profiles” on page 48 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg				
Manage Partition Data: Restore “Manage Partition Data” on page 46 rstprofdata	X	X	X	X
Manage Partition Data: Initialize “Manage Partition Data” on page 46 rstprofdata	X	X		
Manage Partition Data: Backup “Manage Partition Data” on page 46 bkprofdata	X	X		X
Recover Partition Data chsysstate rstprofdata	X	X		X
Manage Partition Data: Delete “Manage Partition Data” on page 46 rmprofdata	X	X		
Save Current Configuration “Save Current Configuration” on page 68 mksyscfg	X	X		
Virtual Resources: Shared Processor Pool Management “Shared processor pool management” on page 48 chhwres lshwres		X		

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Virtual Resources: Shared Memory Pool Management “Shared Memory Pool Management” on page 49 lshwres lsmemdev chhwres		X		
Virtual Resources: Virtual Storage Management “Virtual Storage Management” on page 49		X		
Virtual Resources: Virtual Network Management “Virtual Network Management” on page 49		X		
<b>Connections</b>				
Service Processor Status “Connections” on page 50 lssysconn	X	X	X	X
Reset or Remove Connections “Connections” on page 50 rmsysconn	X	X		
Disconnect Another HMC “Connections” on page 50		X		
Add Managed System “Connections” on page 50 mksysconn	X	X		
<b>Hardware (Information)</b>				
Adapters: Host Channel “Host Channel Adapter (HCA)” on page 55 lshwres	X	X	X	X

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Adapters: Host Ethernet "Host Ethernet Adapter (HEA)" on page 55 chhwres lshwres	X	X	X	X
Adapters: Switch Network Interface "Switch Network Interface" on page 69 lshwres	X	X	X	X
View Hardware Topology "View Hardware Topology" on page 55	X	X	X	X
Virtual I/O Adapters: SCSI "Virtual IO Adapters" on page 69 lshwres	X	X	X	X
Virtual I/O Adapters: Ethernet "Virtual IO Adapters" on page 69 lshwres	X	X	X	X
<b>Dynamic Logical Partitioning</b>				
Processor "Processor" on page 69 chhwres lshwres	X	X		X
Memory "Memory" on page 70 chhwres lshwres	X	X		X
Physical Adapters "Physical Adapters" on page 70 chhwres lshwres	X	X		X

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Virtual Adapter “Virtual Adapter” on page 70 chhwres lshwres	X	X		X
Host Ethernet “Host Ethernet” on page 70 chhwres lshwres	X	X		X
<b>Updates</b>				
Change Licensed Internal Code for the current release “Change Licensed Internal Code for the current release” on page 106 lslic updlic		X		X
Upgrade Licensed Internal Code to a new release “Upgrade Licensed Internal Code to a new release” on page 107 lslic updlic		X		X
Check system readiness “Check system readiness” on page 108 updlic		X		X
View system information “View system information” on page 108 lslic		X		X
Update HMC updhmc lshmc		X		X
<b>Console Window</b>				

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Open Terminal Window “Open Restricted Shell Terminal” on page 94 mkvterm	X	X		X
Close Terminal Connection rmvterm	X	X		X
Open Shared 5250 Console	X	X		X
Open Dedicated 5250 Console	X	X		X
<b>Serviceability</b>				
Manage Serviceable Events “Manage Serviceable Events” on page 99 chsvcevent lssvcevents		X		X
Create Serviceable Event “Create Serviceable Event” on page 98		X		X
Reference Code History “Reference Code History” on page 58 lsrefcode	X	X	X	X
Control Panel Functions: (20) Type, Model, Feature “Control Panel Functions” on page 58 lssyscfg	X	X		
Hardware: Add FRU “Add FRU” on page 58		X		X
Hardware: Add Enclosure “Add Enclosure” on page 58		X		X
Hardware: Exchange FRU “Exchange FRU” on page 58		X		X
Hardware: Remove FRU “Remove FRU” on page 59		X		X
Hardware: Remove Enclosure “Remove Enclosure” on page 59		X		X
Hardware: Power On/Off Unit “Power On/Off IO Unit” on page 59		X		X



Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Manage Dumps “Manage Dumps” on page 59 dump cpdump getdump lsdump startdump lsfru	X	X		X
Collect VPD “Collect VPD” on page 60	X	X	X	X
Edit MTMS “Edit MTMS” on page 60		X		
FSP Failover: Setup “FSP Failover” on page 60 chsyscfg lssyscfg		X		
FSP Failover: Initiate “FSP Failover” on page 60 chsysstate		X		
<b>Capacity on Demand (CoD)</b>				
Enter CoD code “Capacity on Demand” on page 61 chcod		X		
View History Log “Capacity on Demand” on page 61 lscod	X	X	X	X
Processor: View Capacity Settings “Capacity on Demand” on page 61 lscod	X	X	X	X
Processor CUoD: View Code Information “Capacity on Demand” on page 61 lscod	X	X	X	X

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Processor: On/Off CoD: Manage "Capacity on Demand" on page 61 chcod		X		
Processor: On/Off CoD: View Capacity Settings "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: On/Off CoD: View Billing Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: On/Off CoD: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: Trial CoD: Stop "Capacity on Demand" on page 61 chcod		X		
Processor: Trial CoD: View Capacity Settings "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: Trial CoD: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: Reserve CoD: Manage "Capacity on Demand" on page 61 chcod		X		
Processor: Reserve CoD: View Capacity Settings "Capacity on Demand" on page 61 lscod	X	X	X	X

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Processor: Reserve CoD: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: Reserve CoD: View Shared Processor Utilization "Capacity on Demand" on page 61 lscod	X		X	X
PowerVM® (formerly known as Advanced POWER® Virtualization): Enter Activation Code "Capacity on Demand" on page 61 chcod		X		
PowerVM: View History Log "Capacity on Demand" on page 61 lscod	X	X	X	X
PowerVM: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Enterprise Enablement: Enter Activation Code "Capacity on Demand" on page 61 chcod		X		
Enterprise Enablement: View History Log "Capacity on Demand" on page 61 lscod	X	X	X	X
Enterprise Enablement: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Other Advanced Functions: Enter Activation Code "Capacity on Demand" on page 61 chcod		X		

Table 6. Systems Management tasks, commands, and default user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Other Advanced Functions: View History Log "Capacity on Demand" on page 61 lscod	X	X	X	X
Other Advanced Functions: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: Manage "Capacity on Demand" on page 61 chcod		X		
Processor: View Capacity Settings "Capacity on Demand" on page 61 lscod	X	X	X	X
Processor: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X
Memory: Manage "Capacity on Demand" on page 61 chcod		X		
Memory: View Capacity Settings "Capacity on Demand" on page 61 lscod	X	X	X	X
Memory: View Code Information "Capacity on Demand" on page 61 lscod	X	X	X	X

This table describes the Frame Management tasks, commands, and default user roles.

Table 7. Frame management tasks, commands, and user roles

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Properties “Properties” on page 61 chsyscfg lssyscfg	X	X	X	X
Initialize Frame(s) “Initialize Frames” on page 73	X	X		X
Initialize All Frames “Initialize All Frames” on page 74	X	X		X
Power off unowned I/O drawers chsysstate	X	X		X
Launch Frame Advanced System Management (ASM) asmmenu	X	X	X	X
Bulk Power Assembly (BPA) Status “Bulk Power Assembly (BPA) Status” on page 75 lssysconn	X	X	X	X
Reset “Reset” on page 75 rmsysconn	X	X		
View VLAN Network Data	X	X	X	X
<b>Serviceability</b>				
Hardware: Fill and Drain Tool Tasks: Fill and Drain Tool Fill		X		X
Hardware: Fill and Drain Tool Tasks: Fill and Drain Tool Drain		X		X
Hardware: Fill and Drain Tool Tasks: Fill and Drain Tool Fill Node		X		X

Table 7. Frame management tasks, commands, and user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Hardware: Fill and Drain Tool Tasks: Fill and Drain Tool Fill Initial System Fill		X		X
Hardware: Fill and Drain Tool Tasks: Fill and Drain Tool Fill System Top Off		X		X

This table describes the Control Panel Functions tasks, commands, and default user roles.

Table 8. Control Panel Functions tasks, commands, and user roles

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
<b>Serviceability</b>				
(21) Activate Dedicated Service Tools "Control Panel Functions" on page 72 chsysstate	X	X		
(65) Disable Remote Service "Control Panel Functions" on page 72 chsysstate	X	X		
(66) Enable Remote Service "Control Panel Functions" on page 72 chsysstate	X	X		
(67) Disk Unit IOP Reset / Reload "Control Panel Functions" on page 72 chsysstate	X	X		
(68) Concurrent Maintenance Power Off Domain "Control Panel Functions" on page 72	X	X		

Table 8. Control Panel Functions tasks, commands, and user roles (continued)

HMC Interface Tasks and Associated Commands	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
(69) Concurrent Maintenance Power On Domain "Control Panel Functions" on page 72	X	X		
(70) IOP Control Storage Dump "Control Panel Functions" on page 72 chsysstate	X	X		

This table describes the commands that are not associated with an HMC UI task, and defines the default user roles that can perform each command.

Table 9. Command line tasks, associated commands, and user roles

Command line tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Change which encryption is used by the HMC to encrypt the passwords of locally authenticated HMC users, or change which encryptions can be used by the HMC Web UI. chhmcencr		X		
List which encryption is used by the HMC to encrypt the passwords of locally authenticated HMC users, or list which encryptions can be used by the HMC Web UI chhmcfs	X	X	X	
Free up space in HMC file systems chhmcfs	X	X		
List HMC file system information lshmcfs	X	X	X	X
Test for removable media readiness on the HMC ckmedia	X	X		X
Obtain required files for an HMC upgrade from a remote site getupfiles	X	X		X

Table 9. Command line tasks, associated commands, and user roles (continued)

Command line tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Provide screen capture on the HMC hmcwin	X	X	X	X
Log SSH command usage logssh	X	X	X	X
Clear or dump partition configuration data on a managed system lpcfgop		X		
List environmental information for a managed frame, or for systems contained in a managed frame lshwinfo	X	X	X	X
List which HMC owns the lock on a managed frame lslock	X	X	X	X
Force an HMC lock on a managed frame to be released rmlock		X		
List the storage media devices that are available for use on the HMC lsmediadev	X	X	X	X
Manage SSH authentication keys mkauthkeys	X	X	X	X
Monitor HMC subsystems and system resources monhmc	X	X	X	X
Remove the utilization data collected for a managed system from the HMC rmlparutil	X	X		X
Enable users to edit a text file on the HMC in a restricted mode rnvi	X	X	X	X
Restore hardware resources after a DLPAR failure rsthwres		X		
Restore upgrade data on the HMC rstupgdata	X	X		X



Table 9. Command line tasks, associated commands, and user roles (continued)

Command line tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Transfer a file from the HMC to a remote system sendfile	X	X	X	X
chsvc	X	X		X
lssvc	X	X	X	X
chstat	X	X		X
lsstat	X	X	X	X
chpwdpolicy		X		
lspwdpolicy	X	X	X	X
mcpwdpolicy		X		
rmpwdpolicy		X		
expdata		X		

## Systems Management for Servers

Systems Management displays tasks to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions for servers.

To perform these tasks, see “Launching tasks for managed objects” on page 7. The tasks listed in the taskpad change as selections are made in the work area. The context is always listed at the top of the taskpad in the format *Task: Object*. These tasks are listed when a managed system is selected.

### Properties

Displays the selected managed system's properties. This information is useful in system and partition planning and resource allocation.

These properties include the following tabs:

#### General

The **General** tab displays the system's name, serial number, model and type, state, attention led state, service processor version, maximum number of partitions, assigned service partition (if designated), and power off policy information.

#### Processor

The **Processor** tab displays information about the managed system's processors including installed processing units, deconfigured processing units, available processing units, configurable processing units, minimum number of processing units per virtual processor and maximum number of shared processor pools.

#### Memory

The **Memory** tab displays information about the managed system's memory including installed memory, deconfigured memory, available memory, configurable memory, memory region size, current memory available for partition usage, and system firmware current memory. The tab also describes the maximum number of memory pools.

#### I/O

The **I/O** tab displays the physical I/O resources for the managed system. The assignment of I/O slots and partition, the adaptor-type, and the slot LP limit information are displayed. The

physical I/O resources information is grouped by units. Select the link in the **Slot** column to display the physical I/O properties of each resource. Select **I/O Pool** to display all of the I/O pools found in the system and the partitions that are participating in the pools.

### Migration

If your managed system is partition-migration capable, the **Migration** tab displays partition migration information.

### Power-On Parameters

The **Power-On Parameters** tab allows you to change the power-on parameters for the next restart by changing the values in the Next fields. These changes will only be valid for the next managed system restart.

### Capabilities

The **Capabilities** tab displays the runtime capabilities of this server. You can verify that the server supports Virtual Trusted Platform Module (VTPM) and Virtual Server Network (VSN).

### Advanced

The **Advanced** tab displays huge page memory capabilities on the managed system, including available huge page memory, configurable huge page memory, current page size, and current maximum huge page memory. To change memory allocation on systems with huge page table support, set the Requested huge page memory (in pages) field to the desired memory. To change the requested value for huge page memory, the system must be powered off.




The Barrier Synchronization Register (BSR) option displays array information.

The Processor Performance option displays the TurboCore mode and the System Partition Processor Limit (SPPL). You can set the next TurboCore mode and the next SPPL value. The SPPL applies to both dedicated processor partitions and shared processor partitions.

The Memory Mirroring option displays the current mirroring mode and the current system firmware mirroring status. You can set the next mirroring mode. You can also launch the memory optimization tool.

You can view the VTPM settings.

### Related information:

-  [Verifying that the server supports Virtual Trusted Platform Module](#)
-  [Viewing Virtual Trusted Platform Module settings](#)
-  [Verifying that the server supports Virtual Server Network](#)

## Update Password

Use the Update Password task to update HMC access and Advanced System Management Interface (ASMI) passwords on the managed system.

The first time you access a managed system using an HMC, the system prompts you to enter passwords for each of the following:

- Hardware Management Console: HMC access
- Advanced System Management Interface: General
- Advanced System Management Interface: Admin

If you are using an HMC to access the managed system before all required passwords have been set, enter the appropriate password for each password that is presented in the Update Password task.

If another HMC subsequently needs access to this managed system, upon attempting to access this HMC the user is presented with the Update Password Failed Authentication window, which will prompt for the HMC access password you entered.

In the event that the HMC access password changes while you are logged in to the managed system, your HMC will discover that it can no longer authenticate after it attempts to reconnect to that managed system. This will result in a state of *Failed Authentication* for that managed system. You will be required to enter the new password before any actions can be performed.

## Operations

Operations contains the tasks for operating managed systems.

### Power On

Use the **Power On** task to start a managed system.

Choose from the following options to power on your managed system:

**Normal:** Select this option to specify that the HMC uses the current setting for the partition start policy to determine how to power on the managed system. The current setting can be one of the following values:

- **Auto-Start Always:** This option specifies that the HMC power on logical partitions automatically after the managed system powers on. If powering on the managed system is the result of a user action, the HMC starts all partitions that are configured for automatic start up. If powering on the managed system is the result of an automatic recovery process, the HMC starts only those logical partitions that were running at the time the system powered off. This option is always available for selection.
- **Auto-Start for Auto-Recovery:** This option specifies that the HMC power on logical partitions automatically only after the managed system powers on as the result of an automatic recovery process. This option is available for selection only when the firmware for the managed system supports this advanced IPL capability.
- **User-Initiated:** This option specifies that the HMC does not start any logical partitions when the managed system powers on. You must start logical partitions manually on the managed system by using the HMC. This option is available for selection only when the firmware for the managed system supports this advanced IPL capability.

You can set the partition start policy from the Power On Parameters page of the Properties task for the managed system.

**System profile:** Selecting this power-on option specifies that the HMC power on the system and its logical partitions based on a predefined system profile. When you select this power-on option, you must select the partition profile that you want the HMC to use to activate logical partitions on the managed system.

**Hardware Discovery:** Selecting this power-on option specifies that the HMC run the hardware discovery process when the managed system powers on. The hardware discovery process captures information about all I/O devices -- in particular those devices not currently assigned to partitions. When you select the hardware discovery power on option for a managed system, the managed system is powered on into a special mode which performs the hardware discovery. After the Hardware Discovery process is complete, the system will be in Operating state with any partitions in the power-off state. The Hardware Discovery process records the hardware inventory in a cache on the managed system. The collected information is then available for use when displaying data for I/O devices or when creating a system plan based on the managed system. This option is available only if the system is capable of using the hardware discovery process to capture I/O hardware inventory for the managed system.

### Power Off

Shut down the managed system. Powering off the managed system will make all partitions unavailable until the system is again powered on.

Before you power off the managed system, ensure that all logical partitions have been shut down and that their states have changed from Running to Not Activated. For more information on shutting down a logical partition, see "Shut Down" on page 63

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

Choose from the following options:

#### **Normal power off**

The Normal power off mode shuts down the system's operations in a controlled manner. During the shutdown, programs running active jobs are allowed to perform cleanup (end-of-job processing).

#### **Fast power off**

The Fast power off mode shuts down the system by stopping all active jobs immediately. The programs running those jobs are not allowed to perform any cleanup. Use this option when you need to shut down the system because of an urgent or critical situation.

## **Power Management**

You can reduce the managed system's processor power consumption by enabling power saver mode.

### **About this task**

To enable power saver mode, do the following:

#### **Procedure**

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server that you want to enable to use power saver mode.
4. In the tasks area, expand **Operations**.
5. Click **Power Management**.
6. Select your desired power saver mode, and click **OK**.

## **LED Status**

View system attention LED information, light specific LEDs to identify a system component, and test all LEDs on a managed system.

The system provides several LEDs that help identify various components, such as enclosures or field replaceable units (FRUs), in the system. For this reason, they are called *Identify* LEDs. Individual LEDs are located on or near the components. The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, or processor). LEDs are either green or amber. Green LEDs indicate either of the following:

- Electrical power is present.
- Activity is occurring on a link. (The system could be sending or receiving information.)

Amber LEDs indicate a fault or identify condition. If your system or one of the components on your system has an amber LED turned on or blinking, identify the problem and take the appropriate action to restore the system to normal.

You can activate or deactivate the following types of identify LEDs:

#### **Identify LED for an enclosure**

If you want to add an adapter to a specific drawer (enclosure), you need to know the machine type, model, and serial number (MTMS) of the drawer. To determine whether you have the correct MTMS for the drawer that needs the new adapter, you can activate the LED for a drawer and verify that the MTMS corresponds to the drawer that requires the new adapter.

### **Identify LED for a FRU associated with a specified enclosure**

If you want to attach a cable to a specific I/O adapter, you can activate the LED for the adapter that is a field replaceable unit (FRU), and then physically verify where to attach the cable. This can be especially useful when you have several adapters with open ports.

You can deactivate a system attention LED or a logical partition LED. For example, you might determine that a problem is not a high priority and decide to repair the problem at a later time. However, you want to be alerted if another problem occurs, so you must deactivate the system attention LED so that it can be activated again if another problem occurs.

Choose from the following options:

#### **Identify LED**

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

#### **Test LED**

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

### **Schedule Operations**

Create a schedule for certain operations to be performed on the managed system without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule power on or off operations for a managed system.

The Scheduled Operations task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the Scheduled Operations window you can do the following:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

You can schedule an operation to occur once or you can schedule it to repeat. You must provide the time and date that you want the operation to occur. If the you want the operation to repeat, you will be asked to select the following:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that you can schedule for the managed system include the following:

#### **Activate on a System Profile**

Schedules an operation on a selected system for scheduling activation of a selected system profile.

**Backup Profile Data**

Schedules an operation to back up profile data for a managed system

**Power Off Managed System**

Schedules an operation for a system power off at regular intervals for a managed system.

**Power On Managed System**

Schedules an operation for a system power on at regular intervals for a managed system.

**Manage Utility CoD processors**

Schedules an operation for managing how your Utility CoD processors are used.

**Manage Utility CoD processor minute usage limit**

Creates a limit for Utility CoD processor usage.

**Modify a Shared Processor Pool**

Schedules an operation for modifying a shared processor pool.

**Move a partition to a different pool**

Schedules an operation for moving a partition to a different processor pool.

**Change power saver mode on a managed system**

Schedules an operation for changing a managed system's power saver mode.

To schedule operations on the managed system, do the following:

1. In the Navigation area, click **Systems Management**.
2. In the Navigation area, click **Servers**.
3. In the work pane, select one or more managed systems.
4. In the taskpad, select the **Operations** task category, then click **Schedule Operations**. The Customize Scheduled Operations window opens.
5. From the Customize Scheduled Operations window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, click **Options** and then click **New**.
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**
  - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**
  - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
6. To return to the HMC workplace, point to **Operations** and then click **Exit**.

**Advanced System Management**

The HMC can connect directly to the Advanced System Management (ASM) interface for a selected system.

ASM is an interface to the service processor that allows you to manage the operation of the server, such as auto power restart, and to view information about the server, such as the error log and vital product data.

To connect to the Advanced System Management interface, do the following:

1. From the **System Management** tasks list, select **Operations**.
2. From the **Operations** task list, select **Advanced System Management (ASM)**.



## Utilization Data

You can set the HMC to collect resource utilization data for a specific managed system or for all systems the HMC manages.

The HMC collects utilization data for memory and processor resources. You can use this data to analyze trends and make resource adjustments. The data is collected into records called events. Events are created at the following times:

- At periodic intervals (30 seconds, 1 minute, 5 minutes, 30 minutes, hourly, daily, and monthly)
- When you make system-level and partition-level state and configuration changes that affect resource utilization
- When you start up, shut down, and change the local time on the HMC

You must set the HMC to collect utilization data for a managed system before utilization data can display for the managed system.

Use the **Change Sampling Rate** task to enable, set and change the sampling rate, or disable sampling collection.

## Rebuild

You can extract the configuration information from the managed system and rebuild the information on the Hardware Management Console (HMC).

This task does not disrupt the operation of the running server.

Rebuilding the managed system updates the information on the HMC about the managed system. Rebuilding the managed system is useful when the state of the managed system is *Incomplete*. The *Incomplete* state means that the HMC cannot gather complete information from the managed system about logical partitions, profiles, or resources.

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

## Change Password

Change the HMC access password on the selected managed system

After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed system.

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

## Configuration

Configuration contains the tasks for configuring your managed system and partitions.

### Create Logical Partition

Access the LPAR Wizard to create a new logical partition (LPAR) on your managed system.

Ensure you have logical partition planning information before you use this wizard. Logical partition planning information can be found at the System Planning Tool (SPT) Web site: <http://www.ibm.com/systems/support/tools/systemplanningtool/>. The SPT is available to assist you in system planning, design, validation and to provide a system validation report that reflects your system requirements while not exceeding system recommendations.

For more information about creating logical partitions, see *Logical Partitioning*.

## System Plans

Record or import specifications for logical partitions, partition profiles, or hardware specifications on a chosen system.

A *system plan* is a specification of the logical partition configuration of a single managed system. A system plan is stored in a file that is called a *system-plan* file and has a file suffix of *.sysplan*. A system-plan file can contain more than one system plan, although multiple plans in a single file are not common.

The **System Plans** tasks creates a record of the hardware and partition configuration of a managed system at a given time. It records specifications for the logical partitions and partition profiles on the selected system. It can also record hardware specifications that the HMC is able to detect.

To maximize the information that the HMC can obtain from the managed system, power on the managed system and activate the logical partitions on the managed system before creating the new system plan.

The **System Plans** tasks are the same tasks that are available from the **System Plans** node from the navigation pane and are documented here: “System Plans” on page 78.

## Partition Availability Priority

Use this task to specify the partition-availability priority of each logical partition on this managed system.

The managed system uses partition-availability priorities in the case of processor failure. If a processor fails on a logical partition, and there are no unassigned processors available on the managed system, the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. This allows the logical partition with the higher partition-availability priority to continue running after a processor failure.

You can change the partition availability priority for a partition by selecting a partition and choosing an availability priority from those listed.

Use the online Help if you need additional information about prioritizing partitions.

## View Workload Management Groups

Display a detailed view of the workload management groups you have specified for this managed system.

Each group displays the total number of processors, processing units for partitions using shared mode processing, and the total amount of memory allocated to the partitions in the group.

## Manage Custom Groups

You can report status on a group basis, allowing you to monitor your system in a way that you prefer.

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

One or more user-defined groups might already be defined on your HMC. Default groups are listed under **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

## Manage Partition Data

A partition profile is a record on the HMC that specifies a possible configuration for a logical partition. When you activate a partition profile, the managed system attempts to start the logical partition using the configuration information in the partition profile.



A partition profile specifies the desired system resources for the logical partition and the minimum and maximum amounts of system resources that the logical partition can have. The system resources specified within a partition profile includes processors, memory, and I/O resources. The partition profile can also specify certain operating settings for the logical partition. For example, you can set a partition profile so that, when the partition profile is activated, the logical partition is set to start automatically the next time that you power on the managed system.

Each logical partition on a managed system that is managed by an HMC has at least one partition profile. You can create additional partition profiles with different resource specifications for your logical partition. If you create multiple partition profiles, you can designate any partition profile on the logical partition to be the default partition profile. The HMC activates the default profile if you do not select a specific partition profile to be activated. Only one partition profile can be active at one time. To activate another partition profile for a logical partition, you must shut down the logical partition before you activate the other partition profile.

A partition profile is identified by partition ID and profile name. Partition IDs are whole numbers used to identify each logical partition that you create on a managed system, and profile names identify the partition profiles that you create for each logical partition. Each partition profile on a logical partition must have a unique profile name, but you can use a profile name for different logical partitions on a single managed system. For example, logical partition 1 cannot have more than one partition profile with a profile name of normal, but you can create a profile named normal for each logical partition on the managed system.

When you create a partition profile, the HMC shows you all of the resources available on your system. The HMC does not verify if another partition profile is currently using a portion of these resources. Therefore, it is possible for you to overcommit resources. When you activate a profile, the system attempts to allocate the resources that you assigned to the profile. If you have overcommitted resources, the partition profile will not be activated.

For example, you have four processors on your managed system. Partition 1 profile A has three processors, and partition 2 profile B has two processors. If you attempt to activate both of these partition profiles at the same time, partition 2 profile B will fail to activate because you have overcommitted processor resources.

When you shut down a logical partition and reactivate the logical partition using a partition profile, the partition profile overlays the resource specifications of the logical partition with the resource specifications in the partition profile. Any resource changes that you made to the logical partition using dynamic logical partitioning are lost when you reactivate the logical partition using a partition profile. This is desirable when you want to undo dynamic logical partitioning changes to the logical partition. However, this is not desirable if you want to reactivate the logical partition using the resource specifications that the logical partition had when you shut down the managed system. Therefore, keep your partition profiles up to date with the latest resource specifications. You can save the current configuration of the logical partition as a partition profile. This allows you to avoid having to change partition profiles manually.

If you shut down a logical partition whose partition profiles are not up to date, and the logical partition is set to start automatically when the managed system starts, you can preserve the resource specifications on that logical partition by restarting the entire managed system using the partition autostart power-on mode. When the logical partitions start automatically, the logical partitions have the resource specifications that the logical partitions had when you shut down the managed system.

Use the Manage Partition Data tasks to do the following:

- Restore partition data. If you lose partition profile data, use the restore task in one of three ways:
  - Restore partition data from a backup file. Profile modifications performed after the selected backup file was created will be lost.

- Restore merged data from your backup file and recent profile activity. The data in the backup file takes priority over recent profile activity if the information conflicts.
- Restore merged data from recent profile activity and your backup file. The data from recent profile activity takes priority over your backup file if the information conflicts.
- Initialize partition data. Initializing the partition data for a managed system will delete all of the currently defined system profiles, partitions, and partition profiles.
- Backup a partition profile to a file.
- Backup partition data to a file.

Use the online Help if you need additional information about managing partition data.

## Manage System Profiles

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

When you activate the system profile, the managed system attempts to activate each partition profile in the system profile in the order specified. A system profile helps you activate or change the managed system from one complete set of logical partition configurations to another.

You can create a system profile that has a partition profile that has overcommitted resources. You can use the HMC to validate the system profile against the currently available system resources and against the total system resources. Validating your system profile ensures that your I/O devices and processing resources are not overcommitted, and it increases the likelihood that the system profile can be activated. The validation process estimates the amount of memory needed to activate all of the partition profiles in the system profile. It is possible that a system profile can pass validation and yet not have enough memory to be activated.

Use this task to do the following:

- Create new system profiles.
- Create a copy of a system profile.
- Validate the resources specified in the system profile against the resources available on the managed system. The validation process indicates whether any of the logical partitions in the system profile are already active and whether the uncommitted resources on the managed system can meet the minimum resources specified in the partition profile.
- View the properties of a system profile. From this task, you can view or change an existing system profile.
- Delete a system profile.
- Activate a system profile. When you activate a system profile, the managed system will attempt to activate the partition profiles in the order specified in the system profile.

Use the online Help if you need additional information about managing system profiles.

## Virtual Resources

Manage shared processor pools, shared memory pools, virtual storage, and virtual networks.

### Shared processor pool management:

You can assign a specific amount of the processing capacity in a shared processor pool to each logical partition that uses shared processors.

Shared processors are physical processors whose processing capacity is shared among multiple logical partitions. By default, all physical processors that are not dedicated to specific logical partitions are grouped together in a *shared processor pool*. This task allows you to view information about your shared processor pool and to make changes to that pool.

Detailed information about configuring shared processor pools is available. For more information, see *Configuring shared processor pools using the HMC version 7 release 3.2.0, or later.*

## Shared Memory Pool Management

Use the Create/Modify Shared Memory Pool wizard to configure a shared memory pool.

### Before you begin

The Create/Modify Shared Memory Pool wizard is only available when the managed system supports the use of *Active Memory™ Sharing*. Active Memory Sharing is a feature that enables you to assign physical memory to a shared memory pool and share that memory among multiple logical partitions.

### About this task

To create or modify a shared memory pool between partitions, do the following:

#### Procedure

1. In the Navigation area, click **Systems Management**.
2. In the Navigation area, click **Servers**.
3. In the work pane, select one or more managed systems.
4. In the taskpad, select the **Operations** task category, then click **Virtual Resources**.
5. Click **Shared Memory Pool Management**. The Create/Modify Shared Memory Pool wizard opens.
6. Complete the steps in the wizard to perform your task.

## Virtual Storage Management

You can create and manage the virtual disks, storage pools, physical volumes, and optical devices in your managed system using the Virtual Storage Management task.

### Before you begin

A single storage pool is created automatically when you install Virtual I/O Server. This storage pool is usually called rootvg.

### About this task

To manage the storage capability of your managed system, do the following:

#### Procedure

1. In the Navigation area, click **Systems Management**.
2. In the Navigation area, click **Servers**.
3. In the work pane, select one or more managed systems.
4. In the contents area, select the VIOS partition for which you want to manage storage details.
5. In the taskpad, select the **Operations** task category, then click **Virtual Resources**.
6. Click **Virtual Storage Management**.

## Virtual Network Management

You can view the state of all the virtual networks on the managed system using the Virtual Network Management task.

### About this task

To view information about the virtual networks on the managed system, do the following:

## Procedure

1. In the Navigation area, click **Systems Management**.
2. In the Navigation area, click **Servers**.
3. In the work pane, select one or more managed systems.
4. In the taskpad, select the **Operations** task category, then click **Virtual Resources**.
5. Click **Virtual Network Management**.

## Connections

You can view the HMC connection status to service processors or frames, reset those connections, connect another HMC to the selected managed system, or disconnect another HMC.

If you have selected a managed system in the work area, the following tasks pertain to that managed system. If you have selected a frame, the tasks pertain to that frame.

### View service processor connection status

View information about the status of the HMC connection to the service processors on the managed system.

#### About this task

To show the service processor connection status to the service processors on the managed system, do the following:

#### Procedure

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server for which you want to view service processor connection status.
4. In the tasks area, expand **Connections**.
5. Select **Service Processor Status**.

### Resetting or removing connections

Reset or remove a managed system from the HMC interface.

#### About this task

To reset or remove connections, do the following:

#### Procedure

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server that you want to reset or remove.
4. In the tasks area, expand **Connections**.
5. Select **Reset or Remove Connections**.
6. Select an option and click **OK**.

### Disconnecting another HMC

You can disconnect a connection between a selected HMC and the managed server.

#### About this task

To disconnect another HMC, do the following:

## Procedure

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server for which you want to disconnect another HMC.
4. In the tasks area, expand **Connections**.
5. Select **Disconnect another HMC**.
6. Select an HMC from the list and click **OK**.

## Adding a managed system

Add systems in the network to the list of systems managed by this HMC.

### About this task

Before you begin, you must assign an IP address or host name to the service processor on the managed system. You can manually assign an IP address to the service processor by using the Advanced System Management Interface (ASMI), or you can use a Dynamic Host Configuration Protocol (DHCP) server on the open network to assign an IP address to the service processor. If you want to reuse an IP address that was previously used by the service processor of a different managed system, ensure that you remove the connection to the other managed system from the Contents area of the HMC before you use this window to add the new managed system. You can remove the connection to the other managed system by using the Reset or Remove Connection task.

You can add a managed system either by entering the IP address or host name or by searching a range of IP addresses. If you enter a range of IP addresses, the HMC searches the range of IP addresses and displays the managed systems that it finds within that range. You can then select the managed systems to which you want to connect.

If you enter the IP address or host name for a specific managed system, you can also enter the password for that managed system here. The HMC stores the password so that the HMC does not need to prompt you for the password when you work with the managed system.

To add managed systems in the network to the list of systems managed by this HMC, do the following:

## Procedure

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server.
4. In the tasks area, expand **Connections**.
5. Select **Add Managed System**.
6. Select an option, enter the required IP address information, and click **OK**.

## Correcting a connection problem

To correct a connection problem between the HMC and the managed system or to correct the state of a managed system in *No Connection*, *Incomplete*, *Recovery*, *Error*, or *Failed Authentication* state, follow the procedures below.

### Correcting a No connection state for a managed system:

The **No connection** state can occur when the HMC is not connected, or the handshake with the managed system failed.

Use this procedure for a system that was previously connected to the same HMC and is now in No connection state. If you have a new system, a new HMC, or have moved your system to a different HMC, refer to Correcting a connection problem between the HMC and a managed system.

1. From the **Systems Management - Servers** work pane, select the managed system.
2. Select **Connections - Service Processor Status**. Record the IP address of the service processor.
3. From the **HMC Management** work pane, select **Test Network Connectivity**.
4. Enter the IP address of the service processor and select **Ping**.
5. Choose from the following options:
  - If the ping is successful, go to step 6.
  - If the ping is not successful, go to step 7.
6. If the ping test is successful, perform the following steps:
  - a. In the **Systems Management - Servers** work pane, ensure that there are no reference codes displayed in the **Reference Code** column for the server in No Connection state. **Note:** A steady reference code could indicate a hardware problem. If the reference code is a clickable link, click the reference code to display possible procedures to correct the problem. If the reference code is not a link or a solution is not presented, contact your next level of support or your hardware service provider.
  - b. Restart the HMC. For more information on restarting the HMC, see “Shut Down or Restart” on page 81.
  - c. If restarting the HMC does not resolve the problem, contact your next level of support or your hardware service provider.
7. If the ping test is not successful, perform the following steps:
  - a. In the **Systems Management - Servers** work pane, ensure that there are no reference codes displayed in the **Reference Code** column for the server in No Connection state. **Note:** A steady reference code could indicate a hardware problem. If the reference code is a clickable link, click the reference code to display possible procedures to correct the problem. If the reference code is not a link or a solution is not presented, contact your next level of support or your hardware service provider.
  - b. If your system has a control panel, check to see if the power light is on. Choose from the following options:
    - If there is power to the managed system, go to step 8.
    - If there is no power to the managed system, “Power On” on page 41 the managed system. After the power is restored, wait 5 minutes for the service processor to re-IPL and the HMC to re-establish contact. If the system is equipped with redundant service processors, allow up to 20 minutes for this step.
8. Verify physical network connectivity:
  - a. Verify that the HMC and the service processor are correctly connected to your Ethernet network.
  - b. Verify that Ethernet link status is good on all network segments which exist between the HMC and the managed system.
  - c. If you think the network might be the problem, connect a cable from the HMC to the service processor and try pinging the failing system. Then choose from the following options:
    - If the ping is successful, put the cables back the way they were and correct the network problem. After the network problem is resolved, repeat this entire procedure.
    - If the ping is not successful, put the cables back the way they were and continue with step 8.d.
  - d. Reset the service processor using the following steps:
    - 1) “Power Off” on page 41 the server.
    - 2) Unplug the AC power cord and re-plug it back in.
    - 3) “Power On” on page 41 the server.

9. If the problem is not resolved by any of the above steps, contact your next level of support or your hardware service provider.

#### **Correcting an Incomplete state for a managed system:**

The **Incomplete** state can occur when the HMC failed to get all of the necessary information from the managed system.

To correct an **Incomplete** state, perform the following steps:

1. From the **Systems Management - Servers** work pane, select the managed system.
2. In the taskpad, select **Operations - Rebuild**.
3. Select **Yes** to refresh the internal representation of the managed system on the HMC.
  - If the state remains **Incomplete**, rebuild the managed system several more times
  - If the state goes to **Recovery**, see “Correcting a Recovery state for a managed system.”
  - If the state remains in **Incomplete** or goes to **Recovery**, continue with the next step.
4. In the taskpad, select **Connections - Reset or Remove Connections** to reset the connection from the managed system to the HMC. If this fails, continue to the next step.
5. Restart the HMC. For more information on restarting the HMC, see “Shut Down or Restart” on page 81.
  - If the state goes to **Recovery**, see “Correcting a Recovery state for a managed system.”
  - If the state remains **Incomplete**, perform the following steps:
    - Verify that there is a redundant HMC.
    - Verify that no one is entering commands from the alternate HMC.
    - Repeat step 1 through 5. If it still fails, continue with the next step.
6. If the problem persists, contact your next level of support or your hardware service provider.

#### **Correcting a Recovery state for a managed system:**

The **Recovery** state can occur when the save area in the service processor assembly is not synchronized with the HMC.

To recover from the **Recovery** state, perform the following steps:

1. Restore partition data. For details, see the **Recover** task in “Manage Partition Data” on page 46. If this solves the problem, this ends the procedure.
2. If the problem is not resolved after restoring partition data, choose the option that describes what happened:
  - If the state remains **Recovery**, retry restoring partition data. If it fails a second time, follow the problem determination procedure for any reference codes you receive.
  - If the state changed to **Incomplete**, see “Correcting an Incomplete state for a managed system.”
  - If the state changed to **No Connection**, see “Correcting a No connection state for a managed system” on page 51.
3. If the problem persists, contact your next level of support or your hardware service provider.

#### **Correcting an Error state for a managed system:**

The **Error** state automatically generates a call to the service support center if the function is enabled.

If the automatic call support function is not enabled, contact your next level of support or your hardware service provider.

#### **Correcting a Failed Authentication state for a managed system:**



The **Failed Authentication** state can occur when the HMC access password for the managed system is not valid.

1. Do you have an HMC password?
  - **Yes:** Enter the HMC password and choose from the following options:
    - If the managed system goes to **Operating, Power Off, or Standby** state, the authentication was successful. This ends the procedure.
    - If the managed system goes to **No connection, Incomplete, Recovery, or Error** state, refer to Correcting the managed system operating state.
  - **No:** Do you have an ASMI admin password?
    - **Yes:** Continue with step 2.
    - **No:** Contact your next level of support to request CE login. Then continue with step 2, using CE login instead of admin password for step 2.a.
2. Perform the following steps:
  - a. Login to the ASMI with admin authority. See “Advanced System Management” on page 44.
  - b. Select **Login Profile**.
  - c. Select **Change Password**.
  - d. In the **User ID to change field**, select **HMC**.
  - e. Enter the ASMI's admin password in the **Current password for user ID admin** field. **Note:** Do not enter the HMC user password.
  - f. Enter the ASMI's admin password.
  - g. Enter a new HMC access password twice and click **Continue**.
  - h. From the **Systems Management - Servers** work pane, select the managed system.
  - i. Select **Update password**.
  - j. Enter the new password that was set in step 2.g. This ends the procedure.

### **Correcting a new connection problem between the HMC and a managed system:**

Use this procedure if you have a new HMC, a new managed system, or have moved your managed system to a different HMC.

If your system was previously connected to the same HMC and is now in **No connection** state, refer to “Correcting a No connection state for a managed system” on page 51.

1. From the **Systems Management - Servers** work pane, select **Connections - Add Managed System** from the taskpad. For more information, see “Connections” on page 50. Does the system appear in the work pane?
  - **Yes:** This ends the procedure.
  - **No:** Continue with step 2.
2. Check for network problems, cables, switches, link lights on the service processor, and so on. Was there a problem?
  - **Yes:** Correct the problem and return to step 1.
  - **No:** Continue with step 3.
3. Reset the service processor to force it to request a new IP address using the following steps:
  - a. “Power Off” on page 41 the server.
  - b. Unplug the AC power cord and re-plug it back in.
  - c. “Power On” on page 41 the server.
4. Did resetting the service processor resolve the problem?
  - **Yes:** This ends the procedure.
  - **No:** Contact your next level of support.



## Hardware Information

Display information about the hardware attached to a selected managed system.

### Adapters

View information about the Host Ethernet Adapters (HEA, also referred to as Integrated Virtual Ethernet adapters) or Host Channel Adapters (HCA) for a selected managed system.

**Related information:**

 [Host Ethernet Adapter](#)

### Host Channel Adapter (HCA):

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

You can show a list of the HCAs for the managed system. You can select an HCA from the list to display the current partition usage for the HCA.

From this task you can display the following:

- The physical location of each HCA on the managed system.
- The number of globally unique identifiers (GUIDs) that are in use on each HCA.
- The number of GUIDs on each HCA that are available to be assigned to logical partitions.
- HMC management status. HCAs that are unable to be managed by an HMC are in an error state.
- The logical partition usage for a selected HCA.

### Host Ethernet Adapter (HEA):

A Host Ethernet Adapter (HEA) allows multiple logical partitions to share a single physical Ethernet adapter.

Unlike most other types of I/O devices, you can never assign the HEA itself to a logical partition. Instead, multiple logical partitions can connect directly to the HEA and use the HEA resources. This allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge on another logical partition.

Use the **Host Ethernet** task to display the ports of the physical HEAs on a selected managed system.

### View Hardware Topology

Display the current hardware topology for the selected managed system and any discrepancies between the current topology and the last valid topology.

High Speed Link (HSL), also known as Remote I/O (RIO), resources provide the connection between system I/O busses and the system processor. HSL/RIO resources are normally configured in loops with the system unit having an HSL/RIO controller resource that handles routing of the data between the system processor and the system I/O busses. System I/O busses connect to the loop with HSL I/O adapter or RIO adapter resources.

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

- The starting location of the physical RIO cable and the RIO connection (cable to port)
- The ending location of the physical RIO cable and the RIO connection (cable to port)

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

To view the current hardware topology and the last valid hardware topology, do the following:

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server.
4. In the tasks area, expand **Hardware Information**.
5. Click **View Hardware Topology**.

## PCIe Hardware Topology

Display information about the Peripheral Component Interconnect Express (PCIe) links that exist for each CEC that is attached to a solid-state drive (SSD) drawer.

The PCIe hardware topology can be viewed only for POWER7 and later processor-based systems. The PCIe hardware topology option is either not available for the earlier firmware systems or an error message is displayed when you click the PCIe hardware topology link.

**Note:** The CEC must be in the operating or standby state to view the PCIe topology. For other states, the PCIe hardware topology option is not available.

To view the PCIe hardware topology, complete the following steps:

1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server.
4. In the tasks area, expand **Hardware Information**.
5. Click **PCIe Hardware Topology**.

## Updates

Perform a guided update of managed system, power, or I/O Licensed Internal Code.

These **Update** tasks are the same tasks that are available from the Updates node of the navigation pane and are documented here: “Managed system updates” on page 105.

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it.

These problems are reported to you as serviceable events. Use the **Manage Events** task to view specific events for selected systems. However, if you notice a problem occurred or you suspect a problem is affecting the system but Problem Analysis has not reported it to you, use the **Create Serviceable Event** task to report the problem to your service provider.

## Manage Serviceable Events

Problems on your managed system are reported to the HMC as serviceable events. You can view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you to view, do the following:

1. From the taskpad, open **Manage Serviceable Events**.
2. Provide event criteria, error criteria, and FRU criteria.
3. Click **OK**.
4. If you do not want the results filtered, select **ALL**.

The Serviceable Events Overview window displays all of the events that match your criteria. The information displayed in the compact table view includes the following:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and use the **Selected** drop down menu to:

- **View event details:** Field-replaceable units (FRUs) associated with this event and their descriptions.
- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Create Serviceable Event

Use this task to report a problem on your managed system to your service provider or to test problem reporting on your managed system.

Submitting a problem is dependent upon whether you have customized your HMC to use the Remote Support Facility (RSF) and if it is authorized to automatically call for service. If so, the problem information and service request is sent to the service provider automatically with a modem transmission.

To report a problem on your managed system:

1. Open the **Create Serviceable Event** task from the Service Management work pane.
2. From the **Report a Problem** window, enter a brief description of your problem in the **Problem Description** input field and then click **Request Service**.

To test problem reporting from the **Report a Problem** window:

1. Select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** input field.
2. Click **Request Service**.

The problems are reported to the service provider for the managed system. Reporting a problem sends to the service provider the information you provide on the **Report a Problem** window, and machine information that identifies the console.

Use the online Help if you need additional information for reporting a problem or testing if problem reporting works.

## Reference Code History

Reference codes provide general diagnostic, troubleshooting, and debugging information.

The most recent reference codes are displayed. To view a history of reference codes, enter the number of codes to retrieve from the history and select **Go**. If detailed information is available on the managed system you are viewing, select the desired reference code to view the details of a specific reference code.

## Control Panel Functions

Learn more about how to display the available virtual control panel functions for the managed system.

**(20) Type, Model, Feature** displays the managed system's machine type, model, and feature code. Also displayed are the CEC IPL Type and the FSP IPL Type for the managed system.

## Hardware

Add, exchange, or remove hardware from the managed system. Display a list of installed FRUs or enclosures and their locations. Select a FRU or an enclosure and launch a step-by-step procedure to add, exchange, or remove the unit.

### Add FRU:

Locate and add a Field Replaceable Unit (FRU).

To add a FRU, do the following:

1. Select an enclosure type from the drop down list.
2. Select an FRU type from the list.
3. Click **Next**.
4. Select a location code from the displayed list.
5. Click **Add**.
6. Click **Launch Procedure**.
7. When you have completed the FRU installation process, click **Finish**.

### Add Enclosure:

locate and add an enclosure.

To add an enclosure, do the following:

1. Select an enclosure type, then click **Add**.
2. Click **Launch Procedure**.
3. When you have completed the enclosure installation process, click **Finish**.

### Exchange FRU:

Use the **Exchange FRU** task to exchange one FRU with another.

To exchange a FRU:

1. Select an installed enclosure type from the drop down list.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin replacing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the installation.

### Exchange Enclosure:

Use the **Exchange Enclosure** task to exchange one enclosure for another.

To exchange an enclosure:

1. Select an installed enclosure, then click **Add** to add the selected enclosure's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin replacing the enclosures identified in **Pending Actions** in the selected system.
3. Click **Finish** when you have completed the enclosure replacement process

### Remove FRU:

Use the **Remove FRU** task to remove a FRU from your managed system.

To remove a FRU:

1. Select an enclosure from the drop down list to display a list FRU types currently installed in the selected enclosure.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin removing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the removal procedure.

### Remove Enclosure:

Use the **Remove Enclosure** task to remove an enclosure.

To remove an enclosure:

1. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin removing the enclosures identified in **Pending Actions** from the selected system.
3. Click **Finish** when you have completed the enclosure removal process.

### Power On/Off IO Unit:

Use the **Power On/Off IO Unit** task to power on or off an IO unit.

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

## Manage Dumps

Manage system, service processor, and power subsystem dumps for systems managed by the HMC.

### system dump

A collection of data from server hardware and firmware, either after a system failure or a manual request. Only perform a system dump under the direction of your next level of support or your service provider.

### service processor dump

A collection of data from a service processor either after a failure, external reset, or manual request.

### **power subsystem dump**

A collection of data from Bulk Power Control service processor. This is only applicable to certain models of managed systems.

Use the Manage Dump task to do the following:

- Initiate a system dump, a service processor dump, or a power subsystem dump.
- Modify the dump capability parameters for a dump type before initiating a dump.
- Delete a dump.
- Copy a dump to media such as a DVD-RAM.
- Copy a dump to another system using FTP.
- Call home a dump by using the Call Home feature to transmit the dump back to your service provider, for example IBM Remote Support, for further analysis.
- View the offload status of a dump as it progresses.

Use the online Help if you need additional information for managing dumps.

### **Collect VPD**

Copy Vital Product Data (VPD) to removable media.

The managed system has VPD that is stored internally. The VPD consists of information such as how much memory is installed, and how many processors are installed. These records can provide valuable information which can be used by remote service and service representatives so that they can help you keep the firmware and software on your managed system up to date.

**Note:** To collect VPD, you must have at least one operational partition. For more information, see Logical Partitioning.

The information in the VPD file can be used to complete the following types of orders for your managed system:

- Install or remove a sales feature
- Upgrade or downgrade a model
- Upgrade or downgrade a feature

Using this task, this information can be sent to removable media (diskette, DVD-RAM, or memory key) for use by you or your service provider.

Use the online Help if you need additional information for collecting VPD.

### **Edit MTMS**

Edit or display the model, type, machine serial (MTMS) or configuration ID of an enclosure.

The MTMS value or configuration ID for an expansion unit may need to be edited during a replacement procedure.

Use the online Help if you need additional information for editing MTMS.

### **FSP Failover**

Enable a secondary service processor if your managed system's primary service processor fails.

FSP Failover is designed to reduce customer outages due to service processor hardware failures. If a redundant service processor is supported for the current system configuration, select **Setup** to set up FSP Failover for the selected managed system. Select **Initiate** to initiate FSP Failover for the selected managed system.

To set up or initiate the FSP failover, do the following:


1. In the navigation area, expand **Systems management**.
2. In the navigation area, expand **Servers**.
3. Select the server.
4. In the tasks area, expand **Serviceability**.
5. In the tasks area, expand **FSP Failover**.
6. Select one of the following options:
  - **Setup** to set up FSP Failover for the selected managed system.
  - **Initiate** to initiate FSP Failover for the selected managed system.

## Capacity on Demand

Activate inactive processors or memory that are installed on your managed server.

Capacity on Demand (CoD) allows you to nondisruptively activate (no boot required) processors and memory. Capacity on Demand also gives you the option to temporarily activate capacity to meet intermittent performance needs, to activate additional capacity on a trial basis, and to access capacity to support operations in times of need.

### Related information:

 [Capacity on Demand](#)

---

## Systems Management for Partitions

Systems Management displays tasks you can perform to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions for partitions.

To launch these tasks, see “Launching tasks for managed objects” on page 7. The following sets of tasks are represented in the taskpad, tasks menu, or context menu. The tasks listed in the taskpad change as selections are made in the work area. The context is always listed at the top of the taskpad in the format Task: Object. These tasks are listed when a partition is selected and the context is Tasks: *partition name*.

## Properties

The **Properties** task displays the selected partition's properties. This information is useful in resource allocation and partition management. These properties include:

### General

The **General** tab displays the partition's name, id, environment, state, resource configuration, operating system, the current profile used when starting the partition, if the partition is suspend-capable, and the system on which the partition is located.

### Hardware

The **Hardware** tab displays the current usage of processors, memory, and I/O on the partition.

**Note:** When the operating system and the hypervisor supports a minimum entitlement of 0.05 processor per virtual processor, the minimum, maximum, and desired processing units can be set to the lowest supported value of 0.05.

### Virtual Adapters

The **Virtual Adapters** tab displays the current configuration of virtual adapters. Virtual adapters allow for the sharing of resources between partitions. From this tab, you can view, create, and edit virtual adapters on the partition.

### Settings

The **Settings** tab displays the boot mode and keylock position of the partition. Also displayed are the current service and support settings for the partition.



**Other** The **Other** tab displays the partition's Workload Management Group (if applicable), and the partition's Power controlling partitions.

## Change Default Profile

Change the default profile for the partition.

Select a profile from the drop down list to be the new default profile.

## Operations

Operations contains the tasks for operating partitions.


### Activate

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

Select the partition profile from the list of profiles and click **OK** to activate the partition. On the **Advanced** tab, select the **No VSI Profile** check box to ignore the failure while configuring the Virtual Station Interface (VSI) profile.

**Note:** As of Version 7.7, or later, you can install a Virtual I/O Server (VIOS) on a logical partition from an HMC by using a DVD, a saved image, or a Network Installation Management (NIM) server.

#### Related information:

 [Activating a partition profile](#)

 [VIOS configuration requirements for using VSI profiles and the VEPA switching mode](#)

### Restart

Restart the selected logical partition or partitions.

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

If you choose to restart VIOS partitions that are acting as the Paging Service Partition (PSP) for a number of client partitions, a warning displays, indicating that you should shut down the client partitions before shutting down the VIOS partition.

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

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

### Operating System

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



### **Operating System Immediate**

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

### **Dump Retry**

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

### **Shut Down**

Shut down the selected logical partition or partitions.

For IBM i logical partitions, use this window only if you cannot shut down the IBM i logical partition from the command line of the operating system. Using this window to shut down an IBM i logical partition will result in an abnormal IPL.

If you choose to shut down VIOS partitions that are acting as the Paging Service Partition (PSP) for a number of client partitions, a warning displays, indicating that you should shut down the client partitions before shutting down the VIOS partition.

Choose from the following options:

#### **Delayed**

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

#### **Immediate**

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

#### **Operating System**

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

#### **Operating System Immediate**

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

### **Manage Attention LED**

Use the **Manage Attention LED** to activate or deactivate an attention LED on your partition.

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

### **Schedule Operations**

Create a schedule for certain operations to be performed on the logical partition without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule an operation to remove resources from a logical partition or move resources from one logical partition to another.

The Scheduled Operations task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the Scheduled Operations window you can do the following:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

You can schedule an operation to occur once or you can schedule it to repeat. You must provide the time and date that you want the operation to occur. If the you want the operation to repeat, you will be asked to select the following:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that you can schedule for a logical partition include the following:

#### **Activate on an LPAR**

Schedules an operation on a selected profile for activation of the selected logical partition.

#### **Dynamic Reconfiguration**

Schedules an operation for adding, removing, or moving a resource (processors or megabytes of memory).

#### **Operating System Shutdown (on a partition)**

Schedules a shutdown of the selected logical partition.

To schedule operations on the HMC, do the following:

1. In the Navigation area, click **Systems Management**.
2. In the work pane, select one or more partitions.
3. In the taskpad, select the **Operations** task category, then click **Schedule Operations**. The Customize Scheduled Operations window opens.
4. From the Customize Scheduled Operations window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, click **Options** and then click **New**.
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details**.

- To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range**.
- To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.

5. To return to the HMC workplace, point to **Operations** and then click **Exit**.

## viosvr cmd

Issue virtual I/O server command.

### Synopsis

```
viosvr cmd -m managed-system {-p partition-name | --id partition-ID} -c "command" [--help]
```

### Description

**viosvr cmd** issues an I/O server command line interface (ioscli) command to a virtual I/O server partition.

The ioscli commands are passed from the Hardware Management Console (HMC) to the virtual I/O server partition over an RMC session. RMC does not allow interactive execution of ioscli commands.

### Options

- m** The name of the managed system which has the virtual I/O server partition to which to issue the command. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- p** The name of the virtual I/O server partition to which to issue the command.  
You must either use this option to specify the name of the partition, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- id** The ID of the virtual I/O server partition to which to issue the command.  
You must either use this option to specify the ID of the partition, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- c** The I/O server command line interface (ioscli) command to issue to the virtual I/O server partition.  
*command* must be enclosed in double quotes. Also, *command* cannot contain the semicolon (;), greater than (>), or vertical bar (|) characters.
- help** Display the help text for this command and exit.

### Delete

Use the **Delete** task to delete the selected partition.

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

### Mobility

Use the Mobility task to migrate your partition to another server, ensure that the requirements for the migration are met, and recover if the partition is in an invalid state.

### Migrate:

Migrate a partition to another managed system.

#### **About this task**

To migrate a partition to another system, do the following:

#### **Procedure**

1. In the navigation area, expand **Systems Management**.
2. Expand **Servers**.
3. Select the server.
4. In the contents area, select the partition you want to migrate to another system.
5. Select **Operations > Mobility > Migrate**. The Partition Migration wizard opens.
6. Complete the steps in the Partition Migration wizard and click **Finish**.

#### **Validate:**

Validate the settings for moving the partition from the source system to the destination system.

#### **About this task**

To validate the settings, do the following:

#### **Procedure**

1. In the navigation area, expand **Systems Management**.
2. Expand **Servers**.
3. Select the server.
4. In the contents area, select the partition you want to migrate to another system.
5. Select **Operations > Mobility > Validate**. The Partition Migration Validation window opens.
6. Fill in the information in the fields, and click **Validate**.

#### **Recover:**

Recover this partition from a migration that did not complete.

#### **About this task**

To recover this partition from a migration that did not complete, do the following:

#### **Procedure**

1. In the navigation area, expand **Systems Management**.
2. Expand **Servers**.
3. Select the server.
4. In the contents area, select the partition you want to recover.
5. Select **Operations > Mobility > Recover**. The Migration Recovery window opens.
6. Complete the information as necessary and click **Recover**.

### **Suspend operations**

You can suspend a logical partition. Ensure that you have validated a logical partition before suspending a logical partition or resuming a suspended logical partition.

#### **Validate:**

You can validate whether a partition can be suspended.

### About this task

To validate a partition for the suspend capability, complete the following steps:

#### Procedure

1. In the navigation area, click **Systems Management > Servers**.
2. In the work pane, select the logical partition.
3. In the taskpad, select the **Operations** task category, and click **Suspend Operations > Validate**.

#### Suspend:

You can suspend a logical partition.

#### Before you begin

Ensure that you have created the logical partition with the suspend capability.

#### Procedure

1. In the navigation area, click **Systems Management > Servers**.
2. In the work pane, select the logical partition.
3. In the taskpad, select the **Operations** task category, and click **Suspend Operations > Suspend**.

#### Related information:

 [Creating a logical partition with suspend capability](#)

#### Resume:

You can resume, recover and shut down a suspended logical partition.

### About this task

To resume a suspended logical partition, complete the following steps:

#### Procedure

1. In the navigation area, click **Systems Management > Servers**.
2. In the work pane, select the logical partition.
3. In the taskpad, select the **Operations** task category, and click **Suspend Operations > Resume**.

## Configuration

**Configuration** contains the tasks for configuring your partitions.

### Manage Profiles

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

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

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

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

## Manage Custom Groups

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

One or more user-defined groups might already be defined on your HMC. Default groups are listed under **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

## Save Current Configuration

Save the current configuration of a logical partition to a new partition profile by entering a new profile name.

This procedure is useful if you change the configuration of a logical partition using dynamic logical partitioning and you do not want to lose the changes when you restart the logical partition. You can perform this procedure at any time after you initially activate a logical partition.

## Hardware Information

Display information about the hardware attached to a selected managed system.

### Adapters

View information about the Host Ethernet Adapters (HEA, also referred to as Integrated Virtual Ethernet adapters) or Host Channel Adapters (HCA) for a selected managed system.

#### Related information:

 [Host Ethernet Adapter](#)

#### Host Ethernet Adapter (HEA):

A Host Ethernet Adapter (HEA) allows multiple logical partitions to share a single physical Ethernet adapter.

Unlike most other types of I/O devices, you can never assign the HEA itself to a logical partition. Instead, multiple logical partitions can connect directly to the HEA and use the HEA resources. This allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge on another logical partition.

Use the **Host Ethernet** task to display the ports of the physical HEAs on a selected managed system.

#### Host Channel Adapter (HCA):

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

You can show a list of the HCAs for the managed system. You can select an HCA from the list to display the current partition usage for the HCA.

From this task you can display the following:

- The physical location of each HCA on the managed system.
- The number of globally unique identifiers (GUIDs) that are in use on each HCA.
- The number of GUIDs on each HCA that are available to be assigned to logical partitions.
- HMC management status. HCAs that are unable to be managed by an HMC are in an error state.
- The logical partition usage for a selected HCA.

### Switch Network Interface:

Use the **Switch Network Interface** task to display a list of the Switch Network Interface (SNI) adapters for the selected managed system.

Displayed is the SNI adapter handle, the name of the partition to the adapter is assigned, the physical location of the adapter, and the host name or IP address of the adapter.

### Virtual IO Adapters

View the topology of currently configured virtual SCSI and virtual Ethernet adapters on a selected partition.

Use the **SCSI** task to view the topology of virtual SCSI adapters on a partition. The following information is displayed:

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

Use the **Ethernet** task to view the current virtual Ethernet configuration for the partition. The following information is displayed:

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

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

## Dynamic Logical Partitioning

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

### Related information:

 [Managing logical partition resources dynamically using the HMC](#)

### Processor

Add or remove processor resources from a logical partition or to move processor resources from one logical partition to another.

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

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

Use the online Help for more information on adding, removing, or moving processor resources.

## Memory

Add or remove memory resources from a logical partition or to move memory resources from one logical partition to another.

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

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

Use the online Help for more information on adding, removing, or moving processor resources.

## Physical Adapters

Add I/O slots to a logical partition without restarting the partition or to move or remove I/O slots from a logical partition without restarting the partition.

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

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

Vary off the I/O slot and all I/O adapters and devices connected to the I/O slot before you remove the I/O slot from the logical partition.

## Virtual Adapter

This task displays a list of all of the virtual adapters that currently exist for this logical partition or partition profile.

Use this task to create, change, or remove a virtual adapter on a logical partition or in a partition profile.

From this task you can:

- Display the properties of a virtual adapter.
- Edit the properties of a virtual adapter.
- Create a new virtual adapter.
- Delete a virtual adapter.

## Host Ethernet

Use **Host Ethernet** tasks to add Logical Host Ethernet Adapter (LHEA) logical ports dynamically to a running logical partition.

Use the **Add** task to add LHEA logical ports dynamically to a running logical partition. These logical ports allow the logical partition to access and use the physical port resources on a physical HEA.

Some operating system or system software versions do not allow you to add logical ports dynamically. Consult the documentation for the operating system or system software for more information.



To add logical ports dynamically to the logical partition, select the HEA whose resources you want to use, select the physical port for which you want to create a logical port, and click **Configure**. You can then configure the logical port and return to this window. If you change your mind about adding a logical port to the logical partition, select the physical port that corresponds to the logical port and click **Reset**. You can then configure a different logical port for that physical port.

When you are done adding logical ports to the running logical partition, click **OK**.

Use the **Move or Remove** task to move LHEA logical ports dynamically from the selected logical partition.

These logical ports allow the logical partition to access and use the physical port resources on a physical HEA. You can move the logical ports dynamically to another running logical partition, or you can leave the logical ports as unassigned.

Some operating system or system software versions do not allow you to move or remove logical ports dynamically. Consult the documentation for the operating system or system software for more information.

To remove logical ports dynamically from the logical partition, select the HEA whose logical ports you want to remove, select the physical port whose logical ports you want to remove and click **OK**.

To move logical ports dynamically from the logical partition to another running logical partition, select the HEA whose logical ports you want to remove, select the physical port whose logical ports you want to move, select the destination logical partition in Logical Partition, and click **OK**.

## Console window

Use the **Open Terminal Window** task to open a terminal window to the operating system running on the selected partition.

Use the **Close Terminal Connection** task to close the connection.

Use the **Open Shared 5250 Console** task to open a shared console with an IBM i partition.

Use the **Open Dedicated 5250 Console** task to open a dedicated console with an IBM i partition.

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it.

These problems are reported to you as serviceable events. Use the **Manage Events** task to view specific events for selected systems. However, if you notice a problem occurred or you suspect a problem is affecting the system but Problem Analysis has not reported it to you, use the **Create Serviceable Event** task to report the problem to your service provider.

### Manage Serviceable Events

Problems on your managed system are reported to the HMC as serviceable events. You can view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you to view, do the following:

1. From the taskpad, open **Manage Serviceable Events**.
2. Provide event criteria, error criteria, and FRU criteria.
3. Click **OK**.
4. If you do not want the results filtered, select **ALL**.

The Serviceable Events Overview window displays all of the events that match your criteria. The information displayed in the compact table view includes the following:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and use the **Selected** drop down menu to:

- **View event details:** Field-replaceable units (FRUs) associated with this event and their descriptions.
- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Reference Code History

Use the **Reference Code History** task to view reference codes that have been generated for the selected logical partition. Reference codes are diagnostic aids that help you determine the source of a hardware or operating system problem.

By default, only the most recent reference codes that the logical partition has generated are displayed. To view more reference codes, enter the number of reference codes that you want to view into **View history** and click **Go**. The window displays that number of the latest reference codes, with the date and time at which each reference code was generated. The window can display up to the maximum number of reference codes stored for the logical partition.

## Control Panel Functions

This task displays the available virtual control panel functions for the selected IBM i partition. The tasks are:

- (21) **Activate Dedicated Service Tools**  
Starts Dedicated Service Tools (DST) on the partition.
- (65) **Disable Remote Service**  
Deactivates remote service on the partition.
- (66) **Enable Remote Service**  
Activates remote service on the partition.
- (68) **Concurrent Maintenance Power Off Domain**  
Concurrent maintenance power domain Power Off.
- (69) **Concurrent Maintenance Power On Domain**  
Concurrent maintenance power domain Power On.

---

## Systems Management for Frames

Set up, configure, view current status, troubleshoot, and apply solutions for frames.

This section describes the tasks you can perform when you select a frame.

To launch these tasks, see “Launching tasks for managed objects” on page 7. The following sets of tasks are represented in the taskpad, tasks menu, or context menu. The tasks listed in the taskpad change as selections are made in the work area. The context is always listed at the top of the taskpad in the format Task: Object. These tasks are listed when a managed system is selected and the context is Tasks: *Frame Name*.

## Properties

Display the selected frame properties.

These properties include the following:

### General

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

### Managed Systems

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

### I/O Units

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

## Update Password

Use the Update Password task to update HMC access and Advanced System Management Interface (ASMI) passwords on the managed system.

The first time you access a managed system using an HMC, the system prompts you to enter passwords for each of the following:

- Hardware Management Console: HMC access
- Advanced System Management Interface: General
- Advanced System Management Interface: Admin

If you are using an HMC to access the managed system before all required passwords have been set, enter the appropriate password for each password that is presented in the Update Password task.

If another HMC subsequently needs access to this managed system, upon attempting to access this HMC the user is presented with the Update Password Failed Authentication window, which will prompt for the HMC access password you entered.

In the event that the HMC access password changes while you are logged in to the managed system, your HMC will discover that it can no longer authenticate after it attempts to reconnect to that managed system. This will result in a state of *Failed Authentication* for that managed system. You will be required to enter the new password before any actions can be performed.

## Operations

Perform tasks on managed frames.

### Initialize Frames

Initialize managed frames.

This operation task is available when one or more frames are selected. It will first power on the unowned I/O units within the selected managed frames, then power on the managed systems within the selected managed frames. The complete initialization process may take several minutes to complete.

**Note:** Managed systems that are already powered on will not be affected. They will not be powered off and back on again.

## Initialize All Frames

Initialize all of your frames.

### About this task

This operation task is available when no managed frame is selected and the **Frames** tab on the navigation area is highlighted. It will first power on unowned I/O units within each managed frame, then power on managed systems within each managed frame.

**Note:** Frames are already powered on when they are connected to HMC. Initializing frames does not power on the frames.

## Rebuild

Update frame information on the HMC interface.

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

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

## Change Password

Change the HMC access password on the selected managed frame.

After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed frame.

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

## Power On/Off IO Unit

Power off an IO unit using the HMC interface.

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

## Configuration

Configuration contains the tasks for configuring your frame. You can manage custom groups using the Configuration task.

### Manage Custom Groups

You can report status on a group basis, allowing you to monitor your system in a way that you prefer.

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

One or more user-defined groups might already be defined on your HMC. Default groups are listed under **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

## Connections

**Connections** tasks allow you to view the HMC connection status to frames or reset those connections.

### Bulk Power Assembly (BPA) Status

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

The HMC displays the following:

- IP address
- BPA Role
- Connection Status
- Connection Error code

If the status is not Connected, the Connection status may be one of the following:

#### Starting/Unknown

One of the Bulk Power Assemblies (BPAs) contained in the frame is in the process of starting. The state of the other BPA cannot be determined.

#### Standby/Standby

Both of the BPAs contained in the frame are in the standby state. A BPA in the standby state is operating normally.

#### Standby/Starting

One of the BPAs contained in the frame is operating normally (in standby state). The other BPA is in the process of starting.

#### Standby/Not Available

One of the BPAs contained in the frame is operating normally (in the standby state), but the other BPA is not operating normally.

#### Pending frame number

A change to the frame number is in progress. No operations can be performed when the frame is in this state.

#### Failed Authentication

The HMC access password for the frame is not valid. Enter a valid password for the frame.

#### Pending Authentication - Password Updates Required

The frame access passwords have not been set. You must set the required passwords for the frame, to enable secure authentication and access control from the HMC.

#### No Connection

The HMC cannot connect to the frame.

#### Incomplete

The HMC failed to get all of the necessary information from the managed frame. The frame is not responding to requests for information.

### Reset

Reset the connection between the HMC and the selected managed frame.

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

## Hardware Information

Display information about the hardware attached to a selected managed frame.

## View RIO Topology

Display the current RIO topology for the selected managed frame and any discrepancies between the current topology and the last valid topology.

High Speed Link (HSL), also known as Remote I/O (RIO), resources provide the connection between system I/O busses and the system processor. HSL/RIO resources are normally configured in loops with the system unit having an HSL/RIO controller resource that handles routing of the data between the system processor and the system I/O busses. System I/O busses connect to the loop with HSL I/O adapter or RIO adapter resources.

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

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

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it. These problems are reported to you as serviceable events. you can view specific events for selected systems and add, remove, or exchange a Field Replaceable Unit (FRU).

### Manage Serviceable Events

Problems on your managed frame are reported to the HMC as serviceable events. You can view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you want to view, do the following:

1. From the taskpad, open **Manage Serviceable Events**.
2. Provide event criteria, error criteria, and FRU criteria.
3. Click **OK**.
4. If you do not want the results filtered, select **ALL**.

The Serviceable Events Overview window displays all of the events that match your criteria. The information displayed in the compact table view includes the following:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and do the following:

- **View event details:** FRUs associated with this event and their descriptions.

- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Hardware

These tasks are used to add, exchange, or remove hardware from the managed frame. From the hardware tasks you can display a list of installed FRUs or enclosures and their locations. Select a FRU or an enclosure and launch a step-by-step procedure to add, exchange, or remove the unit.

### Add FRU:

Use the **Add FRU** task to locate and add a FRU.

To add a FRU, do the following:

1. From the drop down list, select an enclosure type.
2. Select an FRU type.
3. Click **Next**.
4. Select a location code.
5. Add the selected enclosure location to Pending Actions by clicking **Add**.
6. Begin adding the selected FRU type to the enclosure locations identified in Pending Actions by clicking **Launch Procedure**.
7. When you have completed the FRU installation process, click **Finish**.

### Add Enclosure:

Use the Add Enclosure task to locate and add an enclosure.

To add an enclosure, do the following:

1. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to Pending Actions.
2. To begin adding the enclosures identified in Pending Actions to the selected system, click **Launch Procedure**.
3. When you have completed the enclosure installation process, click **Finish**.

### Exchange FRU:

Exchange one FRU with another.

To exchange a FRU, do the following:

1. Select an installed enclosure type.
2. Select an FRU type.
3. Click **Next**.
4. Select a location code for a specific FRU.
5. Click **Add**.
6. Select **Launch Procedure**.
7. When you have completed the installation, click **Finish**.

### Exchange Enclosure:



Exchange one enclosure for another.

To exchange an enclosure, do the following:

1. Select an installed enclosure, then click **Add** to add the selected enclosure's location code to Pending Actions.
2. Begin replacing the enclosures identified in Pending Actions in the selected system by clicking **Launch Procedure**.
3. When you have completed the enclosure replacement process, click **Finish**.

#### **Remove FRU:**

Remove a FRU from your managed system.

To remove a FRU, do the following:

1. Select an enclosure from the drop down list.
2. Select an FRU type from the displayed list of FRU types for this enclosure.
3. Click **Next**.
4. Select a location code for a specific FRU.
5. Click **Add**.
6. Select **Launch Procedure**.
7. When you have completed the removal procedure, click **Finish**.

#### **Remove Enclosure:**

Remove an enclosure identified by the HMC.

To remove an enclosure, do the following:

1. Select an enclosure type, then click **Add**.
2. Click **Launch Procedure**.
3. When you have completed the enclosure removal process, click **Finish**.

---

## **System Plans**

Display the tasks used to record or import specifications for logical partitions, partition profiles, or hardware specifications on a chosen system.

To display the tasks available for a system plan, select a system plan from the System Plan work pane table.

### **View System Plan**

Review the detailed information in the selected system plan.

The System Plan Viewer consists of four main areas:

#### **Title pane**

Displays basic information about the System Plan Viewer and the application from which you accessed the viewer.

#### **Navigation pane**

Provides a navigation tree of the system plan that you are viewing.

#### **Contents pane**

Provides the detailed view of the information in the system plan that you are viewing.

#### **Actions pane**

Contains action buttons that allow you to work with the system plan.



Use the navigation tree to determine which aspects of the system plan to view. Some levels of the tree can be expanded or collapsed to reveal more entries.

Use the online Help for more information on viewing a system plan.

## Create System Plan

This task is used to create a new system plan for a system that this HMC manages. The new system plan contains specifications for the logical partitions and partition profiles of the managed system that you used to create the plan.

The new system plan also can contain hardware information that the HMC is able to obtain from the selected managed system. However, the HMC might not be able to detect all system hardware and partition settings. For example, the HMC is not able to detect the types of disk drives installed on the managed system unless the HMC uses Resource Monitoring and Control (RMC) to monitor resources on the managed system.

To maximize the information that the HMC can obtain from the managed system, power on the managed system and activate the logical partitions on the managed system before creating the new system plan.

When you use the HMC to create a system plan for a managed system, you can capture partition configuration information and a limited amount of associated hardware configuration information. Additionally, you can set up Resource Monitoring and Control (RMC) prior to creating a system plan to capture more detailed information. Although it may cause the creation of the system plan to take several more minutes to finish processing, by using RMC you can capture disk drive and tape drive configuration information for a managed system in the system plan.

Use the online Help for more information on creating a system plan.

## Deploy System Plan

Select the system plan that you want to deploy and the name of the managed system on which you want to deploy the plan.

This task uses the Deploy System Plan wizard to perform the following actions, depending on the contents of the system plan. To learn more about deploying system plans, read the following:

If the system plan contains logical partition information, you can use the wizard to create the specified logical partitions on the managed system. You can choose to create all the logical partitions specified within the system plan, or you can choose which logical partitions in the system plan that you want to create.

Use the online Help for more information on deploying a system plan.

## Export System Plan

This task is used to export a system plan to other systems or other HMCs.

You have three options for exporting the selected system-plan file:

- You can export the system file to the local system on which you are running the browser to access the HMC.
- You can export the system-plan file to removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices.
- You can export the system-plan file to a remote file transfer protocol (FTP) site. Exporting a system-plan file by means of FTP allows you to import the system-plan file into a different HMC. You can then deploy a system plan in the file to a system that the other HMC manages.

Use the online Help for more information on exporting a system plan.

## Import System Plan

This task is used to import a system plan to other systems or other HMCs.

You can save this system plan and import the plan on other systems that this HMC manages that have hardware that is identical to the hardware in the system plan. You can import the system plan on another HMC and use it to deploy the system plan to other systems the target HMC manages that have hardware that is identical to the hardware in the system plan.

You can also import a system plan created using the System Planning Tool (SPT) at <http://www.ibm.com/systems/support/tools/systemplanningtool/>. The SPT is available to assist you in system planning, design, validation and to provide a system validation report that reflects your system requirements while not exceeding system recommendations. The SPT is a PC-based browser application designed to be run in a standalone environment. The SPT emulates an LPAR configuration and validates that the planned partitions are valid. It allows you to test the placement of hardware within the system to ensure that the placement is valid. When you have prepared your partitioning plan using the SPT, you can save this plan in a system plan file. You can import this file into your HMC and deploy the system plan to a managed system that is managed by the HMC. When you deploy the system plan, the HMC creates the logical partitions from the system plan on the managed system.

You can import a system-plan file from one of three sources:

- You can import a system file from the local system on which you are running the browser to access the HMC.
- You can import a system-plan file from removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices.
- You can import a system-plan file from a remote file transfer protocol (FTP) site. Importing a system-plan file by means of FTP allows you to deploy a system plan from a source other than the current HMC.

Use the online Help for more information on importing a system plan.

## Remove System Plan

This task is used to permanently remove the specified system plan from the HMC.

**Note:** Removing the system plan from the HMC does not undo any partition or hardware configuration changes that occurred if the specified system plan was deployed on a managed system.

Use the online Help for more information on removing a system plan.

---

## HMC Management tasks

The tasks that are available on the Hardware Management Console (HMC) for the **HMC Management** tasks are described.

To open these tasks, see “HMC Management” on page 12.

**Note:** Depending on the task roles assigned to your user ID you may not have access to all the tasks. See Table 4 on page 15 for a listing of the tasks and the user roles allowed to access them.

## HMC Management - Operations

These tasks describe the tasks you can perform to operate your HMC.

## View HMC Events

View a record of system events occurring on the HMC. System events are individual activities that indicate when processes occur, begin and end, succeed or fail.

To view HMC events, do the following:

1. In the HMC Management work pane, click **View HMC Events**. Use the menu bar to change to a different time range, or to change how the events display in the summary. You can also use the table icons or the **Select Action** menu on the table toolbar to display different variations of the table.
2. When you are done viewing the events, select **View** on the menu bar, then click **Exit**.

Use the online Help for additional information about viewing HMC events.

## Shut Down or Restart

This task enables you to shut down (power off the console) or to restart the console.

1. Open the **Shut Down or Restart** task from the HMC Management work pane.
2. From the **Shut Down or Restart** window, you can:
  - Select **Restart the HMC** to automatically restart the HMC once the shut down has occurred.
  - Do not select **Restart the HMC** if you do not want to automatically restart the HMC.
3. Click **OK** to proceed with the shut down, otherwise click **Cancel** to exit the task.

Use the online Help if you need additional information about shutting down or restarting the HMC.

### Related information:

“Import Service Key” on page 92

Before you can import a service key file into an HMC, a service key file must first be created on the Kerberos server for the HMC host. The service key file contains the host principal of the HMC client, for example, `host/example.com@EXAMPLE.COM`. In addition to KDC Authentication, the host service key file is used to enable password-less SSH (Secure Shell) login using GSSAPI.

“Remove Service Key” on page 93

## Schedule Operations

Create a schedule for certain operations to be performed on the HMC itself without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule a backup of important HMC information to DVD to occur once, or set up a repeating schedule.

The **Scheduled Operations** task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the **Scheduled Operations** window you can:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operation that can be scheduled for the HMC is:

### **Backup Critical Console Data**

Schedules an operation to back up the critical console hard disk information for the HMC.

To schedule operations on the HMC, do the following:

1. Open the **Schedule Operations** task from the HMC Management work pane.
2. From the **Schedule Operations** window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, point to **Options** and then click **New**.
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details**.
  - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range**.
  - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
3. To return to the HMC workplace, point to **Options** and then click **Exit**.

Use the online Help to get additional information for scheduling an operation.

### **Format Media**

This task formats a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

You can use this task to format the following DVD-RAMs:

- Backup/restore
- Service data.

You can format a diskette by supplying a user-specified label.

To format a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key, do the following:

1. Open the **Format Media** task from the HMC Management work pane.
2. From the **Format Media** window, select the type of media you want to format, then click **OK**.
3. Make sure your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
4. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information for formatting a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

## Back up HMC Data

This task backs up (or archives) the data that is stored on your HMC hard disk that is critical to support HMC operations.

Back up the HMC data after changes have been made to the HMC or information associated with logical partitions.

The HMC data stored on the HMC hard drive can be saved to a DVD-RAM on a local system, a remote system mounted to the HMC file system (such as NFS), or sent to a remote site using File Transfer Protocol (FTP).

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

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

**Note:** Use the archived data only in conjunction with a reinstallation of the HMC from the product CDs.

To back up the HMC critical data:

1. Open the **Back up HMC Data** task from the HMC Management work pane.
2. From the **Back up HMC Data** window, choose the archive option you want to perform.
3. Click **Next**, then follow the appropriate instructions depending on the option you chose.
4. Click **OK** to continue with the backup process.

Use the online Help if you need additional information for backing up the HMC data.

## Restore HMC Data

This task is used to select a remote repository for restoring critical backup data for the HMC.

1. Open the **Restore HMC Data** task from the HMC Management work pane.
2. From the Restore HMC Data window, click **Restore from a remote Network File System (NFS) server**, **Restore from a remote File Transfer Protocol (FTP) server**, **Restore from a remote Secure Shell File Transfer Protocol (SFTP) server**, or **Restore from a remote removable media**.
3. Click **Next** to proceed or **Cancel** to exit the task without making any changes.

Use the online Help if you need additional information about restoring critical backup data for this HMC.

## Save Upgrade Data

This task uses a wizard to save upgrade data to selected media. This data consists of files that were created or customized while running the current software level. Saving this data to selected media is performed prior to an HMC software upgrade.

1. Open the **Save Upgrade Data** task from the HMC Management work pane.
2. From the **Save Upgrade Data** window, this wizard takes you through the steps required for saving your data. Select the type of media you want to save your data to, then click **Next** to proceed through the task windows.
3. Click **Finish** when you have completed the task.

Use the online Help if you need additional information for saving upgrade data.

## Change Network Settings

This task allows you to view the current network information for the HMC and to change network settings.

1. Open the **Change Network Settings** from the HMC Management work pane.

2. From the **Change Network Settings** window, you can work with the following tabs:

#### **Identification**

Contains the host name and domain name of the HMC.

#### **Console name**

Your HMC user name, the name that identifies your console to other consoles on the network. This is the short host name, for example: hmc1.

#### **Domain name**

A name that Domain Name Services (DNS) can translate to the IP address. For example, DNS might translate the domain name www.example.com to 198.105.232.4. (The long host name consists of the console name plus a period plus the domain name, for example: hmc.endicott.yourcompany.com.)

#### **Console description**

This is for your use only. An example might be: Main HMC for customer finance.

#### **LAN Adapters**

A summarized list of all (visible) Local Area Network (LAN) adapters. You can select any of these and click **Details...** to open a window allowing you to change addressing, routing, other LAN adapter characteristics, and firewall settings.

#### **Name Services**

Specify the DNS and domain suffix values for configuring the console network settings.

#### **Routing**

Specify the routing information and default gateway information for configuring the console network settings.

The **Gateway address** is the route to all networks. The default gateway address (if defined) informs this HMC where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside the area, it is usually because of an incorrectly configured default gateway.

You can assign a specific LAN to be the **Gateway device** or you can choose "any."

You can select **Enable 'routed'** to start the routed daemon, which allows it to run and allows any routing information to be exported from the HMC.

3. Click **OK** when you have completed this task.

**Note:** Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

Use the online Help to get additional information for customizing the network settings.

### **Test Network Connectivity**

Display network diagnostic information for the console's TCP/IP connection. Send an echo request to a remote host.

To view information concerning the networking configuration on this HMC, do the following:

1. In the HMC Management work pane, click **Test Network Connectivity**. The Test Network Connectivity window opens.
2. Click the following tabs to view the network information.
  - Ping
  - Interfaces
  - Ethernet Settings
  - Address
  - Routes

- Address Resolution Protocol (ARP)
- Sockets
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Protocol (IP)

3. Click **Cancel** when you have completed this task.

Use the online Help to get additional information on your console's network information.

## View Network Topology

Display a tree view of the network nodes known to this Hardware Management Console. Examples of such nodes are managed systems, logical partitions, storage, and other Hardware Management Consoles.

To view the network topology, do the following:

1. In the HMC Management work pane, click **View Network Topology**.
2. Do the following:
  - View attributes of a node by selecting the node in the tree view that is shown in the left pane. Attributes vary according to the type of node. Some examples are IP address, host name, location code, and status. Click **Refresh** to rediscover the topology and to query the nodes again for status and other attributes.
  - Save a snapshot of the current topology (select an item in the **Current Topology**, then click **Save**) and view it in the saved reference topology. You can view attributes of a node in the saved topology by selecting the node in the tree view that is shown in the left pane under **Saved Topology**.
  - Test network connectivity to a node by selecting the node in either the current or the saved topology views and clicking **Ping Current Node** or **Ping Saved Node**, available only for nodes that include an IP address or a host name.
3. When you have completed this task, click **Close**.

Use the online Help if you need additional information for viewing the network topology of the HMC.

## Tip of the Day

View information about using the HMC. When you enable this feature, a different fact or tip is displayed each time you log in.

The Tip of the Day window opens as long as **Show tips each time you log on** is selected on the window. You can also look at additional information by clicking **Previous Tip** or **Next Tip**.

To prevent this window from displaying each time you log in, you can deselect **Show tips each time you log on**, then click **Close**.

To access this task at any time, do the following:

1. In the HMC Management work pane, click **Tip of the Day**.
2. Select options as previously specified.
3. To save the changes or exit the task, click **Close**.

## View Licenses

View the Licensed Internal Code that you have agreed to for this HMC.

You can view licenses at any time. To view licenses, do the following:

1. In the HMC Management work pane, click **View Licenses**.
2. Click on any of the license links to view more information.

**Note:** This list does not include programs and code provided under separate license agreements.



3. Click **OK**.

## Change User Interface Settings

Customize settings that control how the HMC interface appears. You can display or hide certain user interface components and icons, display or hide specific navigation nodes, and determine whether or not to save user interface settings changes.

**Note:** User interface changes apply to the currently logged on user ID only.

To change user interface settings, do the following:

1. From the HMC Management work pane, click **Change User Interface Settings**. Optionally, you can also open the task by clicking on the logged on user name link displayed in the task bar below the banner. All items are selected in the Change User Interface Settings window by default.
2. Click **Apply** or **OK** for the change to take affect.
3. If you select **Save settings as my defaults at logoff**, any customization done to the following items are saved when the user logs off:
  - Displayed user interface components, such as the banner and taskpad
  - Displayed navigation and work pane icons
  - Displayed nodes in the navigation pane
  - Table view customization, such as filters, sorts, column sizing, ordering, and visibility settings
4. To restore all of the user interface settings to the original defaults, click **Factory Defaults**.

For additional information for changing the user interface settings, use the online Help.

## Change Date and Time

Change the time and date of the battery-operated HMC clock and add or remove time servers for the Network Time Protocol (NTP) service.

Use this task in the following situations:

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

**Note:** The time setting will adjust automatically for daylight saving time in the time zone you select.

To change the date and time, do the following:

1. In the HMC Management work pane, click **Change Date and Time**.
2. Click the **Customize Console Date and Time** tab.
3. Enter the date and time information.
4. Click **OK**.

To change the time server information, do the following:

1. In the HMC Management work pane, click **Change Date and Time**.
2. Click the **NTP Configuration** tab.
3. Provide the appropriate information for the time server.
4. Click **OK**.

If you need additional information for changing the date and time of the HMC or for adding or removing time servers for the Network Time Protocol (NTP) service, use the online Help.

## Launch Guided Setup Wizard

This task uses a wizard to set up your system and HMC.

1. Open the **Launch Guided Setup Wizard** from the HMC Management work pane.
2. From the **Launch Guided Setup Wizard - Welcome** window it is recommended that you have certain prerequisites on hand. Click **Prerequisites** in the **Launch Guided Setup Wizard - Welcome** window for the information. When you have completed that, this wizard takes you through the following tasks required to set up your system and HMC. As you complete each task, click **Next** to proceed.



- a. Change HMC Date and Time
  - b. Change HMC passwords
  - c. Create additional HMC users
  - d. Configure HMC Network Settings (This task cannot be performed if you are accessing the **Launch Guided Setup Wizard** remotely.)
  - e. Specify contact information
  - f. Configure connectivity information
  - g. Authorize users to use the Electronic Service Agent software tool and configure notification of problem events.
3. Click **Finish** when you have completed all the tasks in the wizard.

**Related information:**

 [Installing and configuring the Hardware Management Console](#)

## HMC Management - Administration

These tasks describe the administration tasks you can perform using your HMC.

### Change User Password

This task allows you to change your existing password used for logging onto the HMC. A password verifies your user ID and your authority to log in to the console.

To change your password:

1. Open the **Change User Password** task from the HMC Management work pane.
2. From the **Change User Password** window specify your current password, specify a new password you want to use, and respecify the new password to confirm in the fields provided.
3. Click **OK** to proceed with the changes.

Use the online Help if you need additional information for changing your password.

### Manage User Profiles and Access

Manage your system users that log on to the HMC. A user profile is a combination of a user ID, server authentication method, permissions, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

Users can be authenticated using local authentication on the HMC, by using Kerberos remote authentication, or by using LDAP authentication. For more information on setting up Kerberos authentication on the HMC, see “KDC Configuration” on page 90. For more information about LDAP authentication, see “Configuring the HMC so that it uses LDAP authentication” on page 93.

If you are using local authentication, the user ID and password are used to verify a user’s authorization to log on the HMC. The user ID must start with an alphabetic character and consist of 1 to 32 characters. The password has the following rules:

- Must begin with an alphanumeric character.
- Must contain at least seven characters, however, this limit may be changed by your system administrator.
- The characters should be standard 7-bit ASCII characters.
- Valid characters to use for the password can be: A-Z, a-z, 0-9 and special characters (~ ! @ # \$ % ^ & \* ( ) \_ + - = { } [ ] \ : " ; ').

If you are using Kerberos authentication, specify a Kerberos remote user ID.

The user profile includes managed resource roles and task roles that are assigned to the user. The *managed resource roles* assign permissions for a managed object or group of objects and the *task roles* define

the access level for a user to perform on a managed object or group of objects. You can choose from a list of available default managed resource roles, task roles, or customized roles created by using the **Manage Task and Resource Roles** task.

See “HMC tasks, user roles, IDs, and associated commands” on page 15 for a listing of all the HMC tasks and the predefined default user IDs that can perform each task.

The default managed resource roles include:

- All System Resources

The default task roles include:

- hmcshervicerep (Service Representative)
- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)
- hmcsuperadmin (Super Administrator).

To add or customize a user profile, do the following:

1. Open the **Manage User Profiles and Access** task from the HMC Management work pane.
2. Complete one of the following steps:
  - From the **User Profiles** window, if you are creating a new user ID, point to **User** on the menu bar and when its menu is displayed, click **Add**. The **Add User** window is displayed.
  - From the **User Profiles** window, if the user ID already exists in the window, select the user ID from the list, and then point to **User** on the menu bar and when its menu is displayed, click **Modify**. The **Modify User** window is displayed.
3. Complete or change the fields in the window, click **OK** when you are done.

Use the online Help if you need additional information for creating, modifying, copying, or removing a user profile.

**Related tasks:**

“Configuring the HMC so that it uses LDAP authentication” on page 93

Configure your HMC so that it uses LDAP (Lightweight Directory Access Protocol) authentication.

**Related information:**

“Manage Task and Resource Roles”

Use this task to define and customize user roles.

## **Manage Task and Resource Roles**

Use this task to define and customize user roles.

**Note:** Predefined roles (default roles) cannot be modified.

A *user role* is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (*task roles*) or it can be created to define the set of managed objects that are manageable for a user (*managed resource roles*). Once you have defined or customized the user roles you can use the **Manage User Profiles and Access** task to create new users with their own permissions.

The predefined managed resource roles include:

- All System Resources

The predefined task roles include:

- hmcshervicerep (Service Representative)
- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)

- hmcsuperadmin (Super Administrator)

To customize managed resource roles or task roles:

1. Open the **Manage Task and Resource Roles** task from the HMC Management work pane.
2. From the **Manage Task and Resource Roles** window, select either **Managed Resource Roles** or **Task Roles**.
3. To add a role, click **Edit** from the menu bar, then click **Add** to create a new role.  
or  
To copy, remove, or modify an existing role, select the object you want to customize, click **Edit** from the menu bar, then click **Copy**, **Remove**, or **Modify**.
4. Click **Exit** when you have completed the task.

Use the online Help to get additional information for customizing managed resource roles and task roles.

#### **Related information:**

“Manage User Profiles and Access” on page 87

Manage your system users that log on to the HMC. A user profile is a combination of a user ID, server authentication method, permissions, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

## **Manage Users and Tasks**

Display the logged on users and the tasks they are running.

1. In the HMC Management work pane, click **Manage Users and Tasks**.
2. In the Manage Users and Tasks window, the following information displays:
  - User you are logged in as
  - Time you logged in
  - Number of tasks running
  - Your access location
  - Information about tasks that are running:
    - Task ID
    - Task name
    - Targets (if any)
    - Session ID
3. Choose to log off or disconnect from a session that is currently running by selecting the session from the Users **Logged On** list, then click **Logoff** or **Disconnect**.  
Alternately, you can choose to switch to another task or end a task by selecting the task from the **Running Tasks** list, then click **Switch To** or **Terminate**.
4. When you have completed this task, click **Close**.

## **Manage Certificates**

Use this task to manage the certificates used on your HMC. It provides the capability of getting information on the certificates used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates or signing certificates.

All remote browser access to the HMC must use Secure Sockets Layer (SSL) encryption. With SSL encryption required for all remote access to the HMC, a certificate is required to provide the keys for this encryption. The HMC provides a self-signed certificate that allows this encryption to occur.

To manage your certificates:

1. Open the **Manage Certificates** task from the HMC Management work pane.
2. Use the menu bar from the **Manage Certificates** window for the actions you want to take with the certificates:

- To create a new certificate for the console, click **Create**, then select **New Certificate**. Determine whether your certificate will be self-signed or signed by a Certificate Authority (CA), then click **OK**.
- To modify the property values of the self-signed certificate, click **Selected**, then select **Modify**. Make the appropriate changes, then click **OK**.
- To work with existing and archived certificates or signing certificates, click **Advanced**. Then you can choose the following options:
  - Delete existing certificates
  - Work with archived certificates
  - Import certificates
  - View issuer certificates

3. Click **Apply** for all changes to take effect.

Use the online Help if you need additional information for managing your certificates.

**Related information:**

“Remote operations” on page 109

Connect to and use the HMC remotely.

## KDC Configuration

View the key distribution center (KDC) servers that are used by this HMC for Kerberos remote authentication.

From this task you can do the following:

- View existing KDC servers
- Modify existing KDC server parameters including realm, ticket lifetime, and clock skew
- Add and configure a KDC server on the HMC
- Remove a KDC server
- Import a service key
- Remove a service key

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

Under Kerberos, a client (generally either a user or a service) sends a request for a ticket to the KDC. The KDC creates a ticket-granting ticket (TGT) for the client, encrypts it using the client's password as the key, and sends the encrypted TGT back to the client. The client then attempts to decrypt the TGT, using its password. If the client successfully decrypts the TGT (i.e., if the client gave the correct password), it keeps the decrypted TGT, which indicates proof of the client's identity.

The tickets have a time availability period. Kerberos requires the clocks of the involved hosts to be synchronized. If the HMC clock is not synchronized with the clock of KDC server, authentication will fail.

A Kerberos realm is an administrative domain, site, or logical network that uses Kerberos remote authentication. Each realm uses a master Kerberos database that is stored on a KDC server and that contains information about the users and services for that realm. A realm might also have one or more slave KDC servers, which store read-only copies of the master Kerberos database for that realm.

To prevent KDC spoofing, the HMC can be configured to use a service key to authenticate to the KDC. Service key files are also known as keytabs. Kerberos verifies the TGT requested was issued by the same KDC that issued the service key file for the HMC. Before you can import a service key file into an HMC, you must generate a service key for the host principal of the HMC client.

**Note:** For MIT Kerberos V5 \*nix distributions, create a service key file by running the `kadmin` utility on a KDC and using the `ktadd` command. Other Kerberos implementations may require a different process to create a service key.

You can import a service key file from one of these sources:

- Removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices. You must use this option locally at the HMC (not remotely), and you must mount the removable media to the HMC before using this option.
- A remote site using secure FTP. You can import a service-key file from any remote site that has SSH installed and running.

To use Kerberos remote authentication for this HMC, complete the following:

- You must enable the Network Time Protocol (NTP) service on the HMC and set the HMC and the KDC servers to synchronize time with the same NTP server. You can enable the NTP service on the HMC by accessing the **“Change Date and Time”** on page 86 task under **HMC Management**.
- You must set the user profile of each remote user to use Kerberos remote authentication instead of local authentication. A user that is set to use Kerberos remote authentication will always use Kerberos remote authentication, even when the user logs onto the HMC locally.

**Note:** You do not need to set all users to use Kerberos remote authentication. You can set some user profiles so that the users can use local authentication only.

- Use of a service key file is optional. Before using a service key file, you must import it into the HMC. If a service key is installed on the HMC, realm names must be equivalent to the network domain name. The following is an example of creating the service key file on a Kerberos server using the `kadmin.local` command assuming the HMC hostname is `hmc1`, the DNS domain is `example.com`, and the Kerberos realm name is `EXAMPLE.COM`:

```
- # kadmin_local kadmin.local: ktadd -k /etc/krb5.keytab host/hmc1.example.com@EXAMPLE.COM
```

Using the Kerberos `ktutil` on the Kerberos server, verify the service key file contents. The output should look like the following:

```
- # ktutil
ktutil: rkt /etc/krb5.keytab
ktutil: l
slot KVNO Principal
```

```
-----
1  9      host/hmc1.example.com@EXAMPLE.COM
2  9      host/hmc1.example.com@EXAMPLE.COM
```

- The HMC Kerberos configuration can be modified for SSH (Secure Shell) login without a password using GSSAPI. For remote login without a password through Kerberos to an HMC, configure the HMC to use a service key. Once the configuration is completed use `kinit -f principal` to obtain forwardable credentials on a remote Kerberos client machine. Then issue the following command to log in to the HMC without having to enter a password: `$ ssh -o PreferredAuthentications=gssapi-with-mic user@host`

### View KDC Server:

Display existing KDC servers on the HMC.

To view existing KDC Servers on your HMC, In the **HMC Management** work pane, click **Configure KDC**. If no servers exist and NTP has not yet been enabled, a warning panel message displays. Enable the NTP service on the HMC and configure a new KDC server as desired.

**Modify KDC Server:** To modify existing KDC server parameters, do the following:

1. In the **HMC Management** pane, click the **KDC Configuration** task.
2. Select a KDC Server.
3. Select a value to modify:
  - **Realm.** A realm is an authentication administrative domain. Normally, realms always appear in upper case letters. It is good practice to create a realm name that is the same as your DNS domain (in upper case letters). A user belongs to a realm if and only if the user shares a key with the authentication server of that realm. Realm names must be equivalent to the network domain name if a service key file is installed on the HMC.
  - **Ticket Lifetime.** Ticket lifetime sets the lifetime for credentials. The format is an integer number followed by one of **s** seconds, **m** minutes, **h** hours, or **d** days. Enter a Kerberos lifetime string such as *2d4h10m*.
  - **Clock skew.** Clock skew sets the maximum allowable amount of clock skew between the HMC and the KDC server before Kerberos considers messages invalid. The format is an integer number that represents number of seconds.
4. Click **OK**.

**Related information:**

“Add KDC server”

Add a Key Distribution Center (KDC) server to this HMC.

**Add KDC server:**

Add a Key Distribution Center (KDC) server to this HMC.

To add a new KDC server, do the following:

1. In the **HMC Management** work pane click **KDC Configuration**.
2. From the **Actions** drop down list, select **Add KDC Server**.
3. Enter the host name or IP address of the KDC server.
4. Enter the KDC server realm.
5. Click **OK**.

**Related information:**

“Modify KDC Server” on page 91

**Remove KDC server:**

Kerberos authentication on the HMC remains enabled until all KDC servers are removed.

To remove a KDC server:

1. Open the **KDC Configuration** task from the **HMC Management** work pane.
2. Select the KDC server from the list.
3. From the **Actions** drop down list, select **Remove KDC Server**.
4. Click **OK**.

**Import Service Key:**

Before you can import a service key file into an HMC, a service key file must first be created on the Kerberos server for the HMC host. The service key file contains the host principal of the HMC client, for example, `host/example.com@EXAMPLE.COM`. In addition to KDC Authentication, the host service key file is used to enable password-less SSH (Secure Shell) login using GSSAPI.

**Note:** For MIT Kerberos V5 \*nix distributions, create a service key file by running the `kadmin` utility on a KDC and using the `ktadd` command. Other Kerberos implementations may require a different process to create a service key.

To import a service key:

1. Open the **KDC Configuration** task from the **HMC Management** work pane.
2. From the **Actions** drop down list, select **Import Service Key**.
3. Select from one of the following:
  - **Local** - The service key must be located on removable media currently mounted on the HMC. You must use this option locally at the HMC (not remotely), and you must mount the removable media to the HMC before using this option. Specify the full path of the service key file on the media.
  - **Remote** - The service key must be located on a remote site available to the HMC via secure FTP. You can import a service key file from any remote site that has SSH (Secure Shell) installed and running. Specify the hostname of the site, a user ID and password for the site, and the full path of the service key file on the remote site.
4. Click **OK**.

Implementation of the service key file will not take effect until the HMC is rebooted.

**Related information:**

“Shut Down or Restart” on page 81

This task enables you to shut down (power off the console) or to restart the console.

**Remove Service Key:** To remove the service key from the HMC:

1. Open the **KDC Configuration** task from the **HMC Management** work pane.
2. From the **Actions** drop down list, select **Remove Service Key**.
3. Click **OK**.

You must reboot the HMC after removing the service key. Failure to reboot may cause login errors.

**Related information:**

“Shut Down or Restart” on page 81

This task enables you to shut down (power off the console) or to restart the console.

## Configuring the HMC so that it uses LDAP authentication

Configure your HMC so that it uses LDAP (Lightweight Directory Access Protocol) authentication.

### Before you begin

**Note:** Before you configure the HMC so that it uses LDAP authentication, you must ensure that a working network connection exists between the HMC and the LDAP servers.

### About this task

To configure your HMC so that it uses LDAP authentication, do the following:

#### Procedure

1. In the Navigation area, click **HMC Management**.
2. In the Contents area, click **LDAP Configuration**. The LDAP Server Definition window opens.
3. Select **Enable LDAP**.
4. Define an LDAP server to use for authentication.
5. Define the distinguished name tree, also known as the search base, for the LDAP server.
6. Click **OK**.



## What to do next

Next, you must configure each remote user's profile so that it uses LDAP remote authentication instead of local authentication.

### Related information:

“Manage User Profiles and Access” on page 87

Manage your system users that log on to the HMC. A user profile is a combination of a user ID, server authentication method, permissions, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

## Remote Command Execution

This task is used to enable remote command execution using the ssh facility.

1. Open the **Remote Command Execution** task from the HMC Management work pane.
2. From the **Remote Command Execution** window, select **Enable remote command execution using the ssh facility**.
3. Click **OK**.

### Related information:

“Remote operations” on page 109

Connect to and use the HMC remotely.

## Remote Virtual Terminal

A Remote Virtual Terminal connection is a terminal connection to a logical partition from another remote HMC. Use this task to enable Remote Virtual Terminal access for remote clients.

1. Open the **Remote Virtual Terminal** task from the HMC Management work pane.
2. From the **Remote Virtual Terminal** window, you can enable this task by selecting **Enable remote virtual terminal connections**.
3. Click **OK** to activate your changes.

Use the online Help to get additional information for enabling a remote terminal connection.

## Open Restricted Shell Terminal

Open a command line session.

**Note:** You cannot perform this task remotely.

In the HMC Management work pane, click **Open Restricted Shell Terminal**.

From the **Restricted Shell** window you can issue commands remotely through secure shell access to the managed system. This provides consistent results and automates administration of managed systems.

## Change Language and Locale

This task sets the language and location for the HMC. After you select a language, you can select a locale associated with that language.

The language and locale settings determine the language, the character set, and other settings specific to the country or region (such as formats for date, time, numbers, and monetary units). Changes made in the **Change Language and Locale** window affect only the language and locale for the HMC itself. If you access the HMC remotely, the language and locale settings on your browser determine the settings that the browser uses to display the HMC interface.

To change the language and locale on the HMC:

1. Open the **Change Language and Locale** task from the HMC Management Work pane.
2. From the **Change Language and Locale** window, choose the applicable language and locale.
3. Click **OK** to apply the change.



Use the online Help if you need additional information for changing the language and locale of the HMC.

## Create Welcome Text

This task allows you to customize the welcome message or to display a warning message that appears on the **Welcome** window before you log onto the HMC. You can use this text to notify users of certain corporate policies or security restrictions applying to the system.

To create a message:

1. Open the **Create Welcome Text** task from the HMC Management work pane.
2. From the **Create Welcome Text** window, enter a message in the input area.
3. Click **OK** to apply the change. The next time you log in to the HMC, your message is displayed.

Use the online Help to get additional information about displaying a message before logging onto the HMC.

## Manage Data Replication

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

The following types of data can be configured:

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

**Note:** Customizable console data is accepted from other HMCs only after specific HMCs and their associated allowable customizable data types have been configured.

Use the online Help to get additional information for enabling or disabling customizable data replication.

### Related information:

“Customizable data replication” on page 113

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

## Managing Install Resources

Add or remove operating environment installation resources for your HMC.

You can use the HMC to deploy a system plan that contains information for installing one or more operating environments on one or more logical partitions. To install an operating environment as part of deploying a system plan, the HMC must be able to access and to use an installation resource for that operating environment.

An operating environment installation resource is the necessary set of installation files for a specific version of an operating environment at a specific release and modification level. The installation resource can be on the local hard drive for the HMC or it can be on a Network Installation Management (NIM) server that the HMC can access.

When you define and create a local installation resource, you must meet the following prerequisites:

- You can define only one local installation resource for a specific operating environment version and modification level. For example, you can define a local installation resource for AIX 5.3 and another for AIX 6.1 but you cannot define two local installation resources for the same AIX version and modification level. This restriction applies to all listed operating environments.
- The HMC must have enough free hard disk space for the necessary set of operating environment installation files. The HMC creates the installation resource in the same local hard drive location that the HMC uses for main store dumps. Consequently, it is recommended that you maintain a certain amount of free hard drive space to avoid potential main store dump problems because main store dumps are necessary to help resolve some types of HMC errors. The typical main store dump averages between 4 to 8 gigabytes (GB), so consider maintaining at least 10 GB of free hard drive space for these dumps when you define and create local installation resources for the HMC.
- You must have the operating environment installation media available to copy to the HMC local hard drive. The type of media that you need varies based on the type of operating environment you want to be able to install. You can use CDs or DVDs as the installation image source for Red Hat and SLES operating environments. However, you can use DVDs only as the installation image source for AIX and Virtual I/O Server operating environments.

When you define a remote NIM server installation resource, you must meet a number of prerequisite conditions to ensure that the HMC can access and use the installation resource:

- The complete set of necessary operating environment installation files must exist on the NIM server within a uniquely named NIM resource group.

**Note:** You can define a remote resource for AIX and Virtual I/O Server operating environments only.

- You can define multiple remote installation resources for a specific operating environment version and modification level, as long as each installation resource is within a different NIM named resource group.
- You must know the fully qualified host name of the NIM server.
- You must know the resource group name that contains the necessary set of operating environment installation files.
- You must set up the HMC to be able to access the NIM server and use the operating environment installation files during system plan deployment. The HMC must be able to run secure shell commands by means of an ssh connection to access the NIM server successfully. Consequently, you must ensure that the HMC can provide an appropriate cryptographic key to the NIM server by completing the following steps:
  1. Open an HMC command prompt and run the following command to generate the RSA keys that the HMC needs for ssh connections and to place the keys in an accessible file in the HMC HOME directory: `ssh-keygen -t rsa -f /home/hscroot/ssh_keys`. This command creates two files: one called `ssh_keys` and one called `ssh_keys.pub` that contain the needed RSA keys. The `ssh_keys` file contains the private key that the HMC needs for establishing an ssh connection and this file needs to remain in the `/home/hscroot` subdirectory; the `ssh_keys.pub` file contains the public key that the NIM server must have to complete the ssh connection with the HMC.
  2. On the remote NIM server, append or copy the content of the `/home/hscroot/ssh_keys.pub` file into the `/.ssh/authorized_keys` file on the NIM server.

**Note:** Remote clients defined on the NIM server remain in place after installation of the operating environment on a partition for post installation management. The short hostname of the system will identify this remote client.

Each installation resource that you define and create for the HMC is available for selection in the **Customize Operating Environment Install** step of the Deploy System Plan Wizard. If the installation resource that you want to use for a selected partition is not available when you perform this step, you can click **New Install Resource** to open the Manage Install Resources window to define and create a new installation resource.

**Related information:**

“System Plans” on page 11

You can display the plans and the tasks used to deploy system plans to managed systems.

**Enhanced password policy**

You can enforce password requirements for locally authenticated users by using the Hardware Management Console (HMC). The enhanced password policy function allows the system administrator to set password restrictions. The enhanced password policy applies to the systems that have HMC installed.

With the enhanced password policy, system administrators can define a single password policy for all users. The HMC provides a medium security password policy, which can be activated by the system administrators to set password restrictions. The system administrator activates the medium security policy or a new user-defined policy. The HMC medium security password policy cannot be removed from the system. The following table lists the attributes of the medium security policy and the default values.

*Table 10. Password attributes for the HMC medium security password policy*

Attribute	Description	Default value
min_pwage	The minimum number of days a password must remain active	1
pwage	The maximum number of days a password might remain active	180
min_length	The minimum length of a password	8
hist_size	The number of previous passwords saved that might not be reused	10
warn_pwage	The number of days a user is warned that the password is about to expire	7
min_digits	The number of digits required to be used in the password	None
min_uppercase	The number of characters that must be uppercase	1
min_lowercase	The number of characters that must be lowercase	6
min_special_chars	The number of special characters that must be in the password	None

**Notes:**

- The HMC medium security password policy does not apply to the **hscroot**, **hscpe**, and **root** user IDs.
- The HMC medium security password policy affects only the locally authenticated users that are managed on the HMC and cannot be enforced on LDAP or Kerberos users.
- The HMC medium security password policy or the user-defined policy allows the system administrators to set the restriction on password reuse.
- The HMC medium security password is read-only and the attributes of HMC medium security password cannot be changed. You can create a new user-defined password to set password restriction.

The HMC medium security password policy can be configured by using the command-line interface (CLI). You can use the following commands to configure the HMC medium security password policy:

### **mkpwdpolicy**

The **mkpwdpolicy** command adds a new password policy by importing the policy from a file, which contains all the parameters, or by creating the policy from the CLI.

### **lspwdpolicy**

The **lspwdpolicy** command lists all the available password policy profiles and searches for specific parameters. You can also view the current active policy.

### **rmpwdpolicy**

The **rmpwdpolicy** command removes an existing inactive password policy.

**Note:** You cannot remove an active medium security policy and the default read-only policy.

### **chpwdpolicy**

The **rmpwdpolicy** command changes parameters in an inactive password policy.

## **Managing the Virtual I/O Server image repository**

As of Version 7.7, or later, you can store the Virtual I/O Server (VIOS) images from a DVD, a saved image, or a Network Installation Management (NIM) server on the HMC. The stored VIOS images can be used for VIOS installation. You must be an HMC super administrator (hmcsuperadmin) to install the VIOS image.

### **About this task**

To manage or to import the VIOS image repository, complete the following steps:

#### **Procedure**

1. In the Console Management work pane, click **Manage Virtual I/O Server Image Repository**.
2. In the Virtual I/O Server Image Repository window, click **Import New Virtual I/O Server Image**.
3. In the Import New Virtual I/O Server Image window, choose to import the VIOS images from a DVD or from a file system.
  - To import the VIOS images from a DVD to the HMC, complete the following steps:
    - a. In the Import Virtual I/O Server Image window, select **Management console DVD**.
    - b. In the **Name** field, enter the VIOS image name that you want to import from the DVD.
    - c. Click **OK**.
  - To import the VIOS images from a Network File System (NFS), File Transfer Protocol (FTP), or Secure Shell File Transfer Protocol (SFTP), complete the following steps:
    - a. In the Import Virtual I/O Server Image window, select **File System**.
    - b. Select **Remote NFS Server**, **Remote FTP Server**, or **Remote SFTP Server**.
    - c. Enter the required details and click **OK**.

---

## **Service Management tasks**

The tasks that are available on the HMC for the **Service Management** tasks are described.

To open these tasks, see “Service Management” on page 12.

**Note:** Depending on the task roles assigned to your user ID you may not have access to all the tasks. See Table 4 on page 15 for a listing of the tasks and the user roles allowed to access them.

### **Create Serviceable Event**

This task reports problems that occurred on your Hardware Management Console to the service provider (for example, the mouse does not work) or lets you test problem reporting.

Submitting a problem is dependent upon whether you have customized this Hardware Management Console to use the Remote Support Facility (RSF) and if it is authorized to automatically call for service. If so, the problem information and service request is sent to the service provider automatically with a modem transmission.

To report a problem on your Hardware Management Console, do the following:

1. Open the **Create Serviceable Event** task from the taskpad.
2. From the **Report a Problem** window, select a problem type from the list displayed.
3. Enter a brief description of your problem in the **Problem Description** input field and then click **Request Service**.

To test problem reporting from the **Report a Problem** window:

1. Select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** input field.
2. Click **Request Service**. The problems are reported to the service provider for the Hardware Management Console. Reporting a problem sends to the service provider the information you provide on **Report a Problem** window, and machine information that identifies the console.

Use the online Help if you need additional information for reporting a problem or testing if problem reporting works.

## Manage Serviceable Events

This task allows you to select the criteria for the set of serviceable events you want to view. When you finish selecting the criteria, you can view the serviceable events that match your specified criteria.

To set the criteria for the serviceable events you to view:

1. Open the **Manage Serviceable Events** task from the Service Management work pane.
2. From the **Manage Serviceable Events** window, provide event criteria, error criteria, and FRU criteria.
3. Click **OK** when you have specified the criteria you want for the serviceable events you want to view.

Use the online Help if you need additional information managing events.

## Load Serviceable Events

This task allows you to load or reload serviceable events from an XML file.

To load serviceable events, do the following

1. Open the **Load Serviceable Events** task from the Service Management work pane.
2. From the **Load Serviceable Events** window, specify the path and name of the XML file.
3. Click **press for update** to proceed.

## Manage Remote Connections

This task enables you to manage remote connections.

**Note:** The HMC's call-home server service must be enabled for you to use this task.

The HMC manages remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, this task allows you to manage the queue manually, if necessary. You can stop transmissions, move priority requests ahead of others, or delete requests.

To manage remote connections, do the following:

1. Open the **Manage Remote Connections** task from the Service Management work pane.

2. From the **Manage Remote Connections** window, a list of transmitting requests being and a list of waiting requests transmitted are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
  - Prioritize a selected request (move it to the top of the queue)
  - Cancel selected requests
  - Cancel all active requests (those being transmitted)
  - Cancel all waiting requests
  - Hold the queue (puts queue on hold after completing current active request)
  - Release the queue
  - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

#### **Related information:**

“Manage Systems Call-Home” on page 101

This task allows you enable or disable the call-home state for managed systems.

## **Manage Remote Support Requests**

This task views or manages call-home requests that the console has submitted.

1. Open the **Manage Remote Support Requests** task from the Service Management work pane.
2. From the **Manage Remote Support Requests** window, a list of active requests and a list of waiting requests are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
  - View all call-home servers
  - Cancel selected requests
  - Cancel all active requests
  - Cancel all waiting requests
  - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

## **Format Media**

This task formats a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

You can use this task to format the following DVD-RAMs:

- Backup/restore
- Service data.

You can format a diskette by supplying a user-specified label.

To format a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key, do the following:

1. Open the **Format Media** task from the HMC Management work pane.
2. From the **Format Media** window, select the type of media you want to format, then click **OK**.
3. Make sure your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
4. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information for formatting a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.



## Manage Dumps

This task manages procedures for dumps of the selected system.

To manage a dump, do the following:

1. Open the **Manage Dumps** task from the Service Management work pane.
2. From the **Manage Dumps** window, select a dump and perform one of the following dump-related tasks:

From **Selected** on the menu bar:

- Copy the dump to media.
- Copy the dump to a remote system.
- Use the call home feature to transmit the dump to your service provider.
- Delete a dump.

From **Actions** on the menu bar:

- Initiate a dump of the hardware and server firmware for the managed system.
- Initiate a dump of the service processor.
- Initiate a dump of the Bulk Power Control service processor.
- Modify the dump capability parameters for a dump type.

From **Status** on the menu bar, you can view the offload progress of the dump.

3. Click **OK** when you have completed this task.

Use the online Help to get additional information for managing dumps.

## Transmit Service Information

Transmit service information so that it can be used for problem determination.

To transmit service information, do the following:

1. In the Service Management work pane, click **Transmit Service Information**.
2. Click one of the following tabs:
  - **Transmit**. Use this page to schedule when to transmit service data to your service provider (specifying frequency in days and time of day) and how you want to transmit the service and performance management information.
  - **FTP**. Use this page to configure the File Transfer Protocol (FTP) information for the FTP server, with or without a firewall, for off loading service information. This service information is extended error data consisting of problem related-data about problems opened on the HMC for the HMC or managed system.
3. Click **OK**.

Use the online Help for additional information about transmitting service information.

## Manage Systems Call-Home

This task allows you enable or disable the call-home state for managed systems.

**Note:** If Customizable Data Replication is **Enabled** on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see "Manage Data Replication" on page 95.

By enabling the call-home state for a managed system this causes the console to automatically contact a service center when a serviceable event occurs. When a managed system is disabled, your service representative is not informed of serviceable events.

To manage call-home for the system(s):

1. Open the **Manage Systems Call-Home** task from the Service Management work pane.
2. From the **Manage Systems Call-Home** window, select a system or systems you want to enable or disable the call-home state.
3. Click **OK** when you have completed the task.

Use the online Help if you need additional information for managing serviceable events notification.

**Related information:**

“Manage Remote Connections” on page 99

This task enables you to manage remote connections.

## Manage Outbound Connectivity

Customize the means for outbound connectivity for the HMC to use to connect to remote service.

**Note:** If Customizable Data Replication is **Enabled** on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see “Manage Data Replication” on page 95.

You can configure this HMC to attempt connections through the local modem, Internet, Internet Virtual Private Network (VPN), or through a remote pass-through system. Remote service is a two-way communication between the HMC and your support system for the purpose of conducting automated service operations. The connection can only be initiated by the HMC.

To customize your connectivity information, do the following:

1. Open the **Manage Outbound Connectivity** task from the Service Management work pane.
2. From the **Manage Outbound Connectivity** window select **Enable local server as call-home server** (a check mark appears) before proceeding with the task.

**Note:** You must first **Accept** the terms described about the information you provided in this task. This allows the local HMC to connect to your service provider's remote support facility for call-home requests.

3. The dial information window displays the following tabs for providing input:
  - Local Modem
  - Internet
  - Internet VPN
  - Pass-Through Systems
4. If you want to allow connectivity over a modem, use the **Local Modem** tab, then select **Allow local modem dialing for service**.
  - a. If your location requires a prefix to be dialed in order to reach an outside line, click **Modem Configuration** and enter the **Dial prefix** in the **Customize Modem Settings** window required by your location. Click **OK** to accept the setting.
  - b. Click **Add** from the **Local Modem** tab page to add a telephone number. When local modem dialing is allowed, there must be at least one telephone number configured.
5. If you want to allow connectivity over the Internet, use the **Internet** tab, then select **Allow an existing internet connection for service**.
6. If you want to configure the use of a VPN over an existing Internet connection to connect from the local HMC to your service provider's remote support facility, use the **Internet VPN** tab.
7. If you want to allow the HMC to use the pass-through systems as configured by the TCP/IP address or host name, use the **Pass-Through Systems** tab.
8. When you complete all the necessary fields, click **OK** to save your changes.



Use the online Help if you need additional information for customizing outbound connectivity information.

## Manage Inbound Connectivity

This task allows your service provider to temporarily access your local console, such as the HMC, or the partitions of a managed system.

To manage inbound connectivity, do the following:

1. Open the **Manage Inbound Connectivity** task from the Service Management work pane.
2. From the **Customize Inbound Connectivity Settings** window:
  - Use the **Remote Service** tab to provide the information necessary to start an attended remote service session.
  - Use the **Call Answer** tab to provide the information necessary to accept incoming calls from your service provider to start an unattended remote service session.
3. Click **OK** to proceed with your selections.

Use the online Help if you need additional information on managing the inbound connectivity.

## Manage Customer Information

This task enables you to customize the customer information for the HMC.

**Note:** If Customizable Data Replication is *Enabled* on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see “Manage Data Replication” on page 95.

The **Manage Customer Information** window displays the following tabs for providing input:

- Administrator
- System
- Account

To customize your customer information, do the following:

1. Open the **Manage Customer Information** task from the Service Management work pane.
2. From the **Manage Customer Information** window, provide the appropriate information on the **Administrator** page.

**Note:** Information is required for fields with an asterisk (\*).

3. Select the **System** and **Account** tabs from the **Manage Customer Information** window to provide additional information.
4. Click **OK** when you have completed the task.

Use the online Help to get additional information about customizing your account information.

## Manage Serviceable Event Notification

This task adds email addresses that notify you when problem events occur on your system and configures how you want to receive notification of system events from the Electronic Service Agent.

To set up notification:

1. Open the **Manage Serviceable Event Notification** task from the Service Management work pane.
2. From the **Manage Serviceable Event Notification** window, you can do the following:
  - Use the **Email** tab to add the email addresses that will be notified when problem events occur on your system.

- Use the **SNMP Trap Configuration** tab to specify locations for sending Simple Network Management Protocol (SNMP) trap messages for Hardware Management Console application program interface events.
3. Click **OK** when you have completed this task.

Use the online Help if you need additional information for managing serviceable events notification.

## Manage Connection Monitoring

This task configures the timers that connection monitoring uses to detect outages and enables or disables connection monitoring for selected machines.

You can view and, if authorized, change connection monitoring settings by machine. Connection monitoring generates serviceable events when communication problems are detected between the HMC and managed systems. If you disable connection monitoring, no serviceable events are generated for networking problems between the selected machine and this HMC.

To monitor the connections, do the following:

1. Open the **Manage Connection Monitoring** task from the Service Management work pane.
2. From the **Manage Connection Monitoring** window, adjust the timer settings, if required, and enable or disable the server.
3. Click **OK** when you have completed the task.

Use the online Help if you need additional information about connection monitoring.

## Call-Home Setup Wizard

Learn how to open the Call-Home Setup wizard using the HMC interface.

### About this task

To open the Call-Home Setup wizard, do the following:

### Procedure

1. In the navigation area, select **Service Management**.
2. In the contents area, select **Call-Home Setup Wizard**. The Connectivity and Call-Home Servers wizard opens. Follow the instructions in the wizard to configure call-home.

---

## Updates

Display tasks to manage Licensed Internal Code (LIC) on your HMC, managed system, power subsystem, or I/O adapters.

Use the **Update HMC** button to update Licensed Internal Code on the HMC. Before updating LIC on the HMC, see “Update HMC” on page 105.

Other tasks are used to update managed system, power subsystem, and I/O adapter LIC. To launch these tasks, see “Launching tasks for managed objects” on page 7. The following sets of tasks are represented in the taskpad, tasks menu, or context menu. The tasks listed in the taskpad change as selections are made in the work area. The context is always listed at the top of the taskpad in the format Task: Object.

To display the tasks, do the following:

1. Select the **Updates** node in the navigation pane.
2. Select a managed object to apply updates on.
3. From the taskpad, click on the task you want to perform.

## Update HMC

Identify HMC version, release, service and build levels.

When you click **Updates**, the HMC displays the following information:

- Version
- Release
- Service Pack
- Build Level
- Base Version
- Serial Number of the HMC
- Bios Version on the HMC

For more information about updating your HMC code, see *Updating, upgrading, and migrating your HMC machine code*.

## Managed system updates

When a managed system is selected, Updates tasks perform a guided update of managed system, power subsystem, or I/O Licensed Internal Code.

Licensed Internal Code can be changed in two ways. You can upgrade the Licensed Internal Code installed on a managed system to a new release, or update the existing Licensed Internal Code running on the system.

An update of a current Licensed Internal Code release may fix problems or add additional function. Updating the Licensed Internal Code may or may not be a disruptive process. Updates that do not disrupt the system are called concurrent updates. To update the Licensed Internal Code currently installed on the managed system, click **Change Licensed Internal Code for the current release** task.

A new release of the Licensed Internal Code may add support for new hardware or add new function. Upgrading the Licensed Internal Code to a new release is *always a disruptive process* requiring a complete shut down, power off, and restart of the system. To upgrade the Licensed Internal Code to a new release, click **Upgrade Licensed Internal Code to a new release**.

Concurrent updates allow the system and the applications running on the system to continue to run as the Licensed Internal Code update is applied. This appreciably lessens the system downtime associated with Licensed Internal Code maintenance. Most updates released will be concurrent. However, certain types of problems are critical to fix and can be fixed only with a disruptive update. **View system information** allows you to view the levels of the Licensed Internal Code available in a repository and determine which of the available updates are concurrent and which are disruptive.

If the update is disruptive, you are given the option of installing and activating (incurring the disruption) or deferring the activation to a more convenient time. Concurrent updates can only be done for managed system Licensed Internal Code.

**Note:** Checking is done before the Licensed Internal Code update to assure that the system is in the correct state for an update. The state of the system must not change during a code update. For example, partitions should not be shut down during the Licensed Internal Code update.

Use the **Flash Side Selection** task to select which flash side will be active after the next activation. (This task is intended for service user mode only.)

Use the **Check system readiness** task to check that all systems selected are in the correct state for the Licensed Internal Code update.

Choose the **View system information** task to view the level of the Licensed Internal Code currently installed on your managed system or I/O. When a repository is selected, **View system information** also displays retrievable levels of the Licensed Internal Code available in the repository.

### Change Licensed Internal Code for the current release

Use this task to apply updates to the currently installed Licensed Internal Code (also known as system firmware) on your system within the current release.

**Important:** The HMC might need to be updated prior to updating the Licensed Internal Code within the current release. Check the minimum HMC code level section at the Firmware and HMC: Firmware Description Files website (<http://www.ibm.com/support/fixcentral/firmware/fixDescriptionFiles>).

If the link to the code from the Fix Central website is not working, contact IBM Service to get the correct RPM and XML files.

For more information about Licensed Internal Code updates, see the following information:

- Licensed Internal Code: Frequently asked questions
- System Firmware (Microcode) Service Strategies and Best Practices guide

If you have completed a code update from a repository to one of your managed systems or power subsystems, that code is available in the hard drive repository on the HMC for installation on other systems. You can select **Hard Drive** to update other managed systems or power subsystems with the same code.

Multiple managed systems can be updated simultaneously by selecting them from the target list.

Files are selectively downloaded to the HMC to apply Licensed Internal Code updates. From this task, you can do the following actions:

- View current levels of Licensed Internal Code on a managed system, power subsystem, or I/O.
- View retrievable levels of Licensed Internal Code in a repository.
- Install and activate Licensed Internal Code updates (update to a new level of the Licensed Internal Code).
- Remove and deactivate Licensed Internal Code updates (downgrade to a previous level of the Licensed Internal Code).

Select **Start Change Licensed Internal Code wizard** to perform a guided update of managed system, power, and I/O Licensed Internal Code, complete the following steps:

1. A **System readiness check** is automatically performed to check that the system is in the right state for the Licensed Internal Code update. If the readiness check fails, actions needed to correct the problems that prevent the update are reported to you.
2. Choose a repository from which to update your system. You can update the system from any of the following repositories:
  - IBM's service website.
  - Removable media. Ensure that the DVD or CD is in the HMC DVD drive or that the USB flash drive is attached to the HMC.
  - FTP site.
  - HMC hard disk drive.

If you choose **FTP site**, you are prompted for the FTP host name, user ID, password, and the directory in which the update is located.

3. Select the type of update to install, which is **Managed system and Power LIC**. If there are no Licensed Internal Code updates available in the repository for the type of update that is chosen, no prompts for installation occur.

4. Confirm that the update as displayed is the correct update. Displayed is the chosen repository, the target, or targets of the update, the concurrency status of the target (disruptive or concurrent), and the type of installation. To change the update, select **Advanced Options**.
5. If no changes are wanted, continue with the update. Accept the license agreement.
6. Confirm the update.
7. A progress window displays until the update completes.

Select **View system information** to examine current Licensed Internal Code levels on a managed system, power subsystem, or I/O, including levels retrievable from a repository.

Select **Advanced features** to update managed system and power the Licensed Internal Code with more options and more targeting choices.

## Upgrade Licensed Internal Code to a new release

A new release level of Licensed Internal Code supports major new function such as the introduction of new hardware models and significant function or features enabled by firmware. In addition to the new function and hardware support, new release levels also contain fixes. Upgrading from one release level to another is disruptive to system operations.

Release levels can be skipped. You can upgrade from release level A to release level D without having to install release level B and C. New release levels of the Licensed Internal Code are installed with this task.

**Important:** The HMC might need to be updated or upgraded prior to upgrading the Licensed Internal Code to a new release. Check the minimum HMC code level section at the Firmware and HMC: Firmware Description Files website (<http://www.ibm.com/support/fixcentral/firmware/fixDescriptionFiles>).

For more information about Licensed Internal Code updates, see the following information:

- Licensed Internal Code: Frequently asked questions
- System Firmware (Microcode) Service Strategies and Best Practices guide

If the link to the code from the Fix Central website is not working, contact IBM Service to get the correct RPM and XML files.

If you have completed a code upgrade from a repository to one of your managed systems or power subsystems, that code is available in the hard drive repository on the HMC for installation on other systems. You can select **Hard Drive** to update other managed systems or power subsystems with the same code.

Multiple managed systems can be upgraded simultaneously by selecting them from the target list.

To install a new release of Licensed Internal Code, do the following:

1. When you select **Upgrade Licensed Internal Code to a new release**, a readiness check is performed on the system before the task progresses. If the readiness check fails, actions needed to correct the problems preventing the upgrade will be reported to you.
2. Choose a repository from which to upgrade your system. You can update the system from any of the following repositories:
  - IBM's service website.
  - Removable media. Ensure that the DVD or CD is in the HMC DVD drive or that the USB flash drive is attached to the HMC.
  - FTP site.
  - HMC hard disk drive.

If you choose **FTP site**, you are prompted for the FTP host name, user ID, password, and the directory in which the update is located.

3. Select the Licensed Internal Code upgrade, managed system or power subsystem you want. After verification of the repository content and targeted systems is completed, the license agreement panel is displayed.
4. Select **Accept** on the license agreement panel, and the confirmation panel is displayed.
5. If any actions are listed at the bottom of the confirmation panel, complete them, and then click **OK** to confirm that the upgrade should begin. A progress panel displays the results as the upgrade proceeds. At the end of the process, the new release level of Licensed Internal Code will be installed on both the t-side (temporary side) and the p-side (permanent side).

## Flash Side Selection

Select which flash side will be active after the next activation.

**Note:** This task is intended for Service User mode only.

**Attention:** If you select p-side for the next activation, this action disables concurrent Licensed Internal Code update.

The flash side is the nonvolatile storage location in the flexible service processor (FSP), divided into t-side (temporary side) and p-side (permanent side), allowing for storing two levels of code. When the p-side is selected, concurrent LIC update is disabled.

## Check system readiness

Use this task to confirm that the managed system is in the correct state to perform a Licensed Internal Code update or upgrade successfully.

Before updating or upgrading Licensed internal code, all managed systems to be updated must be in Operating, Standby, Power Off, or Recovery state. All flexible service processors (FSP) for the managed system must be correctly connected to the HMC. Any problems found during the check will be reported to you to correct before updating LIC. A readiness check will automatically be performed before any update or upgrade begins.

## View system information

Examine current LIC levels on the managed system, including installed, activated, and accepted levels. If a repository is selected, this task also displays retrievable levels available in a repository.

The **Installed** level of LIC is the level that will be activated and loaded into memory at the next system restart. The **Activated** level of LIC is the level that is activated and loaded into memory at this time. The **Accepted** level of LIC is a committed level of LIC that can be returned to, if necessary. This is the level of code on the p-side (permanent side). The **Inactivated Deferred** level of LIC is the latest inactivated level that contains deferred updates. A deferred update requires a system restart to activate.

**Concurrent LIC update status** indicates whether concurrent LIC update is enabled or disabled. A concurrent update can be installed and activated without rebooting any partitions or disrupting applications.

**Reason for disablement** indicates why concurrent LIC update is disabled. This might include the following:

- The permanent side is active
- A temporary LIC level is active

A concurrent LIC update can be installed and activated without rebooting partitions or disrupting applications.



---

## Remote operations

Connect to and use the HMC remotely.

Remote operations use the GUI used by a local HMC operator or the command line interface (CLI) on the HMC. You can perform operations remotely in the following ways:

- Use a remote HMC
- Use a Web browser to connect to a local HMC
- Use an HMC remote command line

The *remote HMC* is an HMC that is on a different subnet from the service processor, therefore the service processor cannot be auto discovered with IP multicast.

To determine whether to use a remote HMC or Web browser connected to a local HMC, consider the scope of control that you need. A remote HMC defines a specific set of managed objects that are directly controlled by the remote HMC, while a Web browser to a local HMC has control over the same set of managed objects as the local HMC. The communications connectivity and communications speed is an additional consideration; LAN connectivity provides acceptable communications for either a remote HMC or Web browser control.

### Related information:

“Manage Certificates” on page 89

Use this task to manage the certificates used on your HMC. It provides the capability of getting information on the certificates used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates or signing certificates.

“Remote Command Execution” on page 94

This task is used to enable remote command execution using the ssh facility.

## Using a remote HMC

A remote HMC gives the most complete set of functions because it is a complete HMC; only the process of configuring the managed objects is different from a local HMC.

As a complete HMC, a remote HMC has the same setup and maintenance requirements as a local Hardware Management Console. A remote HMC needs LAN TCP/IP connectivity to each managed object (service processor) that is to be managed; therefore, any customer firewall that may exist between the remote HMC and its managed objects must permit HMC to service processor communications to occur. A remote HMC may also need communication with another HMC for service and support. Table 11 shows the ports a remote HMC uses for communications.

*Table 11. Ports used by a Remote HMC for Communications*

Port	Use
udp 9900	HMC to HMC discovery
tcp 9920	HMC to HMC commands

A remote HMC needs connectivity to IBM (or another HMC that has connectivity to IBM) for service and support. The connectivity to IBM might be in the form of access to the Internet (through a company firewall), or a dialed connection through a customer-provided switched telephone connection that uses the supplied modem (see “Manage Outbound Connectivity” on page 102). A remote HMC cannot use the supplied modem for communication with a local HMC or a service processor.

Performance and the availability of the status information and access to the control functions of the service processor depends on the reliability, availability, and responsiveness of the customer network that

interconnects the remote HMC with the managed object. A remote HMC monitors the connection to each service processor and attempts to recover any lost connections and can report those connections that cannot be recovered.

Security for a remote HMC is provided by the HMC user-login procedures in the same way as a local HMC. As with a local HMC, all communication between a remote HMC and each service processor is encrypted. Certificates for secure communications are provided, and can be changed by the user if desired (see “Manage Certificates” on page 89).

TCP/IP access to the remote HMC is controlled through its internally managed firewall and is limited to HMC related functions.

## Using a web browser

If you need occasional monitoring and control of managed objects connected to a single local HMC, use a web browser. An example of using the web browser might be an off-hours monitor from home by an operator or system programmer.

Each HMC contains a web server that can be configured to allow remote access for a specified set of users. If a customer firewall exists between the web browser and the local HMC, the ports must be accessible, and the firewall should allow incoming requests on these ports. Table 12 shows the ports a web browser needs for communicating with an HMC.

*Table 12. Ports used by a web browser for communications to the HMC*

Port	Use
tcp 443	Secure browser access to web server communication
tcp 8443	Secure browser access to web server communication
tcp 9960	Browser applet communication

After an HMC has been configured to allow web browser access, a web browser gives an enabled user access to all the configured functions of a local HMC, except those functions that require physical access to the HMC, such as those that use the local diskette or DVD media. The user interface presented to the remote web browser user is the same as that of the local HMC and is subject to the same constraints as the local HMC.

The web browser can be connected to the local HMC using a LAN TCP/IP connection and using only encrypted (HTTPS) protocols. Logon security for a web browser is provided by the HMC user-login procedures. Certificates for secure communications are provided, and can be changed by the user (see “Manage Certificates” on page 89).

Performance and the availability of the status information and access to the control functions of the managed objects depends on the reliability, availability, and responsiveness of the network that interconnects the web browser with the local HMC. Because there is no direct connection between the web browser and the individual managed objects, the web browser does not monitor the connection to each service processor, does not do any recovery, and does not report any lost connections. These functions are handled by the local HMC

The web browser system does not require connectivity to IBM for service or support. Maintenance of the browser and system level is the responsibility of the customer.

If the URL of the HMC is specified using the format `https://xxx.xxx.xxx.xxx` (where `xxx.xxx.xxx.xxx` is the IP address) and Microsoft Internet Explorer is used as the browser, a hostname mismatch message is displayed. To avoid this message, a Firefox browser is used or a hostname is configured for the HMC, using the **Change Network Settings** task (see “Change Network Settings” on page 83), and this hostname



is specified in the URL instead of an IP address. For example, you can use the format `https://hostname.domain_name` or `https://hostname` (for example, using `https://hmc1.ibm.com` or `https://hmc1`).

## Using the HMC remote command line

An alternative to performing tasks on the HMC graphical user interface is using the command line interface (CLI).

You can use the command line interface in the following situations:

- When consistent results are required. If you have to administer several managed systems, you can achieve consistent results by using the command line interface. The command sequence can be stored in scripts and run remotely.
- When automated operations are required. After you have developed a consistent way to manage the managed systems, you can automate the operations by invoking the scripts from batch-processing applications, such as the **cron** daemon, from other systems.

On a local HMC, you can use the command line interface in a terminal window. To open a terminal window, use the **Open Restricted Shell Terminal** task from the HMC Management work pane.

## Setting up secure script execution between SSH clients and the HMC

You must ensure that your script executions between SSH clients and the HMC are secure.

HMCs typically are placed inside the machine room where managed systems are located, so you might not have physical access to the HMC. In this case, you can remotely access it using either a remote Web browser or the remote command line interface.

**Note:** To enable scripts to run unattended between an **SSH** client and an HMC, the SSH protocol must already be installed on the client's operating system.

To enable scripts to run unattended between an **SSH** client and an HMC, do the following:

1. Enable remote command execution. For more information, see “Enabling and disabling HMC remote commands” on page 112
2. On the client's operating system, run 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.

3. On the client's operating system, use `ssh` and run the **mkauthkeys** command to update the HMC user's `authorized_keys2` file on the HMC by using the following command:

```
ssh hmcuser@hmchostname "mkauthkeys --add '<the contents of $HOME/.ssh/id_rsa.pub>' " "
```

To delete the key from the HMC, can use the following command:

```
ssh hmcuser@hmchostname "mkauthkeys --remove 'joe@somehost' "
```

To enable password prompting for all hosts that access the HMC through **ssh**, use the **scp** command to copy the key file from the HMC: `scp hmcuser@hmchostname:.ssh/authorized_keys2 authorized_keys2`

Edit the `authorized_keys2` file and remove all lines in this file. Then copy it back to the HMC: `scp authorized_keys2 hmcuser@hmchostname:~/.ssh/authorized_keys2`

## Enabling and disabling HMC remote commands

You can enable or disable the remote command line interface access to the HMC.

To enable or disable remote commands, do the following:

1. Open the **Remote Command Execution** task from the HMC Management work pane.
2. From the **Remote Command Execution** window:
  - To enable remote commands, select **Enable remote command execution using the ssh facility**.
  - To disable remote commands, make sure **Enable remote command execution using the ssh facility** is not selected.
3. Click **OK**.

## Web browser requirements

Learn about the requirements your web browser must meet to monitor and control the HMC.

HMC web browser support requires HTML 2.0, JavaScript 1.0, Java™ Virtual Machine (JVM), and cookie support in browsers that will connect to the HMC. Contact your support personnel to assist you in determining if your browser is configured with a Java Virtual Machine. The web browser must use HTTP 1.1. If you are using a proxy server, HTTP 1.1 must be enabled for the proxy connections. Additionally, pop-ups must be enabled for all HMCs addressed in the browser if running with pop-ups disabled. The following browsers have been tested:

**Microsoft Internet Explorer 6.0, Internet Explorer 7.0, Internet Explorer 8.0, and Internet Explorer 9.0 are supported.**

- Internet Explorer 10.0 Preview is not supported; however, the Internet Explorer compatibility mode might alleviate most problems.
- If your browser is configured to use an Internet proxy, then local Internet addresses are included in the exception list. Consult your network administrator for more information. If you still need to use the proxy to get to the Hardware Management Console, enable **Use HTTP 1.1 through proxy connections** under the **Advanced** tab in your Internet Options window.

### Mozilla Firefox

HMC Version 7.6 supports Mozilla Firefox Version 4 through Mozilla Firefox Version 10. Ensure that the JavaScript options to raise or lower windows and to move or resize existing windows are enabled. To enable these options, click the **Content** tab in the browser's Options dialog, click **Advanced** next to the Enable JavaScript option, and then select the Raise or lower windows option and the Move or resize existing windows options. Use these options to easily switch between HMC tasks.

### Other web browser considerations

Session cookies need to be enabled in order for ASMI to work when connected to HMC remotely. The ASM proxy code saves session information and uses it.

### Internet Explorer

1. Click **Tools > Internet Options**.
2. Click the **Privacy** tab and select **Advanced**.
3. Determine whether **Always allow session cookies** is checked.
4. If not checked, select **Override automatic cookie handling** and **Always allow session cookies**.
5. For the First-party Cookies and Third-party Cookies, choose block, prompt, or accept. Prompt is preferred, in which case you are prompted every time a site tries to write cookies. Some sites need to be allowed to write cookies.

### Firefox

1. Click **Tools > Options**.
2. Click the **Cookies** Tab.
3. Select **Allow sites to set cookies**.
4. If you want to allow only specific sites, select **Exceptions**, and add this HMC to allow access.

## Preparing to use the web browser

Perform the necessary steps to prepare to use a web browser to access the HMC.

Before you can use a web browser to access an HMC, you must do the following:

- Configure the HMC to allow remote control for specified users.
- For LAN-based connections, know the TCP/IP address of the HMC to be controlled, and have correctly set up any firewall access between the HMC and the web browser.
- Have a valid user ID and password assigned by the access administrator for HMC web access.

## Logging in to the HMC from a LAN-connected web browser

Log in to the HMC remotely from a LAN-connected web browser.

Use the following steps to log in to the HMC from a LAN-connected web browser:

1. Ensure that your web browser PC has LAN connectivity to the desired HMC.
2. From your web browser, enter the URL of the desired HMC, using the format *https://hostname.domain\_name* (for example: *https://hmc1.ibm.com*) or *https://xxx.xxx.xxx.xxx*.

If this is the first access of the HMC for the current web browser session, you can receive a certificate error. This certificate error is displayed if:

- The web server contained in the HMC is configured to use a self-signed certificate and the browser has not been configured to trust the HMC as an issuer of certificates,
- The HMC is configured to use a certificate signed by a Certificate Authority (CA) and the browser has not been configured to trust this CA.

In either case, if you know that the certificate being displayed to the browser is the one used by the HMC, you can continue and all communications to the HMC will be encrypted.

If you do not want to receive notification of a certificate error for the first access of any browser session, you can configure the browser to trust the HMC or the CA. In general, to configure the browser, use one of the following methods:

- You must indicate that the browser will permanently trust the issuer of the certificate
- By viewing the certificate and installing, to the database of trusted CAs, the certificate of the CA that issued the certificate used by the HMC.

If the certificate is self-signed, the HMC itself is considered the CA that issued the certificate.

3. When prompted, enter the user name and password assigned by your administrator.

---

## Customizable data replication

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

**Note:** Before enabling this replication service, you may want to save your original data settings in case you need to restore these settings at a future time. See “Save Upgrade Data” on page 83.

The following types of data can be configured:

- Customer information data
  - Administrator information (customer name, address, telephone number, and so on.)

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

The Customizable Data Replication service can be enabled for the following types of operations:

- **Peer-to-peer** (see “Peer-to-peer replication”).  
Provides automatic replication of the selected customized data types between peer HMCs. Changes made on any of these consoles are replicated to the other consoles.
- **Master-to-slave** (see “Master-to-slave replication” on page 115).  
Provides automatic replication of the selected customized data types from one or more designated master HMCs to one or more designated slave HMCs. Changes made on a master console are automatically replicated to the slave console.

**Related information:**

“Manage Data Replication” on page 95

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

## Peer-to-peer replication

Configure automatic replication of the selected customized data types between peer HMCs.

To configure automatic replication of the selected customized data types between peer HMCs, do the following:

1. Log in the HMC using a user ID that has administrator roles.
2. In the HMC Management work pane, click **Manage Data Replication**.
3. Select **Enable**.
4. Click **New**.
5. Complete one of the following steps:
  - Select an HMC to be used as a data source from the list, and click **Add**.
  - In the **TCP/IP Address Information** field, type the TCP/IP address of the HMC to be a used as a data source, and then click **Find**.
6. In the **Customizable Data Types** list, select the types of data that you want to replicate from a peer HMC currently selected.
7. Choose one of the following actions:
  - Click **Save** to close the Manage Data Replication window.
  - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
  - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the master provide their levels to the local machine. This option is not available if the local HMC is not defined to have any data sources.
  - Click **Status** to show the status of this task on this machine.

8. Repeat these steps on each of the HMCs that you want to act as peers with one another. Once communication is established between the HMCs, the requested types of customizable data are automatically replicated from one HMC to the other immediately following the change in the data itself.

## Master-to-slave replication

Master-to-slave replication provides automatic replication of the selected customized data types from one or more designated master HMCs to one or more designated slave HMCs.

To set up a master console, do the following:

1. Log in the HMC using a user ID that has administrator roles.
2. From the HMC Management work pane, click **Manage Data Replication**.
3. Select **Enable**, then click **Save**.

**Note:** If you want to configure additional master consoles, see “Peer-to-peer replication” on page 114

To set up the slave console, do the following:

1. Log in the HMC using a user ID that has administrator roles.
2. Select **Manage Data Replication**.
3. Select **Enable**.
4. Click **New**.
5. Complete one of the following steps:
  - Select an HMC to be used as a master data source from the list, then click **Add**.
  - In the **TCP/IP Address Information** field, enter the TCP/IP address of the HMC to be used as the master data source, then click **Find**.
6. Select the types of data that you want to accept from the HMC.

**Note:** When configuring a HMC as a slave, you should check the types of customizable data from the **Local Customizable Data Change Warnings** list that should generate warnings to a user when manual changes are made to that data on this HMC. Manually updating data on the slave HMC will change the local data level to a higher level than the master. Changes on the master HMC will then not replicate to this HMC until the master data level exceeds that on the slave, or a **Sync from Master** or **Push to Slaves** task is run to resynchronize the data levels on master and slave.

7. Choose one of the following actions:
  - Click **Save** to close the Manage Data Replication window.
  - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
  - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the masters provide their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
  - Click **Status** to show the status of this task on this machine.
8. Repeat these steps on any additional HMCs that you want to configure as a slave.
9. Once communication is established between all of the HMCs, the master consoles remains synchronized with each other, providing redundancy in the event that one of the master consoles becomes unavailable. The slave consoles are kept synchronized with whichever master console provides the data to them first.

## Data replication

As data is replicated from one HMC to another, an internal level indicator for the data being replicated is recorded each time the data is altered on the data source. Learn about how to force the replication of data from one or more data sources.

Each HMC keeps track of the level indicator for each type of data and will not accept data from a data source when the level indicator is not greater than that on the receiving HMC.

If you need to force the replication of data from one or more data sources and the level indicator on the receiving HMC is greater than that of the data sources, do the following:

1. Log in the HMC using a user ID that has administrator roles.
2. In the HMC Management work pane, click **Manage Data Replication**.
3. Deselect all the data types from the **Customizable Data Types** list.

**Note:** If you just want to reset the level indicator for a particular data type, just deselect that data type.

4. Click **Save**.
5. In the HMC Management work pane, click **Manage Data Replication**.
6. Select the types of data from the **Customizable Data Types** list you just deselected.
7. Click **Save**.

**Note:** Deselecting and then reselecting the data types resets the internal level indicators for the specified types of data and forces replication of the data from the data sources.

---

## 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 grant you any license to these patents. You can send license inquiries, in writing, to the manufacturer.

For license inquiries regarding double-byte character set (DBCS) information, contact the Intellectual Property Department in your country or send inquiries, in writing, to the manufacturer.

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** THIS PUBLICATION IS PROVIDED "AS IS " WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. 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.

Any references in this information to websites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this product and use of those websites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact the manufacturer.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the



same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to the manufacturer, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. The manufacturer, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. The manufacturer shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. \_enter the year or years\_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

---

## Programming interface information

This Managing the Hardware Management Console publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM Hardware Management Console Version 7 Release 7.7.0 Maintenance Level 0.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).



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

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

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

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

---

## Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

**Applicability:** These terms and conditions are in addition to any terms of use for the the manufacturer website.

**Personal Use:** You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

**Commercial Use:** You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of the manufacturer.

**Rights:** Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.





Printed in USA