Power Systems

Managing the Hardware Management Console

Note

Before using this information and the product it supports, read the information in “Notices” on page 117.

This edition applies to IBM Hardware Management Console Version 9 Release 2 Maintenance Level 950 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Managing the HMC

Learn how to use the Hardware Management Console (HMC).

About this task

Learn about the tasks that you can use on the console and how to navigate by using the web-based user interface with graphical views of managed systems and simplified navigation.

Note: Many of the HMC tasks that are listed here can also be performed by using PowerVC. For more information about the tasks that you can perform by using PowerVC, see HMC and PowerVC.

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.

November 2020

- Added the following topics:
  - "Validate Maintenance Readiness" on page 61
  - "Manage Virtual I/O Server Backups" on page 84
- Updated the following topics:
  - "Create Partition" on page 42
  - "Serviceable Events Manager" on page 47
  - "Add FRU" on page 50
  - "Exchange FRU" on page 51
  - "Remove FRU" on page 51
  - "Partition content pane" on page 56
  - "Partition Properties" on page 57
  - "Serviceable Events Manager" on page 63

May 2020

- Updated the following topics:
  - "HMC tasks, user roles, IDs, and associated commands" on page 9
  - "Partition Templates" on page 83
  - "Hardware Virtualized I/O" on page 66

February 2020

Updated the following topic:

- "VIOS Images" on page 83

November 2019

- Added the following topic:
  - "Logging on to the Hardware Management Console (HMC) when PowerSC MFA is configured on the HMC" on page 3

- Updated the following topics:
  - “Introduction to the HMC” on page 2
  - “Predefined user IDs and passwords” on page 4
  - “Partition Properties” on page 57
  - “Hardware Virtualized I/O” on page 66
  - “Console Default Settings” on page 77
  - “Backup Management Console Data” on page 80
  - “Partition Templates” on page 83
  - “Manage Task and Resource Roles” on page 89
  - “Manage Event Notification” on page 104

May 2019

- Added the following topics:
  - “Netboot” on page 58
  - “Manage Groups” on page 72
- Updated the following topics:
  - “System content pane” on page 30
  - “Create Partition” on page 42
  - “Processor, Memory, I/O” on page 43
  - “Partition content pane” on page 56
  - “Change User Password” on page 86

August 2018

- Added the following topics:
  - “Manage MFA” on page 96
  - “Console Default Settings” on page 77
  - “Managing OpenBMC-based and BMC-based systems by using the HMC” on page 110
- Updated the “Change Network Settings” on page 75 topic.

December 2017

- Added information for HMC Version 9, Release 1, or later on IBM Power Systems servers that contain the POWER9™ processor.

Introduction to the HMC

Learn about some of the concepts and functions of the Hardware Management Console (HMC) and the user interface that is used for accessing those functions.

You can configure and manage servers on the HMC. 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 9, Release 1.

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 is assigned by a customer-

supplied DHCP server or manually assigned by using the Advanced System Management Interface (ASMI).

Physical proximity

Before HMC Version 7, at least one local HMC was required to be physically located near the managed systems. As an alternative to the local HMC, you can use a supported device, such as a personal computer that has connectivity and authority to operate through a remotely attached HMC. The local device must be in the same room as your server and at a distance of 8 m (26 ft) from your server. The local device must have the functional capability that is equivalent to the HMC that it replaces and that is needed by the service representative to service the system. For a virtual HMC, the functional capabilities also include the method of transferring service data, such as firmware updates or diagnostic data, and transferring the log information to and from the HMC.

Redundant or Dual HMCs

A server might be managed by either 1 or 2 Hardware Management Consoles. When two Hardware Management Consoles manage one system, they are peers, and each HMC can be used to control the managed system. The best practice is to attach one HMC to the supported networks or HMC ports of the managed systems. The networks are intended to be independent. Each HMC might be the DCHP 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.

Redundant or Dual HMCs that manage the same server must not be at different version and release levels. For example, an HMC at Version 7 Release 7.1.0 and an HMC at Version 7 Release 3.5.0 cannot manage the same server. The HMCs must be at the same version and release level.

When the server is connected to the higher version of the management console, the partition configuration is upgraded to the latest version. After the partition configuration upgrade, lower levels of the management consoles will not be able to interpret the data correctly. After the server is managed by the higher version of the management console, you must first initialize the server before you can go back to the lower version of the management console. You can restore a backup that is taken at the older level or re-create the partitions. If the server is not initialized, one of the following outcomes can occur depending on the version of the lower-level HMC:

- HMC Version 7 Release 7.8.0 and later reports a connection error of **Version mismatch** with reference code **Save Area Version Mismatch**.
- HMC Version 7 Release 7.7.0 and earlier might report a server state of **Incomplete** or **Recovery**. In addition, partition configuration corruption can also occur.

Logging on to the Hardware Management Console (HMC) when PowerSC MFA is configured on the HMC

Learn how to log in to the HMC when IBM PowerSC Multi-factor Authentication (MFA) is configured on the HMC.

If IBM PowerSCMFA is enabled on the HMC and the user is configured on the PowerSC MFA server, you can choose to log in to the HMC by first entering the user ID and a policy name that is provided by your security administrator. You are then prompted to provide additional credentials.

In the HMC login page, if you click **Policy Name**, the authentication mechanism is set to the in-band authentication type. For example, if the policy that you want to use is associated with the Rivest-Shamir-Adleman (RSA) authentication method, you can enter the secure ID passcode that you received from the RSA secure ID device or the application. Then, click **Next or Sign In** to log in to the HMC.

Notes:

- If MFA is not enabled on the HMC, you can log in to the HMC with the user ID and password.
- If you obtain a cache token credential (CTC) code from the PowerSC MFA server that is configured by your security administrator, enter the CTC code in the **Password** field.

Predefined user IDs and passwords

Predefined user IDs and passwords are included with the Hardware Management Console (HMC). It is imperative to the security of your system that you change the `hscroot` predefined password immediately.

If the password expires when you try to log in to the HMC, complete the following steps:

1. Enter the **Current Password** and the **New Password**.
2. Re-enter the new password in the **Confirmation new password** field.
3. Click **OK**. If the new password complies with the current password policy, the password for the HMC is changed.

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 be used only by a member of the super administrator role.

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 title bar, the navigation area, the content pane, the menu pod, and the dock pod.

The *title bar*, across the top of the workplace window, identifies the product, any user that is logged in, and help options.

The *navigation area*, in the left portion of the window, contains the primary navigation links for selecting your system and starting tasks for your HMC.

The *content pane*, in the middle portion of the window, displays information that is based on the current selection from the navigation area. For example, when **All Systems** is selected in the navigation area, all the available systems are shown in the content pane.

The *menu pod*, in the left portion of the window, is displayed after you select a system and provides quick access to commonly used HMC tasks and views of resources and properties.

The *dock pod*, in the right portion of the window, displays the *Pins* function that can be used to pin any user-selected HMC task. This function allows for quick access to these tasks.

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 you drag 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 task within the work pane border that separates the resources table from the taskpad.

You can change the layout of the *content pane* according to your preference by clicking **Display Gallery View**, **Display Table View**, or **Display Relationship View**.

You can reposition columns in tables by selecting and dragging a column to a new position. You can also select which columns to display by clicking the drop-down menu that is located next to the last column of each table. You can save your preferences by clicking the **Save User Preferences** icon.

You can change how many rows are displayed in tables on each page by clicking one of the **Items per page** (**10**, **20**, **30**, or **50**) icons that are located below each table.

Note: Pop-up windows must be enabled for full functionality of the HMC.

Overview of menu options

Learn about the menu options and associated tasks that are available in the Hardware Management Console (HMC).

The menu options and tasks that are described in this section are available in the HMC interface.

Table 2. HMC menu options

Menu	Submenu	Options/Tasks
Resources 	All Systems	View All Systems
	All Partitions	View All Partitions
	All Virtual I/O Servers	View All Virtual I/O Servers
	All Frames	View All Frames
	All Power Enterprise Pools	View All Power Enterprise Pools
	All Shared Storage Pool Clusters	View All Shared Storage Pool Clusters
	All Groups	View All Groups

Table 2. HMC menu options (continued)		
Menu	**Submenu**	**Options/Tasks**
HMC Management 	Console Settings	Launch Guided Setup Wizard
		View Network Topology
		Test Network Connectivity
		Change Network Settings
		Change Performance Management Settings
		Change Date and Time
		Change Language and Locale
	Console Management	Shut Down or Restart the Management Console
		Schedule Operations
		View Licences
		Update the Hardware Management Console
		Manage Install Resources
		Manage Virtual I/O Server Image Repository
		Format Media
		Backup Management Console Data
		Restore Management Console Data
		Save Upgrade Data
		Manage Data Replication
	Template Library	System and Partition Library
	Updates	Not available (use the Update the Hardware Management Console option instead)

Table 2. HMC menu options (continued)		
Menu	**Submenu**	**Options/Tasks**
Users and Security 	Users and Roles	Change User Password
		Manage User Profiles and Access
		Manage Users and Tasks
		Manage Task and Resource Roles
	Systems and Console Security	Manage Certificates
		Manage LDAP
		Manage KDC
		Enable Remote Command Execution
		Enable Remote Operation
		Enable Remote Virtual Terminal

Table 2. HMC menu options (continued)		
Menu	**Submenu**	**Options/Tasks**
Serviceability 	Console Events Logs	View Console Events window
	Serviceable Events Manager	Serviceable Events Manager window
	Events Manager for Call Home	Events Manager for Call Home window
	Service Management	Create Serviceable Event
		Manage Remote Connections
		Manage Remote Support Requests
		Manage Dumps
		Transmit Service Information
		Schedule Service Information
		Format Media
		Perform Management Console Trace
		View Management Console Logs
		View Component Logs
		Electronic Service Agent Setup Wizard
		Authorize User
		Enable Electronic Service Agent
		Manage Outbound Connectivity
		Manage Inbound Connectivity
		Manage Customer Information
		Manage Serviceable Event Notification
		Manage Connection Monitoring

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 complete different tasks on the managed system. HMC roles are either predefined or customized.

The roles that are discussed refer to HMC users; operating systems that are 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 different 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 9.

You can assign managed systems and logical partitions to individual HMC users. This action 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.

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

Table 3. Predefined HMC Roles

Role	Description	HMC User ID
Operator	The operator is responsible for daily system operation.	**hmcoperator**
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.	**hmcsuperadmin**
Product engineer	A product engineer helps 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.	
Service representative	A service representative is an employee who is at your location to install, configure, or repair the system.	**hmcservicerep**
Viewer	A viewer can view HMC information, but cannot change any configuration information.	**hmcviewer**
Client live update	The client live update role is intended for use when you are using the AIX Live Update capability on a partition of a managed system. A client live update user has authority that is limited to what is necessary to complete a live update on AIX.	**hmcclientliveupdate**

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.

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 108.

Some tasks can only be performed using the command line. For a listing of those tasks, see Table 9 on page 26.

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

Table 4. HMC task groupings	
HMC tasks and the corresponding user roles, IDs, and commands	**Associated table**
HMC Management	Table 5 on page 10
Service Management	Table 6 on page 13
Systems Management	Table 7 on page 15
Control Panel Functions	Table 8 on page 24

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

Table 5. 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)**
"Backup Management Console Data" on page 80 bkconsdata	X	X		X
Backup Profile Data bkprofdata	X	X		X
Change BMC Certificates chbmccert	X	X		X
Certificate Management chhmccert lshmccert mkhmccert		X		
"Change Date and Time" on page 76 chhmc lshmc	X	X		X
"Change Language and Locale" on page 77 chhmc lshmc	X	X	X	X
Change HMC Configuration chipsec chpsm chusrtca	X	X		X

Table 5. 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 Network Settings" on page 75 chhmc lshmc	X	X		X
Change Proxy Configuration chproxy		X		X
"Change User Password" on page 86 chhmcusr	X	X	X	X
List BMC Certificates lsbmccert	X	X	X	X
List HMC Configuration lsipsec lspsm lsusrtca	X	X	X	X
List HMC Encryption Task lshmcencr	X	X	X	
List System Plan lssysplan		X		
List Proxy Configuration lsproxy	X	X	X	X
"Manage KDC" on page 92 chhmc lshmc getfile rmfile		X		
"Manage LDAP" on page 92 lshmcldap chhmcldap		X		
"Launch Guided Setup Wizard" on page 73		X		

Table 5. 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)**
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" on page 90		X		
"Manage Data Replication" on page 81	X	X		
"Manage Task and Resource Roles" on page 89 chaccfg lsaccfg mkaccfg rmaccfg		X		
"Manage User Profiles and Access" on page 86 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		
"Manage Users and Tasks" on page 89 lslogon termtask	X	X	X	X
Open 5250 Console	X	X		X
"Enable Remote Command Execution" on page 97 chhmc lshmc	X	X		X
"Enable Remote Operation" on page 97 chhmc lshmc	X	X	X	X

Table 5. 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)**
"Enable Remote Virtual Terminal" on page 97	X	X		X
"Restore Management Console Data" on page 81	X	X		X
"Save Upgrade Data" on page 81 saveupgdata	X	X		X
"Schedule Operations" on page 78	X	X		
"Shut Down or Restart" on page 78 hmcshutdown	X	X		X
"Serviceable Events Manager" on page 47 lssvcevents	X	X		X
"View Licenses" on page 79	X	X	X	X

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

Table 6. 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" on page 48		X		X
"Serviceable Events Manager" on page 98 chsvcevent cpfile lssvcevents mksvcevent updpmh		X		X

Table 6. 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" on page 80 formatmedia	X	X		X
"Manage Dumps" on page 99 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Transmit Service Information" on page 100 chsacfg lssacfg	X	X		
"Enable Electronic Service Agent" on page 102	X	X		X
"Manage Outbound Connectivity" on page 102	X	X		X
"Manage Inbound Connectivity" on page 103	X	X		X
"Manage Customer Information" on page 103	X	X		X
"Authorize User" on page 101		X		
"Manage Event Notification" on page 104 chsacfg lssacfg	X	X		X
"Manage Connection Monitoring" on page 104	X	X	X	X
"Electronic Service Agent Setup Wizard" on page 101		X		X

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

Table 7. 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)**
"General Settings" on page 43 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
migrlpar	X	X	X	X
optmem	X	X		X
lsmemopt	X	X	X	X
lsrrstartlpar	X	X		
Update Password chsyspwd		X		
Change Default User Interface Settings	X	X	X	X
List CEC Property lscomgmt lsiotopo	X	X	X	X
List Utilization Data lslparutil	X	X	X	X
Operations				
"Power Off" on page 31 chsysstate	X	X		X
"Activate" on page 58 chsysstate	X	X		X
"Save Current Configuration" on page 63 chsysstate	X	X		X

Table 7. 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)**
"Restart" on page 58 chsysstate	X	X		X
"Shut Down" on page 59 chsysstate	X	X		X
chlparstate	X	X		X
LED Status: Deactivate Attention LED "Attention LED" on page 35 chled	X	X		
LED Status: Identify LED "Attention LED" on page 35	X	X	X	X
LED Status: Test LED "Attention LED" on page 35	X	X	X	X
"Schedule Operations" on page 33	X	X		
"Launch ASM Interface" on page 34 asmmenu	X	X		X
"Rebuild" on page 35 chsysstate	X	X		
"Power Management" on page 32 chpwrmgmt lspwrmgmt		X		
"Delete" on page 59 rmsyscfg	X	X		X
"Mobility" on page 61 lslparmigr migrlpar	X	X		X

Table 7. 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 Profiles" on page 62 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
Manage System Plan cpsysplan rmsysplan		X		
Make System Plan mksysplan		X		
Deploy System Plan deploysysplan		X		
Change N_Port Login chnportlogin	X	X		X
RR Start LPAR lsrrstartlpar rrstartlpar	X	X		
Migrate LPAR migrdbg refdev	X	X		
Make Profile Data mkprofdata	X	X		
Restore Profile Data migrcfg	X	X		
Remove Profile Data rmprofdata	X	X		

Table 7. 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 Pmem CEC Config: Initialize Profile Data: Restore Profile Data rstprofdata For option "--retainpmemvolume" (access only for hmcsuperadmin)	X	X		
Vios Admin Op: Virtual IO Server Command viosvrcmd For option "--admin" (access only for hmcsuperadmin and hmcoperator)	X	X		X
"Operations" on page 31	X	X	X	X
Configuration				
"Create Partition from Template" on page 37		X		
"Deploy System from Template" on page 37		X		
"Capture Configuration as Template" on page 37		X		
Change CEC Property chprimhmc	X	X		
Change Trusted System Key chtskey		X		
"Create Partition" on page 42		X		
List LPAR Property lsmigrdbg	X	X	X	X
Hibernate LPAR lsrsdevsize	X	X		
List N_Port Login lsnportlogin	X	X		X
LS Profile Space lsprofspace	X	X	X	X

Table 7. 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)**
List Trusted System Key lstskey	X	X	X	X
"Manage Custom Groups" on page 63	X	X		X
"Manage Profiles" on page 62 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg	X	X	X	X
Manage License Keys chlickey	X	X		
Manage Utilization Data chlparutil	X	X		X
Save Current Configuration "Save Current Configuration" on page 63 mksyscfg	X	X		
ViewSPP lsmemdev	X	X	X	X
Connections				
"Service Processor Status" on page 36 lssysconn	X	X	X	X
"Reset or Remove Connections" on page 36 rmsysconn	X	X		
Add Connection mksysconn	X	X		
Open V Term mkvterm	X	X		X

Table 7. 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)**
Close V Term rmvterm	X	X		X
"Disconnect Another HMC" on page 36		X		
Hardware (Information)				
"Hardware Operations" on page 50	X	X	X	X
Updates				
"Change Licensed Internal Code" on page 38 lslic updlic		X		X
"Check System Readiness" on page 38 updlic		X		X
"View System Information" on page 38 lslic		X		X
Update HMC updhmc lshmc		X		X
Serviceability				
"Serviceable Events Manager" on page 63 chsvcevent lssvcevents		X		X
Change SNMP Alerts chspsnmp	X	X		X
"Create Serviceable Event" on page 48		X		X
"Reference Code Log" on page 64 lsrefcode	X	X	X	X

Table 7. 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)**
"Control Panel Functions" on page 64 lssyscfg	X	X		
"Add FRU" on page 50		X		X
"Add Enclosure" on page 52		X		X
"Exchange FRU" on page 51		X		X
"Remove FRU" on page 51		X		X
"Remove Enclosure" on page 52		X		X
"Power On/Off Unit" on page 50		X		X
"Manage Dumps" on page 49 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Collect VPD" on page 49	X	X	X	X
"Type, Model, Feature" on page 50		X		
"Setup FSP Failover" on page 52 chsyscfg lssyscfg		X		
"Initiate FSP Failover" on page 52 chsysstate		X		
List CEC Property lsprimhmc	X	X	X	X
Capacity on Demand (CoD)				
Enter CoD code chcod		X		

Table 7. 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)**
View History Log lscod	X	X	X	X
Change CEC Property chcomgmt	X	X		
CoD Pool Management: Change CoD chcodpool	X	X		
Change CoD mkcodpool		X		
Change VET Code chvet		X		
List CoD Information lscodpool	X	X	X	X
List VET Information lsvet	X	X	X	X
Processor: View Capacity Settings lscod	X	X	X	X
Processor CUoD: View Code Information lscod	X	X	X	X
Processor: On/Off CoD: Manage chcod		X		
Processor: On/Off CoD: View Capacity Settings lscod	X	X	X	X
Processor: On/Off CoD: View Billing Information lscod	X	X	X	X
Processor: On/Off CoD: View Code Information lscod	X	X	X	X

Table 7. 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: Trial CoD: Stop chcod		X		
Processor: Trial CoD: View Capacity Settings lscod	X	X	X	X
Processor: Trial CoD: View Code Information lscod	X	X	X	X
Processor: Reserve CoD: Manage chcod		X		
Processor: Reserve CoD: View Capacity Settings lscod	X	X	X	X
Processor: Reserve CoD: View Code Information lscod	X	X	X	X
Processor: Reserve CoD: View Shared Processor Utilization lscod	X		X	X
PowerVM® (formerly known as Advanced POWER® Virtualization): Enter Activation Code chcod		X		
PowerVM: View History Log lscod	X	X	X	X
PowerVM: View Code Information lscod	X	X	X	X
Enterprise Enablement: Enter Activation Code chcod		X		
Enterprise Enablement: View History Log lscod	X	X	X	X

Table 7. 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)**
Enterprise Enablement: View Code Information lscod	X	X	X	X
Other Advanced Functions: Enter Activation Code chcod		X		
Other Advanced Functions: View History Log lscod	X	X	X	X
Other Advanced Functions: View Code Information lscod	X	X	X	X
Processor: Manage chcod		X		
Processor: View Capacity Settings lscod	X	X	X	X
Processor: View Code Information lscod	X	X	X	X
Memory: Manage chcod		X		
Memory: View Capacity Settings lscod	X	X	X	X
Memory: View Code Information lscod	X	X	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)**
Serviceability				

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)**
(21) Activate Dedicated Service Tools chsysstate	X	X		
(65) Disable Remote Service chsysstate	X	X		
(66) Enable Remote Service chsysstate	X	X		
(67) DIsk Unit IOP Reset / Reload chsysstate	X	X		
(68) Concurrent Maintenance Power Off Domain	X	X		
(69) Concurrent Maintenance Power On Domain	X	X		
(70) IOP Control Storage Dump chsysstate	X	X		
(71) Product Engineering Debug Tools pedbg				
(72) PE Shell Access pesh	X	X	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 getupgfiles	X	X		X
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		

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)**
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
Monitoring 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
mkpwdpolicy		X		
rmpwdpolicy		X		
expdata		X		

Session handling

Learn about session limitations in the Hardware Management Console (HMC).

Session limitations

The HMC does not support disconnected sessions. A session logoff and a session disconnect are both considered as a session logoff. This means that you cannot reconnect to the same session to resume your task or tasks that were initiated from a previous session. Every login through the HMC creates a new session.

1. If you initiate long running tasks from the HMC interface and then log off from the session, the long running tasks continue to run in the background. However, when you log in again, a new session is created and the task progress panels (which helps track the progress of the previous tasks) are no longer available. In this scenario, if you need to check the progress of the tasks that were initiated from a previous session, you can run the respective command line interface (CLI) commands, check the state of the managed resource, or check the console event logs.

   Note: Some examples of long running tasks include the following tasks:

   System management for servers:

   - Deploy system plan
   - Code update
   - Hardware - Prepare for hot repair or upgrade

   System management for partitions:

- DLPAR memory in large units in the order of Terabytes
- Live Partition Mobility (LPM)
- Suspend or resume

HMC management:

- Backup management console data
- Restore management console data
- Save upgrade data

2. If you fail to reauthenticate within the time that is specified in the verify timeout settings, you are automatically logged off from the current session.
3. The idle timeout user property task is not functional. The HMC interface uses the default value of **0** for the idle timeout setting. If you set a different value for this setting, it is ignored.

   Note: Session, idle, and verify timeout properties are set for a user and it can be different for different users on the same HMC.

Version mismatch state for a managed system

The **Version mismatch** state can occur when the redundant or dual Hardware Management Consoles (HMCs) that manage the same server are at different version and release levels.

The **Version mismatch** state can occur for any of the following reasons:

- FSP firmware and HMC versions are incompatible.
- An HMC Version 7.7.8 or later is connected to a server that was managed by a newer version of the HMC.
- An HMC Version 7.7.8 or later is connected to a server that was managed by a lower version of the HMC and does not have enough space present to upgrade the data to HMC Version 7.7.8 or later.
- The hypervisor or server brand or model is not supported by this version of the HMC.

To recover from the **Version mismatch** state, select the appropriate action, depending on the reference code that is displayed:

- **Save Area Version Mismatch**

  HMC Version 7.7.8 and later blocks attempts to manage a server with a configuration at a newer level by posting a new **Connection error** state and reference code. If an HMC Version 7.7.8 or later is connected to a server that was managed by a newer version of the HMC that updated the configuration format, then the HMC reports a connection error of **Version mismatch** with the reference code **Save Area Version Mismatch**. This error prevents accidental corruption of the configuration.

  If you want to continue on a lower HMC version, then you must first initialize the server in the lower version of the HMC before you proceed to run any operation.

- **Profile Data Save Area is full**

  The HMC uses a storage area on each managed server to store the server configuration, primarily PowerVM partition profiles. HMC Version 7.8.0 and later increases the usage of the storage area by adding another (mostly hidden) profile for each partition. Servers that already contain many profiles might not have sufficient space to allow the HMC Version 7.8.0 and later to run properly.

  HMC Version 7.8.0 and later checks for sufficient space in this storage area and stops the connection process with a connection state of **Version mismatch** and a reference code of **Profile Data Save Area is full** if sufficient space does not exist.

- **Connecting 0000-0000-00000000 (Unsupported Hypervisor)**

  A connection state of **Version mismatch** and a reference code of **Connecting 0000-0000-00000000 (Unsupported Hypervisor)** is returned when the server is configured for a hypervisor other than PowerVM.

To recover from this state, first start the ASM by selecting the server with the **Version mismatch** and selecting **Operations** and then **Launch Advanced System Manager (ASM)**.

On models that support multiple hypervisors, the hypervisor mode setting can be found in the ASM by selecting **System Configuration** and then **Hypervisor Configuration**. The hypervisor mode shows a setting of either PowerVM or OPAL.

If OPAL is the wanted configuration, then you must remove this connection from the HMC by selecting **Connections** and then **Reset or Remove Connections**. Next, select **Remove Connections** and click **OK**.

Note: The OPAL hypervisor is not supported on the HMC.

If PowerVM is the wanted configuration, select **PowerVM** from the hypervisor mode menu and click **Continue**.

Note: The setting can be changed only when the server is powered off. To power off the server select **Power/Restart Control** and then **Power On/Off System**. Click **Save Settings and Power off** .

- **Connection not allowed**

  A connection state of **Version mismatch** and a reference code of **Connection not allowed 0009-0008-00000000** is returned when the FSP firmware and HMC versions are incompatible.

  To recover from this state, install an HMC version that supports the managed server model.

For more information about correction a **Version mismatch** state, see Version mismatch errors.

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.

These tasks are listed when a managed system is selected. The tasks listed in the menu pod change as selections are made in the work area.

System content pane

View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

The content pane, in the middle portion of the window, displays all the available systems and the associated information for each server. You can choose to display the information in a table view or a gallery view.

Each system displays the current state of the system, the number of central processing units (CPUs) that are in use, CPUs that are available, the amount of random access memory (RAM) that is in use, and the RAM that is available. Additionally, if you choose a tabular format view, you can filter the information to be displayed by selecting the drop-down arrow in the upper-right corner of the table. Select the check box corresponding to the field that you want to display on the table. If you are using HMC Version 9.1.930, in the **All Systems** table, you can also view information about the activated and deferred firmware levels.

You can click the **properties** icon to display the following information:

- Current state
- Reference code
- Machine type
- Serial number
- System location
- Firmware level
- Group tags
- Attention LED

You can click the **capacity** icon to display the following information:

- Date of collection.
- Processor usage (installed, activated, available, average, and peak). The bar graph and the numerical value show the average usage (average divided by activated) in a percentage. The threshold line on the bar graph shows the peak threshold (peak divided by activated). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Memory allocation (installed, activated, available, average, and peak). The bar graph and the numerical value show the average usage (average divided by activated) in a percentage. The threshold line on the bar graph shows the peak threshold (peak divided by activated). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Network I/O usage (sent and received in kilobytes per second and in packets per second). The bar graph and the numerical value show the average usage ((average transferred bytes divided by the number of adapters) divided by the maximum transferred bytes) in a percentage. The threshold line on the bar graph shows the high threshold (maximum transferred bytes). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Storage I/O usage (written and read information in kilobytes per second). The bar graph and the numerical value show the average usage ((average transferred bytes divided by the number of adapters) divided by the maximum transferred bytes) in a percentage. The threshold line on the bar graph shows the high threshold (maximum transferred bytes). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Data collection.

You can hover over the systems in the **All systems** window to view the system model description.

Operations

Operations contains the tasks for operating managed systems.

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 59

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 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 startup. 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 is powered off. This option is always available for selection.
- **Stop at Partition Standby**: This option specifies that logical partition startup is in standby mode after the managed system powers on and the HMC does not start any logical partitions when the managed system powers on. If powering on the managed system is the result of an automatic recovery process and the HMC is used to start a logical partition, the HMC starts all logical partitions that were running at the time the system is powered off. This option is available for selection only when the firmware for the managed system does not support advanced IPL capabilities.
- **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 that are 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 that 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 you display data for I/O devices or when you create 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 Management

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

About this task

To enable power saver mode, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to enable the power saver mode and click **Actions** > **View All Actions**.
3. Select **Power Management** under **Operations**.
4. Choose from any of the following Power Saver mode options:
   - **Disable All modes**: Disables the Power Saver mode. The processor clock frequency is set to a nominal value and the power that is used by the system remains at a nominal level.

- **Enable Static mode**: Reduces the power consumption by reducing the processor clock frequency and the voltage to fixed values. This option also reduces the power consumption of the system while still delivering predictable performance.
- **Enable Dynamic Performance mode**: Causes the processor frequency to vary based on processor use. During periods of moderate or high use, the processor frequency is set to the maximum value allowed, which might be higher than the nominal frequency. Additionally, the frequency is set to a value that is less than the nominal frequency during periods of low processor use.
- **Enable Maximum Performance mode**: Causes the processor frequency to be set at a fixed value that you can specify. You can set the maximum limit of the processor frequency and power consumption of the system.

Note: Enabling any of the power saver modes causes changes in the processor frequencies, changes in processor use, changes in power consumption, and varying performance.

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 might 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 perform the following tasks:

- Schedule an operation to run later.
- 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 you want the operation to repeat, you are asked to select the following options:

- 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 operations:

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.

Monitor/Perform Dynamic Platform Optimize
Schedules an operation for performing dynamic platform optimization and for sending an email notification alert to a user.

To schedule operations on the managed system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select one or more managed systems and click **Actions** > **Schedule Operations**.
3. From the **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 that 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 that you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation that 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.
4. To close the window, click **Options** and then click **Exit**.

Launch ASM Interface

The Hardware Management Console (HMC) can connect directly to the Advanced System Management Interface (ASMI) for a selected system.

The ASMI 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, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content area, select one or more managed systems and click **Actions** > **View All Actions** > **Launch Advanced System Management (ASM)**.

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 Hardware Management Console (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 and then, enter a new password and verify it by entering it again.

Attention LED

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 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 states:

- Electrical power is present.
- Activity is occurring on a link. (The system might 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 flashing, identify the problem and take the appropriate action to restore the system back 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 step 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 later. 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:

Turn Attention LED Off
From this task, you can deactivate the system attention LED.

Identify Attention LED
Displays the current Identify LED states for all the location codes that are 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 one or more LEDs by selecting the corresponding button.

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

Connections

You can view the Hardware Management Console (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 select a managed system in the work area, the following tasks pertain to that managed system. If you select a frame, the tasks pertain to that frame.

Service Processor Status

View information about the status of the Hardware Management Console (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, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the service processor connection status and click **Actions** > **View All Actions** > **Service Processor Status**.

Reset or Remove Connections

Reset or remove a managed system from the Hardware Management Console (HMC) interface.

About this task

To reset or remove connections, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server that you want to reset or remove and click **Actions** > **Reset or Remove System Connection**.
3. Select one of the options from **Reset Connection** or **Remove Connection** and click **OK**.

Disconnect Another HMC

You can disconnect a connection between a selected Hardware Management Console (HMC) and the managed server.

About this task

To disconnect another HMC, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to disconnect another Management Console and click **Actions** > **View All Actions** > **Disconnect Another HMC**.
3. Select an HMC from the list and click **OK**.

System Templates

System templates contain configuration details for resources such as system properties, shared processor pools, reserved storage pool, shared memory pool, Host Ethernet adapters, and SR-IOV adapters. Many of the system settings that you previously configured by using separate tasks are available in the **Deploy System from Template** wizard. For example, you can configure the Virtual I/O Servers, virtual network bridges, and virtual storage settings when you use the wizard to deploy a system from a system template.

The template library includes predefined system templates, which contain configuration settings based on common usage scenarios. Predefined system templates are available for your immediate use.

You can also create custom system templates that contain configuration settings that are specific to your environment. You can create a custom template by copying a predefined template and changing it to fit your needs. Or, you can capture the configuration of an existing system and save the details in a template. Then, you can deploy that template to other systems that require the same configuration.

Deploy System from Template

You can deploy systems by using system templates that are available in the template library of the Hardware Management Console (HMC). The Deploy System from Template wizard guides you to provide target system-specific information that is required to complete the deployment of the selected system.

Create Partition from Template

You can create a partition by using partition templates that are available in the template library of the Hardware Management Console (HMC). The Create a Partition from Template wizard guides you through the deployment process and configuration steps.

Capture Configuration as Template

You can capture the configuration details of a running server and save the information as a custom system template by using the Hardware Management Console (HMC). This function is useful if you want to deploy multiple servers with the same configuration. If you want to use a predefined template, you do not need to complete this task.

To capture configuration as a template, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the system information and click **Actions** > **View All Actions**
3. Click **Capture Configuration as Template with Physical I/O** or **Capture Configuration as Template without Physical I/O**.
4. Enter a template name and description, and then click **OK**.

Use the online Help if you need additional information about capturing the configuration as a template.

Updates

Display tasks to view system information, manage updates on your Hardware Management Console (HMC), or check system readiness.

View System Information

Display information on a selected system from the Hardware Management Console (HMC).

To view the network topology, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the system information and click **Actions** > **Updates** > **View System Information**.
3. Select a LIC repository from the list and click **OK**.
4. When you have completed this task, click **Close**.

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

Change Licensed Internal Code

Change the Licensed Internal Code of a managed system by using your Hardware Management Console (HMC).

You can change the Licensed Internal Code for the current release or to a new release.

To change the Licensed Internal Code, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the system information and click **Actions** > **Updates**.
3. Select **Change Licensed Internal Code** > **for the Current Release** or **Change Licensed Internal Code** > **to a New Release**.

   Note: Click **Start Change Licensed Internal Code** wizard to start a guided update of managed system, power, and I/O Licensed Internal Code (LIC). Click **View System Information** to examine current LIC levels, including retrievable levels. Click **Select Advanced Features** to update the managed system and power the LIC with more options and more targeting choices.
4. Select an action from the list and click **OK**.
5. When you complete this task, click **Close**.

Use the online Help if you need additional information for changing the Licensed Internal Code of the HMC.

Check System Readiness

Check the readiness of the Licensed Internal Code of a selected system from the Hardware Management Console (HMC).

To check system readiness, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the system information and click **Actions** > **Updates** > **Check System Readiness**.
3. When you have completed this task, click **OK**.

Use the online Help if you need additional information for checking system readiness of the HMC.

SR-IOV Firmware Update

Update the driver firmware for SR-IOV adapters on your Hardware Management Console (HMC).

Note: The adapter must be in shared mode.

To update the firmware for SR-IOV adapters, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to view the system information and click **Actions** > **Updates** > **SR-IOV Firmware Update**.
3. Select and right-click an adapter or adapters to get the context menu.
4. Select the type of firmware update to start.

   Note: Either the adapter driver firmware can be updated or both the adapter driver and adapter firmware can be updated. During the update operation of the adapter or adapter driver firmware, configured logical ports on the adapter might experience a temporary disruption of network traffic. Each adapter can take between 2 - 5 minutes to update. Updates are performed serially.
5. When you have completed this task, click **Close**.

Use the online Help if you need additional information for updating the driver or firmware for SR-IOV adapters.

Legacy

You can view **legacy** tasks that are available on the Hardware Management Console (HMC).

If you select a managed system in the work area, the following **legacy** tasks pertain to that managed system.

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 when a processor fails. If a processor fails on a logical partition and unassigned processors are not available on the managed system, then the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. This task 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 by choosing an availability priority from the list.

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 that you specify for the managed system.

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

Manage System Profiles

A system profile is an ordered list of partition profiles that is used by the Hardware Management Console (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 to activate or change the managed system from one set of logical partition configurations to another.

You can create a system profile that has a partition profile with 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 that is needed to activate all of the partition profiles in the system profile. A system profile can pass validation and yet not have enough memory to be activated.

Use this task to complete the following tasks:

- Create new system profiles.
- Create a copy of a system profile.
- Validate the resources that are 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 that are 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 attempts to activate the partition profiles in the order that is specified in the system profile.

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

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 by using the configuration information in the partition profile.

A partition profile specifies the wanted system resources for the logical partition and the minimum and maximum amounts of system resources that the logical partition can have. The system resources that are 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 such 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 more 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 that are 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 whether another partition profile is 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 overcommit resources, the partition profile is not 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 fails to activate because you overcommitted processor resources.

When you shut down a logical partition and reactivate the logical partition by 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 by using dynamic logical partitioning are lost when you reactivate the logical partition that uses a partition profile. This action is required when you want to undo dynamic logical partitioning changes for the logical partition. However, this action is not required if you want to reactivate the logical partition that uses 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 task avoids having to change partition profiles manually.

If you shut down a logical partition whose partition profiles are not up to date, and if 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 by 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 complete the following tasks:

- Restore partition data. If you lose partition profile data, use the restore task in one of the following ways:
  - Restore partition data from a backup file. Profile modifications that are completed after the selected backup file was created are 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 deletes all of the currently defined system profiles, partitions, and partition profiles.
- Back up a partition profile to a file.
- Back up partition data to a file.

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

Utilization Data

You can set the Hardware Management Console (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 that are 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, 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 to disable sampling collection.

Create Partition

You can quickly create partitions with minimum resources.

To create a partition, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to create a partition and click **Actions** > **View System Partitions**.
3. Click **Create Partition**.
4. Complete the required information in the **Basic Partition Configuration**, **Processor Configuration**, and **Memory Configuration** tabs. If you want to assign all the system resources to the partition, select the **Assign all system resources** check box.
5. To create multiple partitions, move the slider to the right and select the **Multiple Partitions View**.
6. To add a new partition definition, click the **(+)** sign located on the top of the partition table.
7. Select the added partition and complete the required information in the **Basic Partition Configuration**, **Processor Configuration**, and **Memory Configuration** tabs. In the **Basic Partition Configuration** tab, you can provide details about the number of partition instances that you want to create. You can create a maximum of 20 partition instances.
8. To remove an existing partition, select the partition that you want to remove and click the **(-)** sign.
9. Click **OK**.

Use the online Help if you need additional information about this task.

Note: If the managed system supports virtual serial number and if the managed system is not in an Enterprise Pool 2.0, the **Virtual Serial Number** can be specified in the **Basic Partition Configuration** tab.

When the firmware level is at FW950 and the managed system has logical partitions that are assigned with virtual serial numbers, the managed system cannot be added to an Enterprise Pool 2.0. Also, if the managed system is in an Enterprise Pool 2.0, virtual serial number cannot be assigned to the logical partitions.

Properties

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

To open the properties tasks that are available for your system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Properties** and then select the properties task that you want to perform from the list.

General Settings

View or change the general and advanced settings for the managed system.

These properties include the following tabs:

General Properties
The **General Properties** 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.

Migration
View the partition mobility properties and change the migration policy for inactive partitions on the managed system.

Power-On Parameters
From the **Power-On Parameters** tab, you can change the power-on parameters for the next restart by changing the values in the **Next Value** fields. These changes are only valid for the next managed system restart.

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 wanted 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 start the memory optimization tool.

You can view the VTPM settings.

Processor, Memory, I/O

View or change the memory, processor, and physical I/O resource settings for the managed system.

These properties include the following tabs:

Processor
The **Processor** tab displays information about the processors of the managed system, which includes:

- installed processing units
- unconfigured processing units
- available processor units
- available with stealable processor units
- configurable processing units
- minimum number of processing units per virtual processor
- maximum number of shared processor pools

The **Available with stealable** field displays the information about the available processing units, which is the sum of the available processing units in the managed system and the number of stealable processing units.

The stealable processor units value is the sum of the processor resources that are assigned to all the powered off or hibernated partitions on the managed system.

Notes:

- The information about stealable processor units is available only when the managed system is in the standby state or in the operating state.
- If the managed system is licensed with Power® IFL processor and if the firmware level is at FW910, or later, the **Available (with stealable)** field is displayed.
- When a POWER9 system is licensed with some IFL processors, the tab also displays the information about the remaining processors that are available for running the AIX or IBM i partitions.

Memory

The **Memory** tab displays information about the memory of the managed system, which includes:

- installed memory
- unconfigured memory
- available memory
- available with stealable memory
- configurable memory
- memory region size
- current memory available for partition usage
- system firmware current memory

The **Available with stealable** field displays the information about the available memory, which is the sum of available memory in the managed system and the amount of stealable memory resources. The tab also displays the maximum number of memory pools that are available.

Note: The information about stealable memory resources is available only when the managed system is in the standby state or in the operating state.

Physical I/O adapters

The **Physical I/O Adapters** 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.

- The **Adapter Description** column displays the physical description of each resource.
- The **Physical Location Code** column displays the physical location code of each resource.
- The **Owner** column displays who currently own the physical I/O. The value of this column can be any of the following values:
  - When a single root I/O virtualization (SR-IOV) adapter is in the shared mode, **Hypervisor** is displayed in this column.
  - When an SR-IOV adapter is in the dedicated mode, **Unassigned** is displayed when the adapter is not assigned to any partition as a dedicated physical I/O.
  - When an SR-IOV adapter is in the dedicated mode, the logical partition name is displayed when the adapter is assigned to any logical partition as a dedicated physical I/O.
- The **Bus Number** column displays the bus number of the resource.
- The **I/O Pools** button displays all of the I/O pools found in the system and the partitions that are participating in the pools.

PowerVM

You can use the PowerVM function on the Hardware Management Console (HMC) to manage the system-level virtualization capabilities of your IBM Power Systems servers.

You can use the PowerVM task to manage virtual resources that are associated with a system, such as configuring a Virtual I/O Server (VIOS), virtual networks, and virtual storage. You can manage the PowerVM functions at the managed system level in response to changes in workloads or to enhance performance.

The PowerVM functions include the following tasks:

- Managing Virtual I/O Servers
- Managing virtual networks
- Managing virtual storage
- Managing hardware virtualized I/O (SR-IOV adapters, host Ethernet adapters (HEAs), and host channel adapters (HCAs))
- Managing a reserved processor pool
- Managing shared processor pools
- Managing a shared memory pool

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

Capacity on Demand

Activate disabled processors or memory that is installed on your managed server.

You can use Capacity on Demand (CoD) to nondisruptively activate (no startup needed) processors and memory. Capacity on Demand also gives you the option to temporarily activate capacity to meet intermittent performance needs, to activate extra capacity on a trial basis, and to access capacity to support operations in times of need.

Capacity on Demand Functions

Learn about the different Capacity on Demand functions that are available for your system.

You can use Capacity on Demand (CoD) to nondisruptively activate (no startup needed) processors and memory. Capacity on Demand also gives you the option to temporarily activate capacity to meet intermittent performance needs, to activate extra capacity on a trial basis, and to access capacity to support operations in times of need.

The **Capacity on Demand Processor** functions include the following tasks:

- View processor settings
- CUoD (permanent) processor
  - View CUoD code information
- On/Off processor
  - Manage
  - View billing information
  - View capacity settings
  - View code information
- Utility processor
  - Manage
  - View capacity settings
  - View code information
  - View shared processor utilization
- Trial processor
  - Stop trial
  - View capacity settings
  - View code information

The **Capacity on Demand Memory** functions include the following tasks:

- View memory settings
- CUoD (permanent) memory

  - View CUoD code information
- On/Off memory
  - Manage
  - View billing information
  - View capacity settings
  - View code information
- Trial memory
  - Stop trial
  - View capacity settings
  - View code information

Use the online Help if you need additional information about Capacity on Demand functions.

Licensed Capabilities

View and edit the runtime capabilities that are supported by the managed system.

You can view which licensed capabilities are active on your managed system. To activate a new licensed capability, click **Enter Activation Code** and enter the activation code.

The licensed functions that are available on the managed system include the following capabilities:

- Active Memory Sharing Capable
- Live Partition Mobility Capable
- Micro-Partitioning® Capable
- PowerVM Partition Simplified Remote Restart Capable
- SR-IOV Capable (Logical Port Limit)
- Virtual I/O Server Capable
- Active Memory Expansion Capable
- Active Memory Mirroring for Hypervisor Capable
- Coherent Accelerator Processor Interface (CAPI)
- AIX Enablement for 256-Core Partition Capable
- Dynamic Platform Optimization Capable
- IBM i 5250 Application Capable

Use the online Help if you need additional information about licensed capabilities.

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 **Serviceable Events Manager** 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.

To open the serviceability tasks that are available for your system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.

3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Select the serviceability task that you want to perform from the list.

Tasks Log

View all the tasks that are currently running or completed on the Hardware Management Console (HMC).

To view the tasks log, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Tasks Log**.
2. You can view the following tabs in the tasks log:
   - **Task name**: Displays the name of task.
   - **Status**: Displays the current state of the task (running or completed).
   - **Resource**: Displays the name of the resource.
   - **Resource type**: Displays the type of resource.
   - **Initiator**: Displays the name of the user that initiated the task.
   - **Start time**: Displays the time that the task was initiated.
   - **Duration**: Displays the amount of time that the task took to complete.

Use the online Help for additional information about viewing the tasks log.

Serviceability

Problem Analysis on the Hardware Management Console (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 **Serviceable Events Manager** 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.

To open the serviceability tasks that are available for your system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Select the serviceability task that you want to perform from the list.

Serviceable Events Manager

Problems on your managed system are reported to the Hardware Management Console (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, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceable events.
3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Click **Serviceable Events Manager**.

5. Provide event criteria, error criteria, and FRU criteria. If you do not want the results to be filtered, select **ALL**. Click **Refresh** to refresh the list of serviceable events based on the criteria filter values.

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

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

The full table view includes more detailed information, including reporting partition ID, primary data event timestamp, duplicate count, notification type, first reported time, reporting name, reporting MTMS, firmware fix, and serviceable event text.

Select a serviceable event and use the **Action** menu to:

- **View Details**: Field-replaceable units (FRUs) associated with this event and their descriptions.
- **View Files**: View the files associated with the selected serviceable event.
- **View Reference Code Description**: View the description of the reference code associated with the selected serviceable event. The option will not be available if additional description is not available.
- **Call Home**: Report the event to your service provider.
- **Repair**: Start a guided repair procedure, if available.
- **Close Event**: After the problem is solved, add comments and close the event.
- **Add PMH Comment**: Add a comment to a PMH for a selected serviceable event. If a PMH number does not exist for a given problem, the Add PMH Comment option is not available.

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

Create Serviceable Event

This task reports problems that occurred on your Hardware Management Console (HMC) 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, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Create Serviceable Event**.
3. From the **Create Serviceable Event** window, select a problem type from the list displayed.
4. 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 Dumps

Manage system, service processor, and power subsystem dumps for systems that are managed by the Hardware Management Console (HMC).

system dump
A collection of data from server hardware and firmware, either after a system failure or a manual request. Perform a system dump only 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 process is only applicable to certain models of managed systems.

Use the **Manage Dump** task to complete the following tasks:

- Initiate a system dump, a service processor dump, or a power subsystem dump.
- Modify the dump capability parameters for a dump type before you initiate a dump.
- Delete a dump.
- Copy a dump to media.
- Copy a dump to another system by using file transfer protocol (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 that 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 rollback a model.
- Upgrade or rollback a feature.

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

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

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

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

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

Hardware Operations
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.

To open the hardware tasks that are available for your system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage hardware tasks.
3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Select the hardware operations task that you want to perform from the list.

Prepare for Hot Repair or Upgrade
Provides a summary of required actions to be performed to isolate a particular hardware component as part of a service procedure.

From the **Component List** table, you can select the component to be repaired using the location code on the system to be repaired as directed by an Authorized Service Representative.

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

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

Add FRU
Locate and add a Field Replaceable Unit (FRU).

To add a FRU to a POWER9 system, complete the following steps:

1. Select an enclosure type from the **Enclosure** menu.
2. Select a FRU type from the displayed list of FRU types for this enclosure, and click **Next**.
3. Select a FRU location, then click **Next** to start the Add FRU procedure for the selected location.
4. Follow the **Procedure** details listed in the window. The **Operation** list displays the correct operations for the procedure that you want to execute. The procedures direct when to perform each operation. Wait until advised to perform the operation before selecting the operation in the **Operation** list. Click **Next** to continue to the next service procedure.

   Note: Select the FRU location image on the header to display the location of the part to be serviced. To see a larger version of the FRU location image in a separate window, click **Display FRU Location**.
5. Click **Finish** to end the service when you have completed the last service procedure.

When the managed system is a POWER8® or earlier, to add a FRU, complete the following steps:

1. Select an enclosure type from the **Add FRU** menu.
2. Select a FRU type from the menu.
3. Click **Next**.
4. Select a location code from the displayed menu.
5. Click **Add**.

6. Click **Launch Procedure**.
7. When you complete the FRU installation process, click **Finish**.

Exchange FRU
Use the **Exchange FRU** task to exchange one field replaceable unit (FRU) with another FRU.

When the managed system is a POWER9 or later, to exchange a FRU, complete the following steps:

1. Select an installed enclosure type from the **Enclosure** menu.
2. Select a FRU type to be replaced, from the displayed list of FRU types for this enclosure and click **Next**.
3. Select a installed FRU location, then click **Next** to start the Exchange / Replace FRU procedure for the selected FRU.
4. Follow the **Procedure** details listed in the window. The **Operation** list displays the correct operations for the procedure that you want to execute. The procedures direct when to perform each operation. Wait until advised to perform the operation before selecting the operation in the **Operation** list. Click **Next** to continue to the next service procedure.

   Note: Select the FRU location image on the header to display the location of the part to be serviced. To see a larger version of the FRU location image in a separate window, click **Display FRU Location**.
5. Click **Finish** when you complete the exchange procedure.

When the managed system is a POWER8 or earlier, to exchange a FRU, complete the following steps:

1. Select an installed enclosure type from the **Exchange FRU** menu.
2. From the displayed list of FRU types for this enclosure, select a 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 that are listed in **Pending Actions**.
7. Click **Finish** when you complete the installation.

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

When the managed system is a POWER9 or later, to remove a FRU, complete the following steps:

1. Select an enclosure from the menu to display a list of FRU types that are currently installed in the selected enclosure.
2. Select a FRU type from the displayed list of FRU types available for removal from the selected system and click **Next**.
3. Select a FRU location, then click **Next** to start the Remove FRU procedure for the selected FRU .
4. Follow the **Procedure** details listed in the window. The **Operation** list displays the correct operations for the procedure you want to execute. The procedures direct when to perform each operation. Wait until advised to perform the operation before selecting the operation in the **Operation** list. Click **Next** to continue to the next service procedure.

   Note: Select the FRU location image on the header to display the location of the part to be serviced. To see a larger version of the FRU location image in a separate window, click **Display FRU Location**.
5. Click **Finish** when you complete the removal procedure.

When the managed system is a POWER8 or earlier, to remove a FRU, complete the following steps:

1. Select an enclosure from the menu to display a list FRU types that are currently installed in the selected enclosure.
2. From the displayed list of FRU types for this enclosure, select a 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 complete the removal procedure.

Add Enclosure
Learn how to locate and add an enclosure.

To add an enclosure, complete the following steps:

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

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

To remove an enclosure, complete the following steps:

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 that are identified in **Pending Actions** from the selected system.
3. Click **Finish** when you complete the enclosure removal process.

Open MES
View MES order numbers and their states, for any MES operations active or inactive for the Hardware Management Console (HMC).

Use **Add MES Order Number** to add a new order number to the list. To add an order number, complete the following steps:

1. Click **Add MES Order Number**.
2. Enter new MES order number.
3. Click **OK**.

Close MES
Close MES order numbers.

Use **Close MES** to close a MES. To close a MES, complete the following steps:

1. Select an open MES order number from the table.
2. Click **OK**.

Setup FSP Failover
Set up 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.

To set up the FSP failover, complete the following steps:

1. In the content pane under **FSP failover**, click **Setup**.
2. Click **OK** to enable automatic failover for the selected system.

Initiate FSP Failover
Initiate 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. Select **Initiate** to start the FSP Failover for the selected managed system.

To start the FSP failover, complete the following steps:

1. In the content pane under **FSP failover**, click **Initiate**.
2. Click **OK** to start the automatic failover for the selected system.

Reference Code Log

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

View reference codes that are generated for the selected managed system. Reference codes are diagnostic aids that help you determine the source of a hardware or operating system problem.

To view the reference code history, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Serviceability** and then click **Reference Code Log**.
4. Select a specific reference code to view the details.

Use the online Help if you need additional information about this task.

RIO Configuration

View the current hardware topology and the last valid hardware topology.

Displays the current hardware and last valid hardware topology. Any discrepancies between the current topology and the last valid topology are identified as errors.

To view the hardware topology, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Serviceability** and then click **RIO Configuration**.
4. View the hardware topology information.

Use the online Help if you need additional information about this task.

PCI Configuration

View information about the Peripheral Component Interconnect Express (PCIe) hardware topology.

The PCIe hardware topology utility provides information about the PCIe links that exist for each system.

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

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Serviceability** and then click **PCI Configuration**.
4. View the PCIe hardware topology.

Use the online Help if you need additional information about this task.

Topology diagrams

Learn how to view the topology diagrams of a partition.

You can use the Hardware Management Console (HMC) to view the topology diagrams of a partition.

Viewing virtual networking diagrams

You can view the end-to-end network configuration for the selected system, by using the Hardware Management Console (HMC). The view of the virtual networks begins with the physical adapter cards and the physical ports that are connected to them. As you scroll down, you can see the defined virtual bridges, link aggregation devices, virtual switches, virtual networks, and partitions in the VIOS.

You can click a resource and drag to pan across the diagram. You can also double-click a resource to highlight that resource and the relationship between its various virtual and physical components in the network. To remove the highlighting, double-click in an empty area of the network diagram. To view more detailed information about a resource, you can right-click a resource and additional information is displayed in a click card. Alternatively, you can hover over the label of a resource area to display the name of the resource as a tooltip.

To view the end-to-end network configuration for the selected system by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Topology** and then click **Virtual Networking Diagram**.
4. Right-click a resource for the selected system to view more detailed information in a click card. You can also hover over the label of a resource area to display the name of the resource as a tooltip.
5. In the upper-right corner of the work pane, click the **zoom in** and **zoom out** icons to achieve the required level of magnification.

   Note: You can also zoom in and zoom out by using the scroll wheel on the mouse from within the diagram.
6. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the virtual networking diagram.

Use the online Help if you need additional information about this task.

Viewing virtual storage diagrams

Two types of virtual storage diagrams are available; systems storage and partition storage. You can view the virtual storage configuration for the selected system, including the physical and virtual components of system storage, by using the HMC. You can also view the virtual storage configuration for a single partition in a particular system, including the physical and virtual components of storage assigned to that particular partition, by using the Hardware Management Console (HMC).

This diagram displays a high-level overview of the contents of the system or a single partition, and not specific component relationships. You can click a resource and drag to pan across the diagram. You can also double-click a resource to highlight that resource and the relationship between its various virtual and physical components in the network. To remove the highlighting, double-click in an empty area of the storage diagram. To view more detailed information about a resource, you can right-click a resource and additional information is displayed in a click card. Alternatively, you can hover over the label of a resource area to display the name of the resource as a tooltip.

To view the virtual storage configuration for the selected system or a single partition by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Topology** and then click **Virtual Storage Diagram**.

   Note: To view the virtual storage diagrams of a single partition in a particular system, select the partition of your choice and then expand **Topology** and click **Partition Virtual Storage Diagram**
4. Right-click a resource for the selected system to view more detailed information in a click card. You can also hover over the label of a resource area to display the name of the resource as a tooltip.
5. In the upper-right corner of the work pane, click the **zoom in** and **zoom out** icons to achieve the required level of magnification.

   Note: You can also zoom in and zoom out by using the scroll wheel on the mouse from within the diagram.
6. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the virtual storage diagram.

Use the online Help if you need additional information about this task.

Viewing SR-IOV and vNIC diagrams

You can view the SR-IOV and virtual Network Interface Controllers (vNIC) configuration for the selected system, including the physical and virtual components, by using the Hardware Management Console (HMC).

This diagram displays the relationships between SR-IOV adapters and other virtual components, such as vNIC. You can click a resource and drag to pan across the diagram. You can also double-click a resource to highlight that resource and the relationship between its various virtual and physical components in the network. To remove the highlighting, double-click in an empty area of the SR-IOV and vNIC diagram. To view more detailed information about a resource, you can right-click a resource and additional information is displayed in a click card. Alternatively, you can hover over the label of a resource area to display the name of the resource as a tooltip.

To view the end-to-end network configuration for the selected system by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Actions** > **View System Partitions**.
3. In the menu pod, expand **Topology** and then click **SR-IOV vNIC Diagram**.
4. Right-click a resource for the selected system to view more detailed information in a click card. You can also hover over the label of a resource area to display the name of the resource as a tooltip.
5. In the upper-right corner of the work pane, click the **zoom in** and **zoom out** icons to achieve the required level of magnification.

   Note: You can also zoom in and zoom out by using the scroll wheel on the mouse from within the diagram.
6. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the SR-IOV and vNIC diagram.

Use the online Help if you need additional information about this task.

Systems Management for Partitions

Systems Management displays tasks that 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.

The following sets of tasks are represented when a partition is selected and is shown in the menu pod or content pane. The tasks that are listed in the menu pod change as selections are made in the work area.

Partition content pane

View and monitor the state, health, and capacity information of all the partitions that are connected to the management console.

The content pane, in the middle portion of the window, displays all the available partition and the associated information for each partition.

Each partition displays the current state of the partition, the reference code, the number of virtual processors that are allocated, and the amount of random access memory (RAM) that is allocated. Additionally, if you choose a tabular format view, you can filter the information to be displayed by selecting the drop-down arrow in the upper-right corner of the table. Select the check box corresponding to the field that you want to display on the table. If you are using HMC Version 9.1.930, or later, in the **All partition** table, you can also view the memory mode of all partitions that are associated with the managed system.

You can click the **properties** icon to display the following information:

- Current state
- System name
- Reference code
- Partition ID
- IP address
- Environment
- OS version
- RMC connection
- Last activated profile
- Contains physical I/O
- Group tags
- Attention LED

You can click the **capacity** icon to display the following information:

- Date of collection.
- Processor usage (type (dedicated, uncapped, or capped), entitled capacity, and virtual processors). When the processor type is dedicated, the bar graph and the numerical value show the used processor usage (used divided by assigned) in a percentage. The threshold line on the bar graph shows the peak threshold (peak divided by assigned). When the processor type is uncapped, the bar graph and the numerical value show the used processor usage (used divided by the number of virtual processors) in a percentage. The threshold line on the bar graph shows the peak threshold (peak divided by the number of virtual processors). When the processor type is capped, then the bar graph and the numerical value show the used processor usage (used divided by entitled) in a percentage. The threshold line on the bar graph shows the peak threshold (peak divided by entitled). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Memory allocation (allocated).
- Network I/O usage (sent and received in terabytes per second and in packets per second). The bar graph and the numerical value show the average usage ((average transferred bytes divided by the

number of adapters) divided by the maximum transferred bytes) in a percentage. The threshold line on the bar graph shows the high threshold (maximum transferred bytes). When the value exceeds the threshold, the bar graph changes to a dashed line format.

- Storage I/O usage (written and read information in kilobytes per second). The bar graph and the numerical value show the average usage ((average transferred bytes divided by the number of adapters) divided by the maximum transferred bytes) in a percentage. The threshold line on the bar graph shows the high threshold (maximum transferred bytes). When the value exceeds the threshold, the bar graph changes to a dashed line format.
- Data collection.

Partition Properties

The **View Partition 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, boot mode to start the operating system, and the system on which the partition is located.

Note: If the managed system supports virtual serial number and if the managed system is not in an Enterprise Pool 2.0, the Virtual Serial Number property is displayed in the **General** tab.

Click **Advanced settings** to also view the list of supported hardware accelerators for a logical partition and Quality of Service (QoS) credits for a specific hardware accelerator. This section is not displayed if the managed system does not support hardware accelerators.

Note: When the HMC is at V9.2.950.0, or later, and when the firmware is at level FW950, or later, the **KeyStore Size** value can be chosen in the range 4 KB - 64 KB as the keystore size of the logical partition. The value of 0 KB indicates that the keystore function is disabled for the logical partition.

Processor
The **Processor** tab displays the current usage of processors.

Note: When the operating system and the hypervisor support 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.

Memory
The **Memory** tab displays properties of the running logical partition that is using the dedicated or the shared memory.

Physical I/O adapter
The **Physical I/O Adapter** tab displays the properties of all the physical I/O adapters that are available for the managed system and that can be assigned to a partition. You can also add and remove an adapter in a partition.

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.

About this task

To open the operations tasks that are available for your partitions, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to manage operations tasks. Click **Actions** > **View Partition Properties**
3. In the menu pod, expand **Partition Actions** and then expand **Operations**.
4. Select the operations task that you want to perform from the list.

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 HMC 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.

Netboot

Use the **netboot** task to network boot an AIX, Linux, or an IBM i partition on your managed system that is in the **Not Activated** state.

The **Network boot** wizard guides you through the steps of installing the operating system on the partition and then activating the partition. Select a partition profile to install the operating system on the partition. Click **Next** to configure the network settings for the logical partition.

Note: For Virtual I/O Server, you must choose the **Install** option from the **Actions** menu to install the VIOS on your managed system that is in the **Not Activated** state.

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 results 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 must shut down the client partitions before you shut 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 to 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 that are running in those jobs are not allowed to perform any job cleanup. This option might cause undesirable results if data is partially updated. Use this option only after a controlled end is 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 operation is complete, the logical partition is shut down and restarted. Use this option only if you 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.

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.

Schedule Operations

Create a schedule for certain operations to be performed on the logical partition.

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 might 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 perform the following operations:

- Schedule an operation to run later.
- 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 you want the operation to repeat, you are asked to select the following time intervals:

- 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 operations:

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, complete the following steps:

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 that 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 that you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation that 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**.

Validate Maintenance Readiness

Use the **Validate Maintenance Readiness** task to validate the readiness of the Virtual I/O Server (VIOS) for maintenance. The VIOS must be in **Running** state with an active Resource Monitoring Control (RMC) connection to perform the validation operation on the VIOS. To complete the validation operation, you must have access to all the partitions of the managed system.

The Hardware Management Console (HMC) validates the readiness of the VIOS for the maintenance. When you execute the maintenance readiness operation, the HMC validates all the client logical partition that use Virtual I/O Servers for Multi-path I/O operation or redundancy setup for the network and storage that is attached to a logical partition. To check the redundancy setup of the network or storage, the HMC gets the inventory information of other Virtual I/O Servers that are associated with the managed system. However, if other VIOS partitions in the system do not have a proper RMC connection, the validation process continues, and results are shown based on the current states of the Virtual I/O Servers.

The page also displays information about all the impacted client partitions that do not have a redundant Virtual SCSI Storage, Virtual Fibre Channel, Virtual networks, and Virtual NIC that is provided by the VIOS.

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, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content pane, select the server. Click **Actions** > **View System Partitions**.
3. In the content pane, select the partition that you want to migrate to another system.
4. Click **Actions** > **Mobility** > **Migrate**. The Partition Migration wizard opens.
5. 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, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content pane, select the server. Click **Actions** > **View System Partitions**.
3. In the content pane, select the partition for which you want to validate the settings.
4. Click **Actions** > **Mobility** > **Validate**. The Partition Migration Validation window opens.
5. 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, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content pane, select the server. Click **Actions** > **View System Partitions**.
3. In the content pane, select the partition that you want to recover.
4. Click **Actions** > **Mobility** > **Recover**. The Migration Recovery window opens.
5. Complete the information as necessary and click **Recover**.

Partition Templates

Partition templates contain details for partition resources, such as physical adapters, virtual networks, and storage configuration. You can create client partitions from the quick-start templates that are available in the template library or from your own user-defined templates on the Hardware Management Console (HMC).

Capture Partition as a Template

You can capture the configuration details of a running partition and save the information as a partition template by using the Hardware Management Console (HMC).

To capture the configuration as a template, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to capture as a template.
3. Click **Actions** > **Templates** > **Capture Partition as a Template**.
4. Enter a template name and description.
5. Click **OK**.

Use the online Help if you need additional information about this task.

Profiles

Learn about the tasks that are available in the **Profiles** menu.

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 Hardware Management Console (HMC). Default groups are listed under **Custom Groups** node under **Configuration**. 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 managing custom 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.

Delete Partition

You can delete a partition and the associated partition profile by using the Hardware Management Console (HMC).

To delete a partition, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to delete.
3. Click **Actions** > **Delete Partition**.
4. Select any options that you want.
5. Click **OK**.

Use the online Help if you need additional information about this task.

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 **Serviceable Events Manager** 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.

Serviceable Events Manager

Problems on your managed partitions are reported to the Hardware Management Console (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, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. Select the server for which you want to manage serviceable events.

3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Click **Serviceable Events Manager**.
5. Provide event criteria, error criteria, and FRU criteria. If you do not want the results that are filtered, select **ALL**. Click **Refresh** to refresh the list of serviceable events based on the criteria filter values.

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

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

The full table view includes more detailed information, including reporting partition ID, primary data event timestamp, duplicate count, notification type, first reported time, reporting name, reporting MTMS, firmware fix, and serviceable event text.

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

- **View Details**: Field-replaceable units (FRUs) associated with this event and their descriptions.
- **View Files**: View the files associated with the selected serviceable event.
- **View Reference Code Description**: View the description of the reference code associated with the selected serviceable event. The option will not be available if additional description is not available.
- **Call Home**: Report the event to your service provider.
- **Repair**: Start a guided repair procedure, if available.
- **Close Event**: After the problem is solved, add comments and close the event.
- **Add PMH Comment**: Add a comment to a PMH for a selected serviceable event. If a PMH number does not exist for a given problem, the Add PMH Comment option is not available.

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

Reference Code Log

Use the **Reference Code Log** 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 **Refresh**. 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.

Virtual I/O

Learn how to view the virtual networks, virtual network interface controllers, and virtual storage of a partition.

You can use the Hardware Management Console (HMC) to view the virtual topology of a partition.

Virtual Networks

You can view and add virtual networks that are associated with the selected logical partition.

The **Virtual Networks** table lists the virtual network name, VLAN ID, virtual switch, virtual network bridge, and virtual Ethernet adapter ID that are associated with each virtual network. You can click **Attach Virtual Network** to view the available virtual networks and attach additional virtual networks to the logical partition.

To view the virtual networks for the selected partitions by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to manage serviceability tasks and click **Actions** > **View Partition Properties**.
3. In the menu pod, expand **Virtual I/O** and then click **Virtual Networks**.

Use the online Help if you need additional information about this task.

Virtual NIC

You can manage all aspects of the virtual Network Interface Controller (NIC) configuration that is associated with the partition.

A virtual NIC is a type of virtual adapter that can be configured on logical partitions to provide a network interface. Each virtual NIC client adapter is backed by an SR-IOV logical port that is owned by the hosting partition.

The **Virtual NIC** table lists all virtual NICs that are configured for the selected partition. A virtual NIC can have one or more backing devices. The maximum number of backing devices per virtual NIC depends on the system. If the virtual NIC has more than one backing device, you can expand the node to view all the backing devices. If the virtual NIC has only one backing device, that backing device is the active backing device. The active backing device is the one that is in use by the virtual NIC. If the managed system is not failover capable, the table displays virtual NICs that have a single backing device.

You can add a virtual NIC to the partition. To add a virtual NIC, click **Add Virtual NIC**. You can configure the virtual NIC only in dedicated mode. You can also modify and view virtual NIC properties. To modify properties of a virtual NIC, select the virtual NIC in the table and click **Action** > **Modify vNIC** . To view the properties of a virtual NIC, select the virtual NIC in the table and click **Action** > **View vNIC**.

To view the virtual NIC for the selected partition by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to manage serviceability tasks and click **Actions** > **View Partition Properties**.

3. In the menu pod, expand **Virtual I/O** and then click **Virtual NICs**.

Use the online Help if you need additional information about this task.

Virtual Storage

You can create, view, and manage the storage capability of the logical partition.

The **Virtual Storage** table displays the Virtual Small Computer Serial Interface (SCSI) devices that are configured to a logical partition. You can also view the information about the physical volume groups, shared storage pool volume, and the logical volume.

You can add the virtual storage resources to a partition. Click **Adapter View** to create, view the adapter configuration of the virtual storage devices that are allocated for the logical partition. Click **Storage View** to view and manage the storage capability of the logical partition.

Physical volumes can be exported to partitions as virtual SCSI disks. Click **Show assigned physical volumes** to view the assigned physical volumes that are assigned to the logical partition.

To add physical volumes to a partition, select the physical volumes from the list and specify the **User Defined Name** for each physical volume that you want to add to the partition and then click **OK**. If you want to change the server adapter ID that is assigned to each physical volume, click **Edit** for each of the physical volumes that you want to update. The **Edit connection** window is displayed. You can specify up to 3 Virtual I/O servers, and then enter the new server adapter ID that you want to assign for the adapter connection.

To add different types of virtual storage devices to a partition, click **Add Virtual SCSI Device**. Select the available virtual storage that you want to add. You can select the virtual storage types such as **Physical Volume**, **Shared Storage Pool Volume**, or **Logical Volume**.

To view the virtual storage for the selected partition by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to manage serviceability tasks and click **Actions** > **View Partition Properties**.
3. In the menu pod, expand **Virtual I/O** and then click **Virtual Storage**.

Use the online Help if you need additional information about this task.

Hardware Virtualized I/O

You can view and change the settings of hardware virtualized I/O adapters, such as single root I/O virtualization (SR-IOV) port adapters and logical host Ethernet adapters (LHEA) for a partition by using the Hardware Management Console (HMC).

To view the hardware virtualized I/O adapters for the selected partition by using the HMC, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Partitions**.
2. Select the partition for which you want to manage serviceability tasks and click **Actions** > **View Partition Properties**.
3. In the menu pod, expand **Virtual I/O** and then click **Hardware I/O**.
4. In the **SRIOV** tab, you can add an SR-IOV logical port to the partition or change the settings of the SR-IOV logical ports. In the **SR-IOV logical port** table, you can also view the information about the logical ports that can be migrated and the information about the backing device that is configured for the logical ports. In the **Logical host Ethernet adapters** (LHEA) tab, you can change the settings of an LHEA adapter. You can also add and remove an LHEA adapter.

Notes:

- With HMC Version 9.1.930, or later, the HMC also supports the RDMA over Converged Ethernet (RoCE) adapter.
- If you are using HMC Version 9.1.940, with firmware at level FW940, or later, you can create logical partitions that have an SR-IOV logical port that can be migrated. You can migrate a logical partition with SR-IOV logical ports when the Migratable option is used to create a backup virtual device when creating a logical port. The backup device can be either a virtual Ethernet or a virtual Network Interface Controller (NIC) adapter. When the HMC is at Version 9.1.940.x, and when the firmware is at level FW940, the Migratable option for the Hybrid Network Virtualization capability is available as a Technology Preview only and is not intended for production deployments. However, when the HMC is at Version 9.1.941.0, or later, and when the firmware is at level FW940.10, or later, the Migratable option for the Hybrid Network Virtualization capability is supported.

Use the online Help if you need additional information about this task.

Systems Management for Frames

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

Properties

Display the selected frame properties.

Frame properties include the following properties:

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 that are 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 that are 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 is not assigned to a managed system.

Operations

Perform tasks on managed frames.

Initialize Frames

Learn how to initialize managed frames.

This operation task is available when one or more frames are selected. It first powers 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 might take several minutes to complete.

Note: Managed systems that are already powered on are not affected and are not 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 first powers 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 Hardware Management Console (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 can take several minutes.

Change Password

Change the Hardware Management Console (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 and then, enter a new password and verify it by entering it again.

Power On/Off IO Unit

Power off an IO unit by using the Hardware Management Console (HMC) interface.

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

Configuration

You can use the **Configuration** tasks to configure your frame. You can also manage custom groups by using the **Configuration** task.

Manage Custom Groups

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

You can also nest groups (a group that is 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 by 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

You can use the **Connections** tasks to view the Hardware Management Console (HMC) connection status to frames or reset those connections.

Bulk Power Assembly (BPA) Status

Use the **Bulk Power Assembly (BPA) 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 operates normally with a connection to either side A or side B. However, for code update operations and some concurrent maintenance operations, the HMC needs connections to both sides.

The HMC displays the following information:

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

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

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 completed 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 are not 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 Hardware Management Console (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 verify that the network settings are correct on both the HMC and the managed frame.

Serviceability

Problem analysis on the Hardware Management Console (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). Use the **Serviceable Events Manager** task to view specific events for selected frames.

To open the serviceability tasks that are available for your frame, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Frames**.
2. Select the frame for which you want to manage serviceability tasks.
3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Select the serviceability task that you want to complete from the list.

Serviceable Events Manager

Problems on your managed frame are reported to the Hardware Management Console (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, complete the following steps:

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

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

- Problem Number.
- PMH Number.
- Reference Code: Click **Reference** code to display a description of the problem reported and actions that can 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 complete the following tasks:

- **View event details**: FRUs associated with this event and the descriptions.
- **Repair the event**: Start 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 start 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, complete the following steps:

1. From the **FRU** menu, select an enclosure type.
2. Select a 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 complete the FRU installation process, click **Finish**.

Add Enclosure

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

To add an enclosure, complete the following steps:

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 that are identified in **Pending Actions** to the selected system, click **Launch Procedure**.
3. When you complete the enclosure installation process, click **Finish**.

Exchange FRU

Exchange one FRU with another FRU.

To exchange a FRU, complete the following steps:

1. Select an installed enclosure type.
2. Select a FRU type.
3. Click **Next**.
4. Select a location code for a specific FRU.
5. Click **Add**.
6. Select **Launch Procedure**.

   Note: This procedure identifies the resources that are impacted by the **Exchange FRU** task, including any resources that are in use by partitions. Workloads that are running on partitions might be impacted if redundancy is not configured. Follow the on-screen instructions to complete the exchange.
7. When you complete the installation, click **Finish**.

Exchange Enclosure

Exchange one enclosure for another enclosure.

To exchange an enclosure, complete the following steps:

1. Select an installed enclosure, then click **Add** to add the selected enclosure's location code to **Pending Actions**.
2. Begin replacing the enclosures that are identified in **Pending Actions** in the selected system by clicking **Launch Procedure**.

3. When you complete the enclosure replacement process, click **Finish**.

Remove FRU

Remove a FRU from your managed system.

To remove a FRU, complete the following steps:

1. Select an enclosure from the menu.
2. Select a 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 complete the removal procedure, click **Finish**.

Remove Enclosure

Remove an enclosure that is identified by the Hardware Management Console (HMC).

To remove an enclosure, complete the following steps:

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

Manage Groups

The **All groups** view provides a mechanism for you to group system resources together in a single view.

Groups may be nested to create customized system resources view.

You can view all the groups that are created by the users of the management console, including cumulative state information for system resources in a group. A custom group can consist of any systems, partitions, and Virtual I/O Servers that are managed by the management console.

To create a new group, complete the following steps:

1. Click **Create group** on the toolbar.
2. In the **Create group** window, specify a group name and description for the group. You can also tag a color to the group that you want to create.
3. Select one or more resources (for example: servers, partitions, or frames) that you want to include in the group that you want to work with.
4. Click **OK** to save the changes and to close the window.

You can edit an existing group to add or remove the resources from the group.

Note: When the last member (resources) of the group is removed, a message is displayed to confirm whether you want to delete the group. Click **Cancel** to retain the group in the **All groups** view.

Power Enterprise Pools

Systems Management for Power Enterprise Pool displays Power Enterprise Pool tasks that you can perform.

You can perform the following operations by using the Power Enterprise Pool offering:

- Add processors or memory to a server.
- Remove processors or memory from a server.
- Update the pool configuration.
- Add a server to the pool.

- Remove an existing server from the pool.
- Add processors or memory to the pool.
- View the following Power Enterprise Pool information:
  - Pool membership information
  - Pool resource information
  - Pool compliance information
  - Pool history log

HMC Management tasks

Learn about the tasks that are available on the Hardware Management Console (HMC) under **HMC Management**.

To open these tasks, see “HMC tasks, user roles, IDs, and associated commands” on page 9.

Note: Depending on the task roles that are assigned to your user ID, you might not have access to all the tasks. See Table 3 on page 9 for a listing of the tasks and the user roles that are allowed to access them.

Launch Guided Setup Wizard

This task uses a wizard to set up your system and HMC.

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Launch Guided Setup Wizard**.
3. 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.
4. Click **Finish** when you have completed all the tasks in the wizard.

View Network Topology

This task allows you to view and ping the connectivity between various network nodes within the Hardware Management Console (HMC).

To view the network topology, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **View Network Topology**.
3. From the **View Network Topology** window, you can ping current and saved nodes.
4. Click **Close** when you have completed this task.

Use the online Help if you need additional information about viewing the network topology.

Test Network Connectivity

This task allows you to view network diagnostic information about the network protocols for the Hardware Management Console (HMC).

To test the network connectivity, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Test Network Connectivity**.
3. From the **Test Network Connectivity** window, you can work with the following tabs:

   Ping
   You can ping the TCP/IP address or name.

   Interfaces
   Displays the statistics for the network interfaces that are currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

   Ethernet Settings
   Displays the settings for the Ethernet cards that are currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

   Address
   Display the TCP/IP addresses for the configured network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

   Routes
   Displays the Kernel IP and IPv6 routing tables and corresponding network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

   ARP
   Displays the contents of the Address Resolution Protocol (ARP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

   Sockets
   Displays information about TCP/IP sockets. To update the information that is currently displayed with the most recent information, click **Refresh**.

   TCP
   Displays information about Transmission Control Protocol (TCP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

   IP Tables
   Displays information (in table format) about the Internet Protocol (IP) packet filter rules. To update the information that is currently displayed with the most recent information, click **Refresh**.

   UDP
   Displays information about User Datagram Protocol (UDP) statistics. To update the information that is currently displayed with the most recent information, click **Refresh**.
4. Click **Cancel** when you have completed this task.

Use the online Help if you need additional information about testing the network connectivity.

Change Network Settings

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

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change Network Settings**.
3. From the **Change Network Settings** window, you can work with the following tabs:

   Identification
   Contains the host name, domain name, and console description of the HMC.

   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.

   Bond LAN Adapters
   Create or delete a Bond LAN adapter. A Bond LAN adapter combines two Ethernet interfaces into a single logical link. To change the settings of the Bond LAN adapter, select a Bond LAN adapter and click **Edit**. You can change the IP address, IP network mask, gateway, and the firewall settings of the Bond LAN adapter.

   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.
4. 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.

Change Performance Monitoring Settings

The Performance and Capacity Monitor tool collects allocation and usage data for virtualized server resources. It displays data in the form of graphs and tables, which are viewable from the Performance and Capacity Monitor home page.

The Performance and Capacity Monitor gathers data and provides capacity reporting and performance monitoring. This information can help you to determine the available capacity and whether your resources might be overextended or underused. In addition, your interpretation of the graphs and tables might be useful for capacity planning and troubleshooting. For more information about The Performance and Capacity Monitor tool, see Using the Performance and Capacity Monitor.

The Performance and Capacity Monitor captures data only from the servers for which you choose to enable data collection.

To enable data collection, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change Performance Monitoring Settings**.
3. Specify the number of days for which you want to store performance data by typing in a number 1 - 366. Alternatively, you can click the up or down arrows next to **Number of days to store performance data** under **Performance Data Storage**.

   Note: By default, the HMC stores data for 180 days. However, you can specify the maximum number of days that the HMC stores data to 366 days.
4. Click the toggle switch in the **Collection** column next to the name of the server for which you want to collect data. Alternatively, you can click **All On** to enable data collection for all of the servers in your environment that the HMC manages.

   Note: You might be prevented from collecting data from all of the servers in your environment because storage space is limited. The HMC prohibits you from enabling data collection from more servers when the HMC determines that it might run out of estimated storage space.
5. Click **OK** to apply the changes and close the window. You can now review the collected data when you access the Performance and Capacity Monitor home page.

Change Date and Time

Change the time and date of the battery-operated Hardware Management Console (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 adjusts automatically for Daylight Saving Time in the time zone you select.

To change the date and time, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change Date and Time**.
3. Click the **Customize Console Date and Time** tab.
4. Enter the date and time information.
5. Click **OK**.

To change the time server information, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change Date and Time**.
3. Click the **NTP Configuration** tab.
4. Provide the appropriate information for the time server.
5. 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.

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. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change Language and Locale**.
3. From the **Change Language and Locale** window, choose the applicable language and locale.
4. 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

Create and display a welcome message or display a warning message that appears before users log on to the Hardware Management Console (HMC).

The text that you enter in the message input area for this task appears on the **Welcome** window after you initially access the console. You can use this text to notify users about certain corporate policies or security restrictions that apply to the system.

To create a welcome text, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Create Welcome Text**.
3. Enter the welcome text that you want to display in the text box.

   Note: A maximum of 8192 characters is allowed.
4. Click **OK**.

For more information about this task, use the online Help.

Console Default Settings

You can modify the default console settings on the Hardware Management Console (HMC).

You can also modify the number of days for which a certificate is valid.

Note: The certificate can be valid for maximum of 3650 days.

To modify the console default settings, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Console Default Settings**.
3. In the **Console Default Settings** window, you can specify the number of days for which the certificate will be valid and you can also configure the time out settings for a HMC session. If you are using HMC

9.1.940, or later, you can specify the maximum number of log in attempts to the HMC graphical user interface (GUI). You can enter a value in the range 3 - 50.

4. When you complete the task, click **OK**.

Use the online Help if you need additional information about this task.

Shut Down or Restart

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

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Shut Down or Restart**.
3. 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.
4. 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.

Schedule Operations

Create a schedule for certain operations to be performed on the Hardware Management Console (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 might 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 later.
- 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 are required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you are 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, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Schedule Operations**.
3. 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 that 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 that you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation that 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.
4. 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.

View Licenses

View the Licensed Internal Code that you agreed to for this Hardware Management Console (HMC).

You can view licenses at any time. To view licenses, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **View Licenses**.
3. Click any of the license links to view more information.

   Note: This list does not include programs and code that is provided under separate license agreements.
4. Click **OK**.

Update the Hardware Management Console

Learn how to update the internal code of the Hardware Management Console (HMC) and view system information and system readiness.

To update the HMC, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.

2. In the content pane, click **Update the Hardware Management Console**. The **Install HMC Corrective Service Wizard** opens.
3. Click **Next** to start the update process.
4. Follow the steps in the wizard to complete the update operation.
5. Click **Finish** when you have completed this task.

Use the online Help if you need additional information about updating the Hardware Management Console.

Format Media

This task formats a diskette or USB 2.0 Flash Drive Memory Key.

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

To format a diskette or USB 2.0 Flash Drive Memory Key, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Format Media**.
3. From the **Format Media** window, select the type of media you want to format, then click **OK**.
4. Make sure that your media is correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
5. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information about this task.

Backup Management Console Data

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

Back up the HMC data after changes are made to the HMC or information that is associated with logical partitions.

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

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

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

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

To back up the HMC critical data, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Backup Management Console Data**.

3. From the **Backup Management Console Data** window, choose the archive option that you want to complete.
4. Click **Next**, then follow the appropriate instructions that are associated with the option you chose.
5. Click **OK** to continue with the backup process.

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

Notes:

- For HMC model 7063-CR1, DVD media is not supported.
- If you are using HMC Version 9.1.940, or later, you can specify a name for the generated backup file. If the backup file exists on the server, select the **Replace file** to replace the contents of the existing file that has the same name.

Restore Management Console Data

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

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Restore Management Console Data**.
3. From the **Restore Management Console 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**.
4. 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. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Save Upgrade Data**.
3. 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.
4. Click **Finish** when you have completed the task.

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

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.

To manage data replication, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Manage Data Replication**.
3. From the **Manage Data Replication** window, choose the appropriate option that you want to perform.

Use the online Help to get additional information for enabling or disabling customizable data replication.

Templates and OS Images

System templates contain configuration details for resources such as system properties, shared processor pools, reserved storage pool, shared memory pool, Host Ethernet adapters, and SR-IOV adapters. Many of the system settings that you previously configured by using separate tasks are available in the Deploy System from Template wizard. For example, you can configure the Virtual I/O Servers, virtual network bridges, and virtual storage settings when you use the wizard to deploy a system from a system template.

The template library includes predefined system templates, which contain configuration settings based on common usage scenarios. Predefined system templates are available for your immediate use. You can view, modify, deploy, copy, import, export, or delete templates that are available in the template library.

You can also create custom system templates that contain configuration settings that are specific to your environment. You can create a custom template by copying a predefined template and changing it to fit your needs. Or, you can capture the configuration of an existing system and save the details in a template. Then, you can deploy that template to other systems that require the same configuration.

To access the Template Library, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, you can access:
   - **System**
   - **Partition**
   - **OS and VIOS Images**
3. When you complete this task, click **Close**.

System Templates

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet adapters, single root I/O virtualization (SRIOV) adapters, Virtual I/O Server (VIOS), virtual networks, and virtual storage.

You can create custom system templates that contain configuration settings that are specific to your environment. You can also create a custom template by copying a predefined template and changing it to fit your needs. Or, you can capture the configuration of an existing system and save the details in a template. Then, you can deploy that template to other systems that require the same configuration. Click the template name to see the details about the template. Select a system template from the list to view, edit, copy, delete, deploy, or export a template.

Use the online Help if you need additional information on system templates.

Partition Templates

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration.

You can create custom partition templates that contain configuration settings that are specific to your environment. You can also create a custom template by copying a predefined template and changing it to fit your needs. Or, you can capture the configuration of an existing system and save the details in a template. Then, you can deploy that template to other systems that require the same configuration. Click the template name to see the details about the template. Select a partition template from the list to view, edit, copy, delete, deploy, or export a template.

Notes:

- If you are using HMC Version 9.1.940, or later, and if you are using a non-captured template to create a logical partition, you can configure an SR-IOV logical port that can be migrated. Select **migratable** in the **Edit** menu of the partition template. You can migrate the logical partition by using the SR-IOV logical port by creating a backup device and associate the SR-IOV logical port to the logical partition. The backup device can either be a virtual Ethernet adapter or a virtual Network Interface Controller (NIC) adapter.
- When the HMC is at Version 9.1.940.x, and when the firmware is at level FW940, the Migratable option for the Hybrid Network Virtualization capability is available as a Technology Preview only and is not intended for production deployments. However, when the HMC is at Version 9.1.941.0, or later, and when the firmware is at level FW940.10, or later, the Migratable option for the Hybrid Network Virtualization capability is supported.

Use the online Help if you need additional information on partition templates.

VIOS Images

Define VIOS images and installation resources for the operating environment that the Hardware Management Console (HMC) can access and use.

You can access the following tasks:

Manage Virtual I/O Server Image Repository

As of HMC 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 navigation area, click the **HMC Management** icon  , and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, select the **OS and VIOS Images** tab, and then click **Manage Virtual I/O Server Image Repository**.
3. In the Virtual I/O Server Image Repository window, click **Import New Virtual I/O Server Image**.
4. 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 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 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**.

Manage Virtual I/O Server Backups

With HMC version 9.2.950, or later, you can manage the I/O configuration of Virtual I/O Servers and manage the backup of the VIOS image on the management console.

About this task

To manage the backup or restore operation of the I/O configuration of the VIOS and to manage the VIOS image, complete the following steps:

Procedure

1. In the navigation area, click the **HMC Management** icon  , and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, select the **VIOS Images** tab, and then click **Manage Virtual I/O Server Backups**.
3. In the Manage Virtual I/O Server Backups window, select the **Virtual I/O Server Configuration Backup** tab. A table is displayed that lists all the backup files of the VIOS configuration that is taken by the HMC. Additionally, you can view the time at which the configuration file was last edited.
   a) To take the backup of the input/output configuration of a VIOS, click **Backup I/O configuration**. In the Backup I/O configuration window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

      The name you specify must consist of 1 - 40 characters including file extension **`.tar.gz`**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   b) To rename an existing backup file that is stored in the HMC, select a configuration file from the table and click **Action** > **Rename**.
   c) To restore the VIOS input/output configuration, select a backup file which contains the I/O configuration of the VIOS that you want to restore, and click **Action** > **Restore**.

4. In the Manage Virtual I/O Server Backups window, click the **Virtual I/O Server Backup** tab. A table is displayed that list all the VIOS image backup that are taken in the HMC. Additionally, you can also view the name and size of the VIOS image, the time when the VIOS image file was last edited, the managed system and the VIOS from which the image was captured.
   a) To take the backup of the VIOS image, click **Create Backup**. In the Create Backup window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

      The name you specify must consist of 1 - 40 characters including file extension **`.tar`**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   b) To rename an existing VIOS image backup file that is stored in the HMC, select a backup file from the table and click **Action** > **Rename**.
   c) To remove a VIOS image backup file from the HMC, select a backup file which contains the VIOS configuration that you want to remove from the table, and click **Action** > **Remove**.
5. Click **OK**.

All System Plans

A system plan is a specification of the logical partition configuration of a single managed system.

The table lists all the system plans that can be used to configure a managed system. You can create your own system plan or import an existing system plan.

Create System Plan

You can create a new system plan for a system that this Hardware Management Console (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.

1. Click **Create**.
2. Select a managed system from the available list and complete the **System plan name** and **Plan description** fields.
3. Check any options that you want.
4. Click **Create**.

Import System Plan

You can import a system plan file to the Hardware Management Console (HMC). The new system plan contains specifications for the logical partitions and partition profiles of the managed system that you used to create the plan.

1. Click **Import**.
2. Select a source to import the system plan file to the HMC.
3. Click **Import**.

Export System Plan

You can export a system plan file from the Hardware Management Console (HMC).

1. Select the system plan from the list and click **Actions** > **Export**.
2. Select a source to export the system plan file to the HMC.
3. Click **Export**.

Deploy System Plan

You can deploy a system plan file to one or more systems that the HMC manages. The managed system that you deploy the system plan on must have hardware that is identical to the hardware in the system plan.

1. Select the system plan from the list and click **Actions** > **Deploy**.
2. Follow the instructions on the **Deploy System Plan** wizard.

Delete System Plan

You can delete a system plan file from the Hardware Management Console (HMC).

1. Select the system plan from the list and click **Actions** > **Delete**.

Refresh

You can refresh the table to see any recent changes to the available system plans.

1. Click **Refresh** to update the table with the latest data.

Use the online Help if you need additional information about this task.

Users and Security tasks

The tasks that are available on the HMC for the **Users and Security** tasks are described.

Note: Depending on the task roles assigned to your user ID you may not have access to all the tasks. See "HMC tasks, user roles, IDs, and associated commands" on page 9 for a listing of the tasks and the user roles allowed to access them.

Change User Password

This task allows you to change your existing password that is used for logging on to the Hardware Management Console (HMC). A password verifies your user ID and your authority to log in to the console.

To change your password, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Change User Password**.
3. From the **Change User Password** window, specify your current password, specify a new password that you want to use, and re-specify the new password for confirmation in the fields provided.

   Note: The new password that you specify must have atleast eight characters.
4. 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 “Manage KDC” on page 92. For more information about LDAP authentication, see “Manage LDAP” on page 92.

For security reasons, remotely authenticated Kerberos or LDAP users cannot lock the local console.

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 8 characters, however, this limit can be changed by your system administrator.
- The characters must 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.

If you select LDAP authentication, no additional information is required.

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 that are created by using the **Manage Task and Resource Roles** task.

See “HMC tasks, user roles, IDs, and associated commands” on page 9 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:

- hmcservicerep (Service Representative)
- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)
- hmcsuperadmin (Super Administrator).

To add or customize a user profile, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage User Profiles and Access**.
3. 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 you are creating a user ID with the same attributes as an existing profile, point to **User** on the menu bar and when its menu is displayed, click **Copy**. The **Copy User** window is displayed.

     Note: Some user profiles are predefined, such as a default ID, and those permissions cannot be changed. However, you can copy a default user profile, such as operator, and then modify the resulting new user profile. The newly defined user cannot have greater permissions than the original copied user profile.
   - From the **User Profiles** window, if you are deleting a user ID, point to **User** on the menu bar and when its menu is displayed, click **Remove**. The **Remove User** window is displayed.

- From the **User Profiles** window, if the user ID 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.
  - To specify timeout and inactivity values, click **User Properties** from the **Modify User** window.

4. 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 and modifying timeout and inactivity values.

Adding, Copying, or Modifying User Profiles

Learn how to add, copy, or modify user profiles.

Users who remotely authenticate through Kerberos or Lightweight Directory Access Protocol (LDAP) must have their profiles set appropriately. You must set the user profile of each remotely authenticated Kerberos or LDAP user to use that type of authentication instead of local authentication. A user that is set to use Kerberos or LDAP remote authentication always uses that type of authentication, even when the user logs into the HMC locally.

Note: The use of Kerberos authentication requires configuration of a key distribution center (KDC) server by using the **KDC Configuration** task. The use of LDAP authentication requires configuration of an LDAP server by using the **LDAP Configuration** task. You do not need to set all users to use Kerberos or LDAP remote authentication. You can set some user profiles so that the users can use local authentication only.

From the Adding, Copying, or Modifying User Profiles window, you can modify the following attributes:

- **User ID**: Enter the user ID for the user profile you are creating or managing. The user name must start with an alphabetic character and consist of 1 to 32 characters.
- **Description**: Enter a meaningful description for your own records.
- **Password**: Enter the password for the user ID.
- **Confirm password**: Enter the password again for verification.
- **Password expires in (days)**: Specify the number of days a password is valid before it expires. This input field is available when **Enforce strict password rules** check box is selected.
- **Manage resource roles**: Displays the managed resource roles that are currently available. Select one or more managed resource roles to define access permissions for this user ID.
- **Task roles**: Displays the task roles that are currently available. Select one task role for this user ID.

Use the online Help if you need additional information about creating, modifying, copying, or removing a user profile and modifying timeout and inactivity values.

User Properties

Learn how to specify timeout and inactivity values for the selected user.

You can specify the amount of time for the following timeout and inactivity tasks:

Timeout Values

- **Session timeout minutes**: Specifies the number of minutes during a logon session that a user is prompted for identity verification. If a value other than zero is specified, the user is prompted after the specified time is reached to reenter their password. If a password is not reentered within the specified amount of time in the **Verify timeout minutes** field, the session is disconnected.
- **Verify timeout minutes**: Specifies the amount of time that is required for the user to reenter their password when prompted, if a value was specified in the **Session timeout minutes** field. If the password is not reentered within the specified time, the session is disconnected.
- **Idle timeout minutes**: Specifies the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session is locked and the screen saver starts. Clicking anywhere on the screen prompts the user for identity verification.

- **Minimum time in days between password changes**: Specifies the minimum amount of time in days that must elapse between changes for the user's password.

Note: A note of zero in any of these fields indicates that there is no expiration of time and it is the default value. You can specify up to a maximum value of 525600 minutes (equivalent to one year).

Inactivity Values

- **Disable for inactivity in days**: Specifies the amount of time in days a user is temporarily disabled after the maximum number of days of inactivity is reached.
- **Never disable for inactivity**: Option to never disable a user's session due to inactivity.
- **Allow remote access via the web**: Option to enable remote web server access for the user you are managing.

Manage Users and Tasks

Display the logged on users and the tasks they are running.

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage Users and Tasks**.
3. 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
4. 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**.
5. When you have completed this task, click **Close**.

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.

If the automatic resource role update function is enabled on the Hardware Management Console (HMC) either through the command line interface or through the Rest API CLI runner job, the HMC user can automatically receive permission to the logical partition that is created. If the logical partition is deleted, the permission is automatically revoked.

The predefined managed resource roles include:

- All System Resources

The predefined task roles include:

- hmcservicerep (Service Representative)
- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)
- hmcsuperadmin (Super Administrator)

To customize managed resource roles or task roles:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage Task and Resource Roles**.
3. From the **Manage Task and Resource Roles** window, select either **Managed Resource Roles** or **Task Roles**.
4. 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**.
5. Click **Exit** when you are have completed the task.

Use the online Help to get additional information for customizing managed resource roles and task roles.

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. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage Certificates**.
3. 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**.

Note: If you have a certificate signed by a Certificate Authority (CA) that consists of a root certificate, intermediate certificate, and a client or leaf certificate, complete the following steps to upload the certificate to the HMC:

- Open the CA signed certificate file by using a text-based editor and split the content of the file and save as three separate files. The first file is the client or leaf certificate, the second file is the intermediate certificate, and the third file is the root certificate.
- Log in to the HMC to import the certificate. First upload the client certificate and click **Yes** for uploading more files. In the new window, upload the intermediate certificate and the root certificate.
- Click **OK** to restart the console.

- 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

4. Click **Apply** for all changes to take effect.

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

Manage Certificate Revocation List

Use this task to create, modify, delete, and import the certificate revocation list that is used on your Hardware Management Console (HMC).

All remote browsers that are accessing the HMC must use Secure Sockets Layer (SSL) encryption. 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 certificate revocation list, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage Certificate Revocation List**.
3. Use the menu bar from the **Manage Certificate Revocation List** window for the actions you want to take with the certificates:
   - To create a new certificate revocation list for the console, click **Import**, then select **New CRL**. Determine whether your certification revocation list is imported from removable media on the console or from the file system on the system that is running the web browser.

     Note: If the list is from removable media, then the certificate revocation list file must be in the top directory on the media.
   - To modify a certificate revocation list on the console, select the certification revocation list from the table, and make appropriate changes, then click **Apply**.
   - To delete a certificate revocation list from the console, click **Selected**, then select **Delete CRL**. Select the certification revocation list, then click **OK**.
   - To work with existing and archived certificates or signing certificates, click **Advanced**.

Use the online Help if you need additional information for managing your certificate revocation list.

Manage LDAP

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, complete the following steps:

Procedure

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Systems and Console Security**.
2. In the content pane, click **Manage LDAP**. The **LDAP Server Definition** window opens.
3. Select **Enable LDAP**.
4. Define an LDAP server to use for authentication (for example, Microsoft Active Directory, Tivoli®, and Open LDAP).
5. Define the LDAP attribute that is used to identify the authenticated user. The default is **uid**, but you can use your own attributes. For Microsoft Active Directory, use **sAMAccountName** as the attribute.
6. Define the distinguished name tree, also known as the search base, for the LDAP server.
7. Click **OK**.

What to do next

If you want to use LDAP authentication, you must configure each remote user's profile so that it uses LDAP remote authentication instead of local authentication.

Manage KDC

View the key distribution center (KDC) servers that are used by this Hardware Management Console (HMC) for Kerberos remote authentication.

From this task, you can complete the following tasks:

- View existing KDC servers.
- Modify existing KDC server parameters that include 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 that is 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, by using its password. If the client successfully decrypts the TGT (for example, 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 fails.

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 that 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 by using the `ktadd` command. Other Kerberos implementations might 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 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 you use this option.
- A remote site that uses secure FTP. You can import a service-key file from any remote site with SSH installed and running.

To use Kerberos remote authentication for this HMC, complete the following tasks:

- 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 76 task from the **HMC Management** icon  , and then selecting **Console Settings**.
- 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 always uses Kerberos remote authentication, even when the user logs on to 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 you use 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 example shows how to create the service key file on a Kerberos server by 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 looks like the following example:

  – `# 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 by using GSSAPI. For remote login without a password through Kerberos to an HMC, configure the HMC to

use a service key. After the configuration is completed, use `kinit -f principal` to obtain forwardable credentials on a remote Kerberos client machine. You can then enter the following command to log in to the HMC without having to enter a password: `$ ssh -o PreferredAuthentications=gssapi-with-mic user@host`.

To manage the KDC, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. From the **Manage KDC** window, select the appropriate task from the available options under the **Actions** menu.
4. When you complete the task, click **OK**.

Use the online Help if you need additional information for Managing KDC.

View KDC Server

Display existing key distribution center (KDC) servers on the Hardware Management Console (HMC).

To view existing KDC Servers on your HMC, click the **Users and Security** icon  , and then select **Users and Roles**. In the content 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

Learn how to modify the key distribution center (KDC) on your Hardware Management Console (HMC).

To modify existing key distribution center (KDC) server parameters, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. Select a KDC Server.
4. 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.
5. Click **OK**.

Add KDC server

Add a Key Distribution Center (KDC) server to this Hardware Management Console (HMC).

To add a new KDC server, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. From the **Actions** drop down list, select **Add KDC Server**.
4. Enter the host name or IP address of the KDC server.
5. Enter the KDC server realm.
6. Click **OK**.

Remove KDC server

Kerberos authentication on the Hardware Management Console (HMC) remains enabled until all key distribution center (KDC) servers are removed.

To remove a KDC server:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. Select the KDC server from the list.
4. From the **Actions** drop down list, select **Remove KDC Server**.
5. Click **OK**.

Import Service Key

Before you can import a service key file into an Hardware Management Console (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, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. From the **Actions** drop down list, select **Import Service Key**.
4. 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.

5. Click **OK**.

Implementation of the service key file will not take effect until the HMC is rebooted.

Remove Service Key

Learn how to remove a service key from your Hardware Management Console (HMC).

To remove the service key from the HMC, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Manage KDC**.
3. From the **Actions** drop down list, select **Remove Service Key**.
4. Click **OK**.

You must reboot the HMC after removing the service key. Failure to reboot may cause login errors.

Manage MFA

Learn how to enable Multi-Factor Authentication (MFA) on the Hardware Management Console (HMC).

Notes:

1. Multi-Factor Authentication is disabled on the HMC by default.
2. For HMC GUI login, when MFA is enabled and the user is configured on the PowerSC MFA server, enter the Cache Token Credential (CTC) code in the password field.
3. For Secure Shell (SSH) login:

   When MFA is enabled, all users that login through SSH are prompted for a CTC code. If the user is configured on the PowerSC MFA server, then you can enter the CTC code at the prompt. If the user is not configured on the PowerSC MFA server, press `Enter` when prompted for CTC code, and then enter the password of the user at the prompt.

To enable Multi-Factor Authentication, complete the following steps:

1. In the navigation area, click the **Users and Security** icon  , and then select **Systems and Console Security**.
2. In the content pane, click **Manage MFA**.
3. From the **Manage MFA** window, select the **Enable multi factor authentication** check box.
4. Enter the following information:
   - **Host name or IP address of the authentication server**
   - **Port of the authentication server**
5. Click **OK**.

Use the online Help if you need additional information about this task.

Enable Remote Command Execution

This task is used to enable remote command execution using the ssh facility.

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Enable Remote Command Execution**.
3. From the **Enable Remote Command Execution** window, select **Enable remote command execution using the ssh facility**.
4. Click **OK**.

Enable Remote Operation

This task is used to allow the HMC to be accessed at a remote workstation through a web browser.

To enable the HMC remote access:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Enable Remote Operation**.
3. Select **Enabled** from the Remote Operation drop-down list, then click **OK**. The HMC can be accessed from a remote workstation using a Web browser.

Use the online Help to get additional information for allowing remote access to the HMC.

Enable 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. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Enable Remote Virtual Terminal**.
3. From the **Enable Remote Virtual Terminal** window, you can enable this task by selecting Enable remote virtual terminal connections.
4. Click **OK** to activate your changes.

Use the online Help to get additional information for enabling a remote terminal connection.

Serviceability tasks

The tasks that are available on the HMC for the **Serviceability** tasks are described.

Note: Depending on the task roles assigned to your user ID you may not have access to all the tasks. See "HMC tasks, user roles, IDs, and associated commands" on page 9 for a listing of the tasks and the user roles allowed to access them.

Tasks Log

View all the tasks that are currently running or completed on the Hardware Management Console (HMC).

To view the tasks log, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Tasks Log**.
2. You can view the following tabs in the tasks log:
   - **Task name**: Displays the name of task.
   - **Status**: Displays the current state of the task (running or completed).
   - **Resource**: Displays the name of the resource.
   - **Resource type**: Displays the type of resource.
   - **Initiator**: Displays the name of the user that initiated the task.
   - **Start time**: Displays the time that the task was initiated.
   - **Duration**: Displays the amount of time that the task took to complete.

Use the online Help for additional information about viewing the tasks log.

Console Events Logs

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

To view console events legs, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Console Events Logs**.
2. 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.
3. 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.

Serviceable Events Manager

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 want to view, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Serviceable Events Manager**.
2. From the **Serviceable Events Manager** 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.

Events Manager for Call Home

Learn how to monitor and approve any data that is being transmitted from an HMC to IBM.

1. In the navigation area, click the **Serviceability** icon  , and then select **Events Manager for Call Home**.
2. From the **Events Manager for Call Home** window, select **Manage Consoles** to manage the list of registered management consoles. You can use the **Event Criteria** to specify the approval state, status, and originating HMC to filter the list of events that are available for all registered management consoles. You can use the criteria to filter the view and select events to view details, view files, and complete call home operations.
3. Click **OK** to exit Events Manager for Call Home and to save the filter values.

Use the online Help if you need additional information about this task.

Create Serviceable Event

This task reports problems that occurred on your Hardware Management Console (HMC) 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, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Create Serviceable Event**.
3. From the **Create Serviceable Event** window, select a problem type from the list displayed.
4. 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 Dumps

Learn how to manage the procedures for dumps of selected systems on your Hardware Management Console (HMC).

To manage a dump, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.

2. In the content pane, click **Manage Dumps**.
3. 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.
4. Click **OK** when you complete this task.

Use the online Help to get additional information for managing dumps.

Transmit Service Information

Transmit service information to your service provider immediately or schedule when to transmit service information for use for problem determination.

To schedule or transmit service information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Transmit Service Information**.
3. In the content pane, click the **Schedule and Send Data** tab to schedule the service information.

   Note: You can also click the following tabs to select the data that you want to send and to configure FTP connections:

   - **Schedule and Send Data**: Transmit information to your service provider immediately or schedule the transmission.
   - **Configure FTP Connection**: Provide configuration data to allow the use of FTP to offload service information.
   - **Send Problem Reports**: Select the data that you want and the destination for the data.
4. Select the types of service information that you want to enable regular transmissions or to send immediately.
   - **Operational Test (Heartbeat) Information -- always enabled**: Send the Problem Event log file.
   - **Hardware Service Information (VPD)**: Send the Vital Product Data (VPD) for all managed systems that are attached to this HMC.
   - **Software Service Information**: Send the VPD for all software that is running on the partitions.
   - **Performance Management Information**: Gather and send the performance management information.
   - **Update Access Key Information**: Verifies and updates Access Key information.
5. Select the interval (in days) and the time to schedule repeating transmissions. To transmit the information immediately, click **Send Now**.
6. Click **OK**.

Use the online Help for additional information about scheduling service information.

Format Media

This task formats a diskette or USB 2.0 Flash Drive Memory Key.

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

To format a diskette or USB 2.0 Flash Drive Memory Key, complete the following steps:

1. In the navigation area, click the **HMC Management** icon  , and then select **Console Managment**.
2. In the content pane, click **Format Media**.
3. From the **Format Media** window, select the type of media you want to format, then click **OK**.
4. Make sure that your media is correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
5. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information about this task.

Electronic Service Agent Setup Wizard

Learn how to open the Electronic Service Agent Setup wizard using the Hardware Management Console (HMC) interface.

About this task

To open the Electronic Service Agent Setup wizard, complete the following steps:

Procedure

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the contents pane, select **Electronic Service Agent Setup Wizard**. The Electronic Service Agent wizard opens. Follow the instructions in the wizard to configure call-home tasks.

Authorize User

Request authorization for Electronic Service Agent. Electronic Service Agent associates your system with a user ID and allows access to system information through the Electronic Service Agent facility. This registration is also used by your operating system to automate service processes for your AIX or IBM i operation system.

To register a user ID, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Authorize User**.
3. Provide a user ID that is registered with the Electronic Service Agent. If you need a user ID, you can register at the IBM Registration website.
4. Click **OK**.

Use the online Help if you need additional information for registering a customer user ID with the eService website.

Enable Electronic Service Agent

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 81.

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. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Enable Electronic Service Agent**.
3. From the **Enable Electronic Service Agent** window, select a system or systems you want to enable or disable the call-home state.
4. Click **OK** when you have completed the task.

Use the online Help if you need additional information for enabling the Electronic Service Agent.

Manage Outbound Connectivity

Customize the means for outbound connectivity for the Hardware Management Console (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 81.

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 the IBM Service Support System for the purpose of conducting automated service operations. The connection can only be initiated by the HMC. IBM Service Support System cannot and never attempts to initiate a connection to the HMC.

To customize your connectivity information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Outbound Connectivity**.
3. 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.
4. The dial information window displays the following tabs for providing input:
   - Local Modem
   - Internet
   - Internet VPN

- Pass-Through Systems

5. 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 **Modern 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.
6. If you want to allow connectivity over the Internet, use the **Internet** tab, then select **Allow an existing internet connection for service**.
7. 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.
8. 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.
9. 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

Learn how to allow your service provider to temporarily access your local console, such as the Hardware Management Console (HMC), or the partitions of a managed system.

To manage inbound connectivity, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Inbound Connectivity**.
3. From the **Manage Inbound Connectivity** settings window, you can perform the following tasks:
   - 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.
4. Click **OK** to proceed with your selections.

Use the online Help if you need additional information about this task.

Manage Customer Information

This task enables you to customize the customer information for the Hardware Management Console (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 81.

The **Manage Customer Information** window displays the following tabs for providing input:

- Administrator
- System
- Account

To customize your customer information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Customer Information**.
3. From the **Manage Customer Information** window, provide the appropriate information on the **Administrator** page.

   Note: Information is required for fields with an asterisk (*).
4. Select the **System** and **Account** tabs from the **Manage Customer Information** window to provide additional information.
5. Click **OK** when you have completed the task.

Use the online Help to get additional information about customizing your account information.

Manage 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, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Event Notification**.
3. From the **Manage Event Notification** window, you can complete the following tasks:
   - Use the **Email** tab to add the email addresses that are notified when problem events occur on your system and when scheduled operations are planned for 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 programming interface events.
4. Click **OK** when you complete this task.

Use the online Help if you need additional information about this task.

Manage Connection Monitoring

Learn how to configure the timers that the 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, complete the following steps:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Connection Monitoring**.
3. From the **Manage Connection Monitoring** window, adjust the timer settings, if required, and enable or disable the server.

4. Click **OK** when you have completed the task.

Use the online Help if you need additional information about connection monitoring.

Remote operations

Connect to and use the Hardware Management Console (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 that is 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 extra consideration. LAN connectivity provides acceptable communications for either a remote HMC or web browser control.

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 might exist between the remote HMC and its managed objects must allow the HMC to service processor communications to occur. A remote HMC might also need communication with another HMC for service and support. Table 10 on page 105 shows the ports that a remote HMC uses for communications.

Table 10. 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).

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 wanted.

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 that are connected to a single local Hardware Management Console (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 setup to allow incoming requests on these ports. Table 11 on page 106 shows the ports that a web browser needs for communicating with an HMC.

Table 11. Ports that are used by a web browser for communications to the HMC

Port	**Use**
TCP 443	Secure (HTTPS) remote interface communication
TCP 8443	Secure browser access to web server communication
TCP 9960	Browser applet communication
[1]This port is opened in the HMC firewall when remote access is enabled in HMC Version 7.8.0 and later. This port must also be opened in any firewall that is between the remote client and the HMC.	

After an HMC is 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 that is 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 by using a LAN TCP/IP connection and by 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.

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 perform 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 by 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 host name mismatch message is displayed. To avoid this message, a Firefox browser is used or a host name is configured for the HMC, by using the **Change Network Settings** task (see “Change Network Settings” on page 75), and this host name is specified in the URL instead of an IP address. For example, you can use the format https://*host name.domain_name* or https://*host name* (for example, by using https://hmc1.ibm.com or https://hmc1).

Preparing to use the web browser

Perform the necessary steps to prepare to use a web browser to access the Hardware Management Console (HMC).

Before you can use a web browser to access an HMC, you must complete the following tasks:

- Configure the HMC to allow remote control for specified users.
- For LAN-based connections, you must know the TCP/IP address of the HMC to be controlled, and correctly set up any firewall access between the HMC and the web browser.
- Have a valid user ID and password that is assigned by the access administrator for HMC web access.

Web browser requirements

Learn about the requirements your web browser must meet to monitor and control the Hardware Management Console (HMC).

HMC web browser support requires HTML 2.0, JavaScript 1.0, Java™ Virtual Machine (JVM), Java Runtime Environment (JRE) Version 7, and cookie support in browsers that connect to the HMC. Contact your support personnel to assist you in determining whether 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-up windows must be enabled for all HMCs addressed in the browser if the browser is running with pop-up windows disabled. The following browsers have been tested:

Google Chrome
HMC Version 8.1 supports Google Chrome Version 33.

Microsoft Internet Explorer
HMC Version 8.1 supports Internet Explorer 9.0, Internet Explorer 10.0, and Internet Explorer 11.0.

Note: The performance CEC task is not supported in Internet Explorer 9.0.

- If your browser is configured to use an Internet proxy, then local IP addresses are included in the exception list. For more information, see your network administrator. 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 8.1 supports Mozilla Firefox Version 17 and Mozilla Firefox Version 24 Extended Support Release (ESR). 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. For more information about the latest Mozilla Firefox ESR levels, see Security Advisories for Firefox ESR.

Note: The following restrictions apply when you are using Mozilla Firefox while the HMC is in NIST SP 800-131a security mode:

- Mozilla Firefox cannot be used for the remote client.
- The local console cannot be used.

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 that 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.

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 must 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 develop a consistent way to manage the managed systems, you can automate the operations by starting 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 the console window.

Setting up secure script execution between SSH clients and the HMC

You must ensure that your script executions between Secure Shell (SSH) clients and the Hardware Management Console (HMC) are secure.

HMCs typically are placed inside the server 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, complete the following steps:

1. Enable remote command execution. For more information, see “Enable Remote Command Execution” on page 97.
2. On the client's operating system, run the SSH protocol key generator. To run the SSH protocol key generator, complete the following steps:
   a. To store the keys, create a directory that is 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>
   ```

   Note: Double quotes (“) are used in commands to ensure that the remote shell can properly process the command. For example:

   ```
   ssh "mkauthkeys hscuser@somehmchost --add 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDa+Zc8+hn1+
   TjEXu640LqnVNB+UsixIE3c649Cgj20gaVWnFKTjcpWVahK/duCLac/zteMtVAfCx7/ae2g5RTPu7FudF2xjs4r
   +NadVXhoIqmA53a
   NjE4GILpfe5vOF25xkBdG9wxigGtJyOKeJHzgnElP7RlEeOBijJDKo5gGE12NVfBxboChm6LtKnDxLi9ahhOYtLlFehJr
   6pV/lMAEu
   Lhd6ax1hWvwrhf/
   h5Ym6J8JbLVL3EeKbCsuG9E4iN1z4HrPkT5OQLqtvC1Ajch1ravsaQqYloMTWNFzM4Qo5O3fZbLc6RuJjtJv8C5t
   4/SZUGHZxSPnQmkuii1z9hxt hscpe@vhmccloudvm179'"
   ```

To delete the key from the HMC, you can use the following command:

```
ssh hmcuser@hmchostname mkauthkeys --remove joe@somehost
```

To enable passwords that prompts 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 and 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 Hardware Management Console (HMC).

To enable or disable remote commands, complete the following steps:

1. In the navigation area, select the managed system and click the **Users and Security** icon  , and then select **Users and Roles**.
2. In the content pane, click **Enable Remote Command Execution**.
3. From the **Enable Remote Command Execution** window, select from the following options:
   - 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.
4. Click **OK**.

Logging in to the HMC from a LAN-connected web browser

Log in to the Hardware Management Console (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 has LAN connectivity to the wanted HMC.
2. From your web browser, enter the URL of the wanted HMC in the format `https://hostname.domain_name` (for example: `https://hmc1.ibm.com`) or `https://xxx.xxx.xxx.xxx`.

   If this connection is the first access of the HMC for the current web browser session, you might receive a certificate error. This certificate error is displayed if any of the following conditions occur:

   - The web server that is contained in the HMC is configured to use a self-signed certificate and the browser is not configured to trust the HMC as an issuer of certificates.
   - The HMC is configured to use a certificate that is signed by a certificate authority (CA) and the browser is not configured to trust this CA.

   In either case, if you know that the certificate that is being displayed to the browser is the one used by the HMC, you can continue and all communications to the HMC is 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 permanently trusts the issuer of the certificate.
   - By viewing the certificate and installing to the database of trusted CAs, the certificate of the CA that issues the certificate is used by the HMC.

   If the certificate is self-signed, the HMC itself is considered the CA that issues the certificate.
3. When prompted, enter the user name and password that is assigned by your administrator.

Managing OpenBMC-based and BMC-based systems by using the HMC

Learn how to manage OpenBMC-based and BMC-based systems by using the Hardware Management Console (HMC).

About this task

Learn about the tasks that you perform from the console and how to navigate the baseboard management controller (BMC) by using the web-based user interface with graphical views of managed systems and simplified navigation.

Note: You cannot manage OpenBMC-based and BMC-based systems while the HMC is running in NIST mode.

Add Managed Systems

Learn how to add a managed Baseboard Management Controller (BMC) system to the Hardware Management Console (HMC).

To add one or more managed BMC systems to the HMC, complete the following steps:

1. From the HMC dashboard, click **Connect Systems**
2. From the **Add Managed Systems** window, you can add a BMC system by completing the following fields:
   - **IP Address/Host name**
   - **Username (BMC system)**

     Notes:

     – For model 8335-GTH and 8335-GTX, the default user name is `admin`.
     – For model 9006-12P and 9006-22P, the default user name is `ADMIN`.
   - **Password**

   Alternatively, you can specify a range of IP addresses and click **OK** to view a list of systems that were discovered. You can select one or more discovered systems to add to the HMC.

   Note: The discovery process can take a long time to complete.
3. Click **OK** to add the managed system to the HMC.

Use the online Help if you need additional information about this task.

Systems Management for Servers

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

These tasks are listed when a managed system is selected. The tasks that are listed in the menu pod change as selections are made in the work area.

Operations

Operations contains the tasks for operating managed systems.

Power Off

Shut down the managed system.

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).

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 default setting is set to the following value:

- **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 startup. 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 is powered off. This option is always available for selection.

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 might 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 perform the following tasks:

- Schedule an operation to run later.
- 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 you want the operation to repeat, you are asked to select the following options:

- 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 operations:

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.

To schedule operations on the managed system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. In the content pane, select one or more managed systems.
3. In the menu pod, select **Actions** > **View All Actions** > **Operations** > **Schedule Operations**.
4. From the **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 that 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 that you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation that 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**.

Launch BMC System Management

The Hardware Management Console (HMC) can connect directly to the Baseboard Management Controller (BMC) for a selected system.

The BMC system management 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 BMC, complete the following steps:

Note: To access the BMC user interface, you must be at the console or have access to the BMC by using a supported web browser.

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. In the content pane, select one or more managed systems.
3. In the menu pod, select **Actions** > **View All actions** > **Operations** > **Launch BMC System Management**.
4. Click **Continue**.

Configuring Call Home

Problems on your BMC-based managed system are reported to the Hardware Management Console (HMC) as events. You can set up alerts to be automatically notified of any events.

Note: You must enable SNMP traps in the HMC to receive alerts. To enable SNMP traps, navigate to **Console Settings** > **Change Network Settings** > **LAN Adapters** > **Details** > **Firewall Settings**. Select **SNMP Traps** and **SNMP Agent** from the table and then click **Allow Incoming**.

To set up alerts for call home, complete the following steps:

Note: This procedure is applicable for model 9006-12P, 9006-22C, and 9006-22P.

1. From the **BMC System Management** window, click **Configuration** > **Alerts**.
2. Select any alert from the table and click **Modify**.

Note: You can set up multiple HMCs to receive traps. Duplicate reporting of events by multiple HMCs is possible as duplicate event verification is not performed.

3. Complete the following fields:
   - **Event Severity**
   - **Destination IP**
4. Click **Save**.
5. Verify the new alert in the table.

Use the online Help if you need additional information about this task.

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.

Updates

Display tasks to view system information, manage updates on your Hardware Management Console (HMC), or check system readiness.

Change Licensed Internal Code

Change the Licensed Internal Code of a managed BMC system by using your Hardware Management Console (HMC).

The system firmware is a combination of the BMC firmware and the PNOR firmware. You must update both the BMC firmware and the PNOR firmware for the system to operate properly. If you update only one type of firmware, but do not update the other type of firmware, system errors might occur.

To change the Licensed Internal Code, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. Select the server for which you want to view system information.
3. In the menu pod, expand **Actions** and then expand **Updates**.
4. Select **Change Licensed Internal Code** > **BMC Change Licensed Internal Code**.
5. Follow the onscreen instructions in the **BMC Change Licensed Internal Code** guided wizard.

   Note: The BMC system must be in the powered off state before you can proceed with the wizard.
6. When you complete this task, click **Close**.

Use the online Help if you need additional information about this task.

Attention LED

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

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 states:

- Electrical power is present.
- Activity is occurring on a link. (The system might 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 flashing, identify the problem and take the appropriate action to restore the system back 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.

You can deactivate a system attention LED. For example, you might determine that a problem is not a high priority and decide to repair the problem later. 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.

Connections

You can view the Hardware Management Console (HMC) connection status to service processors, reset those connections, connect another HMC to the selected managed system, or disconnect another HMC.

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

Service Processor Status

View information about the status of the Hardware Management Console (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, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. Select the server for which you want to view service processor connection status.
3. In the menu pod, select **Actions** > **View All Actions** > **Connections** > **Service Processor Status**.

Reset or Remove Connections

Reset or remove a managed system from the Hardware Management Console (HMC) interface.

About this task

To reset or remove connections, complete the following steps:

Procedure

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. Select the server that you want to reset or remove.

3. In the menu pod, select **Actions** > **View All Actions** > **Connections** > **Reset or Remove Connections**.
4. Select **Reset Connection** or **Remove Connection**.
5. Click **OK**.

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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 or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM'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 actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

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

Accessibility features for IBM Power Systems servers

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The IBM Power Systems servers include the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Power Systems servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content

Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power Systems servers.

The IBM Power Systems servers online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Keyboard navigation

This product uses standard navigation keys.

Interface information

The IBM Power Systems servers user interfaces do not have content that flashes 2 - 55 times per second.

The IBM Power Systems servers web user interface relies on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The IBM Power Systems servers web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

The IBM Power Systems servers include certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s user name and IP address for purposes of session management. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en/ in the section entitled "Cookies, Web Beacons and Other Technologies".

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 9 Release 2 Maintenance Level 950.

Trademarks

IBM, the IBM logo, and 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 Copyright and trademark information.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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.

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 IBM 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 IBM.

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 IBM.

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.

IBM 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 IBM, 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.

IBM 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.