Power Systems

Managing the Hardware Management Console by using the HMC Enhanced+ interface

Power Systems

Managing the Hardware Management Console by using the HMC Enhanced+ interface

Note
Before using this information and the product it supports, read the information in "Notices" on page 91.

This edition applies to IBM Hardware Management Console Version 8 Release 8.7.0 Maintenance Level 0 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Managing the HMC by using the HMC Enhanced+ interface

Learn how to use the Hardware Management Console (HMC) by using the HMC Enhanced+ interface.

Note: The procedures and functions of the HMC Enhanced + Tech Preview (Pre-GA) interface, which was an option that was provided with HMC version 8.20, are the same as the HMC Enhanced+ interface that is provided with HMC version 8.30. Only the HMC Enhanced+ is referred to in the documentation, but that content also applies to the HMC Enhanced + Tech Preview (Pre-GA) interface.

The HMC Enhanced+ interface provides an intuitive interface work environment with graphical views of managed systems and simplified navigation. Learn about the tasks that you can use on the console and how to navigate by using the web-based user interface.

Note: The functions of the HMC Enhanced interface, which was an option that was provided with HMC version 8.10.1, or later, are now available as a part of the HMC Enhanced+ interface that is provided with HMC version 8.30.

What's new in Managing the HMC through the HMC Enhanced+ interface

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

August 2017

- The HMC Classic interface is not supported on Hardware Management Console (HMC) version 8.7.0, or later. The functions that were previously available with the HMC Classic interface are now available with the HMC Enhanced+ interface.
- Added the following topics:
  - "Partition Availability Priority" on page 28
  - "Manage Partition Data" on page 29
  - "Manage System Profiles" on page 29
  - "View Workload Management Groups" on page 29
  - "Utilization Data" on page 31
  - "Systems Management for Frames" on page 47
  - "Create Welcome Text" on page 57
  - "Manage Certificate Revocation List" on page 71
  - "All System Plans" on page 65
- Updated the following topics:
  - "Transmit Service Information" on page 80
  - "Events Manager for Call Home" on page 78

October 2016

- Added the "Tasks Log" on page 77 topic.
- Updated the "Using the web-based user interface" on page 3 topic.

May 2016

- Updated the "Transmit Service Information" on page 80 topic.

October 2015

- Added the following topics:
  - "SR-IOV Firmware Update" on page 32
  - "Test Network Connectivity" on page 54
  - "View Network Topology" on page 53
  - "Update the Hardware Management Console" on page 59
  - "OS and VIOS Images" on page 63
  - "Adding, Copying, or Modifying User Profiles" on page 68
- Updated the "Templates and OS Images" on page 62 topic.

June 2015

- The procedures and functions of the HMC Enhanced + Tech Preview (Pre-GA) interface, which was an option that was provided with HMC version 8.20, are the same as the HMC Enhanced+ interface that is provided with HMC version 8.30. Only the HMC Enhanced+ is referred to in the documentation, but that content also applies to the HMC Enhanced + Tech Preview (Pre-GA) interface.
- The functions of the HMC Enhanced interface, which was an option that was provided with HMC version 8.10.1, or later, are now available as a part of the HMC Enhanced+ interface that is provided with HMC version 8.30.
- Added the "User Properties" on page 69 and "Session handling" on page 20 topics.
- Updated the "Power Management" on page 23 topic.

November 2014

- Added information about the HMC Enhanced + Tech Preview (Pre-GA) interface for HMC Version 8, Release 2, or later on IBM® Power Systems™ servers that contain the POWER8® processor.

Introduction to the HMC

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

The HMC allows you to configure and manage servers. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To ensure consistent function, each HMC is shipped preinstalled with the HMC Licensed Machine Code Version 8, Release 3.

Note: Virtualization is not supported on the IBM Power® System S824L (8247-42L) server.

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

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

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

Redundant or Dual HMCs
: A server might be managed by either one or two HMCs. When two HMCs manage one system, they are peers, and each HMC can be used to control the managed system. The best practice is to attach one HMC to the service networks or HMC ports of the managed systems. The networks

are intended to be independent. Each HMC might be the 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.

Predefined user IDs and passwords

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

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

Table 1. Predefined HMC user IDs and passwords

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

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, help options, and the logo.

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

The *content pane*, in the right portion of the window, displays information 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 selecting 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 dragging the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size. You can also do this within the work pane border that separates the resources table from the taskpad.

Note: Pop-up windows must be enabled to use all the 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 Enhanced+ 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)
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 perform different tasks on the managed system. HMC roles are either predefined or customized.

The roles that are discussed in this section 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 varying levels of access to tasks available on the HMC interface. For more information about the tasks each HMC user role can perform, see “HMC tasks, user roles, IDs, and associated commands” on page 7.

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

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.	**hmcpe**
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 perform 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 88.

Some tasks can only be performed using the command line. For a listing of those tasks, see Table 9 on page 18.

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
Service Management	Table 6 on page 10
Systems Management	Table 7 on page 11
Control Panel Functions	Table 8 on page 17

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 60 bkconsdata	X	X		X
"Change Date and Time" on page 56 chhmc lshmc	X	X		X
"Change Language and Locale" on page 57 chhmc lshmc	X	X	X	X
"Change Network Settings" on page 55 chhmc lshmc	X	X		X
"Change User Password" on page 66 chhmcusr	X	X	X	X
"Manage KDC" on page 72 chhmc lshmc getfile rmfile		X		
"Manage LDAP" on page 72 lshmcldap chhmcldap		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 Guided Setup Wizard" on page 53		X		
Launch Remote Hardware Management Console	X	X	X	X
Lock HMC Screen	X	X	X	X
Logoff or Disconnect	X	X	X	X
"Manage Certificates" on page 70		X		
"Manage Data Replication" on page 61	X	X		
"Managing Installation Resources" on page 63	X	X		
"Manage Task and Resource Roles" on page 70 chaccfg lsaccfg mkaccfg rmaccfg		X		
"Manage User Profiles and Access" on page 67 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		
"Manage Users and Tasks" on page 69 lslogon termtask	X	X	X	X
Open 5250 Console	X	X		X
"Enable Remote Command Execution" on page 76 chhmc lshmc	X	X		X
"Enable Remote Operation" on page 76 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 77	X	X		X
"Restore Management Console Data" on page 61	X	X		X
"Save Upgrade Data" on page 61 saveupgdata	X	X		X
"Schedule Operations" on page 58	X	X		
"Shut Down or Restart" on page 58 hmcshutdown	X	X		X
"Serviceable Events Manager" on page 33 lssvcevents	X	X		X
"View Licenses" on page 59	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 34		X		X
"Serviceable Events Manager" on page 78 chsvcevent lssvcevents		X		X
"Manage Remote Connections" on page 79	X	X		X
"Manage Remote Support Requests" on page 80	X	X	X	X
"Format Media" on page 60	X	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)
"Manage Dumps" on page 80 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Transmit Service Information" on page 80 chsacfg lssacfg	X	X		
"Enable Electronic Service Agent" on page 82	X	X		X
"Manage Outbound Connectivity" on page 83	X	X		X
"Manage Inbound Connectivity" on page 84	X	X		X
"Manage Customer Information" on page 84	X	X		X
"Authorize User" on page 82		X		
"Manage Serviceable Event Notification" on page 84 chsacfg lssacfg	X	X		X
"Manage Connection Monitoring" on page 85	X	X	X	X
"Electronic Service Agent Setup Wizard" on page 82		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)
"Other Properties" on page 21 lshwres	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)**
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
Update Password chsyspwd		X		
Change Default User Interface Settings	X	X	X	X
Operations				
"Power Off" on page 22 chsysstate	X	X		X
"Activate" on page 42 chsysstate	X	X		X
"Save Current Configuration" on page 46 chsysstate	X	X		X
"Restart" on page 42 chsysstate	X	X		X
"Shut Down" on page 42 chsysstate	X	X		X
chlparstate	X	X		X
LED Status: Deactivate Attention LED "Attention LED" on page 26 chled	X	X		
LED Status: Identify LED "Attention LED" on page 26	X	X	X	X
LED Status: Test LED "Attention LED" on page 26	X	X	X	X
"Schedule Operations" on page 24	X	X		
"Launch ASM Interface" on page 25 asmmenu	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)**
"Rebuild" on page 25 chsysstate	X	X		
"Power Management" on page 23 chpwrmgmt lspwrmgmt		X		
"Delete" on page 43 rmsyscfg	X	X		X
"Mobility" on page 44 lslparmigr migrlpar	X	X		X
"Manage Profiles" on page 45 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
"Operations" on page 22	X	X	X	X
Configuration				
"Create Partition from Template" on page 28		X		
"Deploy System from Template" on page 28		X		
"Capture Configuration as Template" on page 28		X		
"Template Library" on page 41		X		
"Manage Custom Groups" on page 46	X	X		X
"Manage Profiles" on page 45 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg	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)**
Save Current Configuration "Save Current Configuration" on page 46 mksyscfg	X	X		
Connections				
"Service Processor Status" on page 27 lssysconn	X	X	X	X
"Reset or Remove Connections" on page 27 rmsysconn	X	X		
"Disconnect Another HMC" on page 27		X		
Hardware (Information)				
"Hardware" on page 35	X	X	X	X
Updates				
"Change Licensed Internal Code" on page 31 lslic updlic		X		X
"Check System Readiness" on page 32 updlic		X		X
"View System Information" on page 31 lslic		X		X
Update HMC updhmc lshmc		X		X
Serviceability				
"Serviceable Events Manager" on page 46 chsvcevent lssvcevents		X		X
"Create Serviceable Event" on page 34		X		X
"Reference Code History" on page 47 lsrefcode	X	X	X	X
"Control Panel Functions" on page 47 lssyscfg	X	X		
"Add FRU" on page 36		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)**
"Add Enclosure" on page 36		X		X
"Exchange FRU" on page 36		X		X
"Remove FRU" on page 36		X		X
"Remove Enclosure" on page 37		X		X
"Power On/Off IO Unit" on page 35		X		X
"Manage Dumps" on page 34 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Collect VPD" on page 35	X	X	X	X
"Type, Model, Feature" on page 35		X		
"Setup FSP Failover" on page 37 chsyscfg lssyscfg		X		
"Initiate FSP Failover" on page 37 chsysstate		X		
Capacity on Demand (CoD)				
Enter CoD code chcod		X		
View History Log lscod	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

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: On/Off CoD: View Billing Information lscod	X	X	X	X
Processor: On/Off CoD: View Code Information lscod	X	X	X	X
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		

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 History Log lscod	X	X	X	X
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		

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		

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 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		
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

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)**
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
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 HMC Enhanced+ interface.

Session limitations

The HMC Enhanced+ interface does not support disconnected sessions like the HMC Classic interface. In the HMC Enhanced+ interface, 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 Enhanced+ interface creates a new session.

1. If you initiate long running tasks from the HMC Enhanced+ 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: You can use the HMC Classic interface to perform long running tasks to avoid these limitations. 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 in the HMC Enhanced+ interface. The HMC Enhanced+ 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.

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.

Other Properties

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

These properties include the following tabs:

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

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

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

I/O The **I/O** tab displays the physical I/O resources for the managed system. The assignment of I/O

slots and partition, the adaptor-type, and the slot LP limit information are displayed. The physical I/O resources information is grouped by units.

- The **Slot** column displays the physical I/O properties of each resource.
- The **I/O Pool** column displays all of the I/O pools found in the system and the partitions that are participating in the pools.
- The **Owner** column displays who currently owns the physical I/O. The value of this column can be any of the following values:
  - When an 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 **Slot LP Limit** column displays the number of logical ports supported by slot or adapter in SR-IOV shared mode.

Migration

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

Power-On Parameters

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

Capabilities

The **Capabilities** tab displays the runtime capabilities of this server. You can verify that the server supports Virtual Trusted Platform Module (VTPM), Virtual Server Network (VSN), Dynamic Platform Optimization (DPO), and SR-IOV capable.

Advanced

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

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

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

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

You can view the VTPM settings.

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 42

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

Choose from the following options:

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

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

Power Management

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

To enable power saver mode, do the following:

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
2. In the content pane, select the server that you want to enable to use power saver mode.
3. In the menu pod, expand **System Actions** and then expand **Operations**.
4. Click **Power Management**.
5. Click **Enabled**.
6. Choose from any of the following Power Saver mode options:
   - **Disable Power Saver mode**: Disables the Power Saver mode. The processor clock frequency is set to its nominal value and the power that is used by the system remains at a nominal level.
   - **Enable Static Power Saver mode**: Reduces the power consumption by lowering the processor clock frequency and the voltage to fixed values. This option also reduces the power consumption of the system while delivering predictable performance.
   - **Enable Dynamic Power Saver (favor power) mode**: Causes the processor frequency to vary based on the processor use. During periods of high use, the processor frequency is set to the maximum value allowed, which might be above the nominal frequency. Additionally, the frequency is lowered below the nominal frequency during periods of moderate and low processor use.
   - **Enable Dynamic Power Saver (favor performance) mode**: Causes the processor frequency to vary based on processor use. During periods of moderate or high use, the processor frequency will be set to the maximum value allowed, which might be above the nominal frequency. Additionally, the frequency is lowered below the nominal frequency during periods of low processor use.
   - **Enable Fixed Maximum Frequency mode**: Causes the processor frequency to be set at a fixed value that you can specify. This option allows you to 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 could schedule power on or off operations for a managed system.

The Scheduled Operations task displays the following information for each operation:
- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the Scheduled Operations window you can do the following:
- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

You can schedule an operation to occur once or you can schedule it to repeat. You must provide the time and date that you want the operation to occur. If the you want the operation to repeat, you will be asked to select the following:
- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

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

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

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

Power Off Managed System
Schedules an operation for a system power off at regular intervals for a managed system.

Power On Managed System
Schedules an operation for a system power on at regular intervals for a managed system.

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

Manage Utility CoD processor minute usage limit
Creates a limit for Utility CoD processor usage.

Modify a Shared Processor Pool
Schedules an operation for modifying a shared processor pool.

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

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

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

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

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, expand **System Actions** and then expand **Operations**.
4. Click **Schedule Operations**
5. 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 you want to delete, point to **Options** and then click **Delete**.
   - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
   - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**.
   - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**.
   - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
6. To return to the HMC workplace, point to **Operations** and then click **Exit**.

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 Servers**.
2. In the content pane, select one or more managed systems.
3. In the menu pod, expand **System Actions** and then expand **Operations**.
4. Select **Launch ASM Interface**.

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. 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 located on or near the components. The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, or processor). LEDs are either green or amber. Green LEDs indicate either of the following:

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

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

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

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

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

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

Choose from the following options:

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

Test Attention LED
Initiates an LED Lamp Test against the selected system. All LEDs will 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 have selected a managed system in the work area, the following tasks pertain to that managed system. If you have selected a frame, the tasks pertain to that frame.

Service Processor Status

View information about the status of the Hardware Management Console (HMC) connection to the service processors on the managed system.

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

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, expand **System Actions** and then expand **Operations**.
4. Select **Service Processor Status**.

Reset or Remove Connections

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

To reset or remove connections, do the following:

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, expand **System Actions** and then expand **Operations**.
4. Select **Reset or Remove Connections**.
5. Select an option and click **OK**.

Disconnect Another HMC

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

To disconnect another HMC, 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 disconnect another HMC.

3. In the menu pod, expand **System Actions** and then expand **Operations**.
4. Select **Disconnect Another HMC**.
5. 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.

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 complete 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 is required when you want to undo dynamic logical partitioning changes for the logical partition. However, this 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 three ways:
  - Restore partition data from a backup file. Profile modifications that are performed 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.

Updates
Display tasks to view system information, manage Licensed Internal Code (LIC) 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 Servers**.
2. Select the server for which you want to view system information.
3. In the menu pod, expand **System Actions** and then expand **Updates**.
4. Select **View System Information**.
5. Select a LIC repository from the list and click**OK**.
6. 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 on your Hardware Management Console (HMC).

You can change the licensed internal code for the current release or to a new release.

To view the 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 **System Actions** and then expand **Updates**.
4. Select **Change Licensed Internal Code**.

Note: Click **Start Change Licensed Internal Code** wizard to perform 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 managed system and power LIC with more options and additional targeting choices.

5. Select an action from the list and click**OK**.
6. When you have completed this task, click **Close**.

Use the online Help if you need additional information for changing the licenses 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 Servers**.
2. Select the server for which you want to view system information.
3. In the menu pod, expand **System Actions** and then expand **Updates**.
4. Select **Check System Readiness**.
5. 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 Servers**.
2. Select the server for which you want to view system information.
3. From the **menu pod**, expand **System Actions** and then expand **Updates**.
4. Select **SR-IOV Firmware Update**.
5. Select and right-click an adapter or adapters to get the context menu.
6. 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.
7. 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.

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 Servers**.
2. Select the server 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 perform from the list.

Serviceable Events Manager

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

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

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
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.
6. Click **OK**.
7. If you do not want the results filtered, select **ALL**.

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

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

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

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

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

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

Create Serviceable Event

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 managed by the HMC.

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

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

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

Use the Manage Dump task to do the following:

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

- View the offload status of a dump as it progresses.

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

Collect VPD

Copy Vital Product Data (VPD) to removable media.

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

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

The information in the VPD file can be used to complete the following types of orders for your managed system:
- Install or remove a sales feature
- Upgrade or downgrade a model
- Upgrade or downgrade a feature

Using this task, this information can be sent to removable media (diskette 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 serial (MTMS) or configuration ID of an enclosure.

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

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

Hardware

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

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 Servers**.
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 task that you want to perform from the list.

Power On/Off IO Unit:

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

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

Add FRU:

Locate and add a Field Replaceable Unit (FRU).

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

Exchange FRU:

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

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

Remove FRU:

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

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

Add Enclosure:

locate and add an enclosure.

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

Remove Enclosure:

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

To remove an enclosure:

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

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 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:

View all open MES order numbers and their states.

Use Close MES Order Number 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:

Setup 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 initiate FSP Failover for the selected managed system.

To initiate the FSP failover, complete the following steps:

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

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 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 pane, click the **Resources** icon  .
2. Click **All Systems**. The All Systems page is displayed.
3. In the work pane, select the system in which the partition is located and click **Actions** > **View System Partitions**. The configuration page opens. You can view the configuration details of the system you selected.
4. In the navigation pane, click **Topology** > **Virtual Networking Diagram** to view the end-to-end network configuration for the selected system.
5. 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.
6. 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.
7. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols used in the virtual networking diagram.

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 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 pane, click the **Resources** icon  .
2. Click **All Systems**. The All Systems page is displayed.
3. In the work pane, select the system in which the partition is located and click **Actions** > **View System Partitions**. The configuration page opens. You can view the configuration details of the system you selected.
4. In the navigation pane, click **Topology** > **Virtual Storage Diagram** to view the virtual storage configuration for the selected system.

   Note: To view the virtual storage diagrams of a single partition in a particular system, select the partition of your choice and then click **Topology** > **Partition Virtual Storage Diagram**.
5. 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.
6. 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.
7. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols used in the virtual storage diagram.

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 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 SR-IOV and vNIC configuration for the selected system by using the HMC, complete the following steps:

1. In the navigation pane, click the **Resources** icon  .
2. Click **All Systems**. The All Systems page is displayed.
3. In the work pane, select the system in which the partition is located and click **Actions** > **View System Partitions**. The configuration page opens. You can view the configuration details of the system you selected.
4. In the navigation pane, click **Topology** > **SR-IOV and vNIC Diagram** to view the SR-IOV and vNIC configuration for the selected system.
5. 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.
6. 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.

7. In the upper-right corner of the work pane, click the **legend** icon to view an explanation of the symbols used in the SR-IOV and vNIC diagram.

Capacity on Demand

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

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

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 function includes the following tasks:

- Managing Virtual I/O Servers
- Managing virtual networks
- Managing virtual storage
- Managing 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

Systems Management for Partitions

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

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

Other Properties

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

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

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

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

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

SR-IOV Logical Ports
The **SR-IOV Logical Ports** tab displays the logical ports that are configured on the partition (view only).

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

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

Change Default Profile

Change the default profile for the partition.

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

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 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.

Template Library

Use the **Template Library** option to access templates that reside in the template library.

You can view, modify, deploy, create, capture, copy, import, export, or delete templates that are available in the template library.

Operations

Operations contains the tasks for operating partitions.

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.
3. In the menu pod, 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.

Restart

Restart the selected logical partition or partitions.

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

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

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

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

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

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

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

Shut Down

Shut down the selected logical partition or partitions.

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

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

Choose from the following options:

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

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

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

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

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 without operator assistance.

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

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

The Scheduled Operations task displays the following information for each operation:
- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the Scheduled Operations window you can do the following:

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

You can schedule an operation to occur once or you can schedule it to repeat. You must provide the time and date that you want the operation to occur. If the you want the operation to repeat, you will be asked to select the following:
- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

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

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

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

Operating System Shutdown (on a partition)
Schedules a shutdown of the selected logical partition.

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

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.

To migrate a partition to another system, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content pane, select the server.
3. In the menu pod, expand **Partitions**, select the partition that you want to migrate to another system.
4. Select **Operations > 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.

To validate the settings, complete the following steps:

1. In the navigation area, click the **Resources** icon  , and then select **All Systems**.
2. In the content pane, select the server.
3. In the menu pod, expand **Partitions**, select the partition that you want to validate the settings for migrating to another system.
4. Select **Operations > 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.

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

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

Configuration

Configuration contains the tasks for configuring your partitions.

Manage Profiles

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

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

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

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

Manage Custom Groups

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

One or more user-defined groups might already be defined on your 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.

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 HMC as serviceable events. You can view the problem, manage problem data, call home the event to your service provider, or repair the problem.

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

1. In the navigation area, click the **Resources** icon  , and then select **All Servers**.
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.
6. Click **OK**.
7. If you do not want the results filtered, select **ALL**.

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

- Problem Number
- PMH Number

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

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

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

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

Reference Code History

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

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

Control Panel Functions

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

(21) Activate Dedicated Service Tools
Starts Dedicated Service Tools (DST) on the partition.

(65) Disable Remote Service
Deactivates remote service on the partition.

(66) Enable Remote Service
Activates remote service on the partition.

(68) Concurrent Maintenance Power Off Domain
Concurrent maintenance power domain Power Off.

(69) Concurrent Maintenance Power On Domain
Concurrent maintenance power domain Power On.

Systems Management for Frames

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

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

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

Operations

Perform tasks on managed frames.

Initialize Frames

Initialize managed frames.

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

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

Initialize All Frames

Initialize all of your frames.

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

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

Rebuild

Update frame information on the HMC interface.

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

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

Change Password

Change the 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. 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 will be disabled for location codes that are not controllable by the HMC.

Configuration

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

Manage Custom Groups

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

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

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

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

Connections

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

The HMC displays the following:
- IP address
- BPA Role
- Connection Status
- Connection Error code

If the status is not Connected, the Connection status may be one of the following 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 performed when the frame is in this state.

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

Pending Authentication - Password Updates Required
The frame access passwords have not been set. You must set the required passwords for the frame, to enable secure authentication and access control from the HMC.

No Connection
The HMC cannot connect to the frame.

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

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

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

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 perform 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, do the following:

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 filtered, select **ALL**.

The Serviceable Events Overview window displays all of the events that match your criteria. The information displayed in the compact table view includes the following fields:
- Problem Number
- PMH Number
- Reference Code - Click **Reference** code to display a description of the problem reported and actions that may be taken to fix the problem.

- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

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

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

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

Hardware

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

Add FRU:

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

To add a FRU, complete the following steps:
1. From the drop down list, 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 have completed the FRU installation process, click **Finish**.

Add Enclosure:

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

To add an enclosure, 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 identified in **Pending Actions** to the selected system, click **Launch Procedure**.
3. When you have completed the enclosure installation process, click **Finish**.

Exchange FRU:

Exchange one FRU with another 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 identified in **Pending Actions** in the selected system by clicking **Launch Procedure**.
3. When you have completed the enclosure replacement process, click **Finish**.

Remove FRU:

Remove a FRU from your managed system.

To remove a FRU, complete the following steps:
1. Select an enclosure from the drop down list.
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 have completed the removal procedure, click **Finish**.

Remove Enclosure:

Remove an enclosure 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 have completed the enclosure removal process, click **Finish**.

Systems Management for Power Enterprise Pool

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 7.

Note: Depending on the task roles assigned to your user ID, you may not have access to all the tasks. See Table 5 on page 8 for a listing of the tasks and the user roles 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 and domain name of the HMC.

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

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

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

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

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

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

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

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

   You can select **Enable 'routed'** to start the routed daemon, which allows it to run and allows any routing information to be exported from the HMC.
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 is available on the Hardware Management Console (HMC) Version 8, Release 1, or later.

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 under used. 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, do 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 HMC clock and add or remove time servers for the Network Time Protocol (NTP) service.

Use this task in the following situations:
- If the battery is replaced in the HMC.
- If your system is physically moved to a different time zone.

Note: The time setting will adjust automatically for daylight saving time in the time zone you select.

To change the date and time, do the following:

1. In the 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, do the following:

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 onto 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.

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 HMC itself without operator assistance.

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

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

The **Scheduled Operations** task displays the following information for each operation:
- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the **Scheduled Operations** window you can:
- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:
- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operation that can be scheduled for the HMC is:

Backup Critical Console Data
Schedules an operation to back up the critical console hard disk information for the HMC.

To schedule operations on the HMC, do the following:

1. 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 you want to delete, point to **Options** and then click **Delete**.
   - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
   - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range**.
   - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
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 have agreed to for this HMC.

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

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 on any of the license links to view more information.

   Note: This list does not include programs and code 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, do the following:

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 your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
5. Click **OK** and then click **Close** to end the task.

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

Backup Management Console Data

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

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

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

Using the HMC, you can back up all important data, such as the following:
- User-preference files
- User information
- HMC platform-configuration files
- HMC log files
- HMC updates through Install Corrective Service.

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

To back up the HMC critical data, 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 you want to perform.
4. Click **Next**, then follow the appropriate instructions depending on 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.

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, single root I/O virtualization (SRIOV) adapters, Virtual I/O Server, virtual networks, and virtual storage. Many of the system settings that you previously configured by using separate tasks are available in the Deploy System or Partition 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 or partition 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 Templates**
   - **Partition Templates**
   - **OS and VIOS Images**
3. When you have completed 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.

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

OS and 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:

Managing Installation Resources:

Add or remove installation resources for the operating environment for your HMC.

You can use the HMC to deploy a system plan that contains information for installing one or more operating environments on one or more logical partitions. To install an operating environment as part of deploying a system plan, the HMC must be able to access and to use an installation resource for that operating environment.

An installation resource for the operating environment is the necessary set of installation files for a specific version of an operating environment, at a specific release and modification level. The installation resource can be located on the local hard drive for the HMC or it can be located on a Network Installation Management (NIM) server that the HMC can access.

When you define and create a local installation resource, you must meet the following prerequisites:

- You can define only one local installation resource for a specific operating environment version and modification level. For example, you can define a local installation resource for AIX 5.3 and another installation resource for AIX 6.1 but you cannot define two local installation resources for the same AIX version and modification level. This restriction applies to all listed operating environments.
- The HMC must have enough free hard disk space for the necessary set of installation files for the operating environment. The HMC creates the installation resource in the same local hard drive location

that the HMC uses for main store dumps. Consequently, it is recommended that you maintain a certain amount of free hard drive space to avoid potential main store dump problems because main store dumps are necessary to help resolve some types of HMC errors. The typical main store dump averages between 4 gigabytes (GB) to 8 GB, so consider maintaining at least 10 GB of free hard drive space for these dumps when you define and create local installation resources for the HMC.

- You must have the installation media for the operating environment available to copy to the HMC local hard drive. The type of media that you need varies based on the type of operating environment you want to install. You can use CDs or DVDs as the installation image source for Red Hat and SUSE Linux Enterprise Server (SLES) operating environments. However, you can use only DVDs as the installation image source for AIX and Virtual I/O Server operating environments.

When you define a remote NIM server installation resource, you must meet a number of prerequisite conditions to ensure that the HMC can access and use the installation resource:

- The complete set of necessary installation files for the operating environment must exist on the NIM server within a uniquely named NIM resource group.

  Note: You can define a remote resource for AIX and Virtual I/O Server operating environments only.
- You can define multiple remote installation resources for a specific operating environment version and modification level, when each installation resource is located within a different NIM named resource group.
- You must know the fully qualified host name of the NIM server.
- You must know the resource group name that contains the necessary set of operating environment installation files.
- You must set up the HMC to be able to access the NIM server and use the operating environment installation files during system plan deployment. The HMC must be able to run secure shell commands by using a secure shell (SSH) connection to access the NIM server successfully. Consequently, you must ensure that the HMC can provide an appropriate cryptographic key to the NIM server by completing the following steps:
  1. Open an HMC command prompt and run the following command to generate the RSA keys that the HMC needs for ssh connections and to place the keys in an accessible file in the HMC HOME directory: `ssh-keygen -t rsa -f /home/hscroot/ssh_keys`. This command creates two files: **ssh_keys** and **ssh_keys.pub** that contain the needed RSA keys. The **ssh_keys** file contains the private key that the HMC needs for establishing an ssh connection and this file needs to be located in the `/home/hscroot` subdirectory; the **ssh_keys.pub** file contains the public key that the NIM server needs to complete the ssh connection with the HMC.
  2. On the remote NIM server, append or copy the content of the **/home/hscroot/ssh_keys.pub** file into the **/.ssh/authorized_keys** file on the NIM server.

Note: Remote clients defined on the NIM server remain at the same location after installation of the operating environment on a partition for post installation management. The short host name of the system identifies this remote client.

Each installation resource that you define and create for the HMC is available for selection in the **Customize Operating Environment Install** step of the Deploy System Plan wizard. If the installation resource that you want to use for a selected partition is not available when you perform this step, you can click **New Install Resource** to open the Manage Install Resources window to define and create a new installation resource.

To open the **Managing Install Resources** task, 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, select the **OS and VIOS Images** tab, and then click **Managing Install Resources**.
3. From the **Managing Install Resources** window, choose appropriate task from the available options.
4. Click **OK** to proceed with the task. Otherwise click **Cancel** to exit the task.

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.

To manage or to import the VIOS image repository, 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, 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**.

   Note: The VIOS images are named **resource1** and **resource2**.
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 the VIOS images from a DVD to the HMC, complete the following steps:
     a. In the Import Virtual I/O Server Image window, select **Management console DVD**.
     b. In the **Name** field, enter the VIOS image name that you want to import from the DVD.
     c. Click **OK**.
   - To import the VIOS images from a Network File System (NFS), File Transfer Protocol (FTP), or Secure Shell File Transfer Protocol (SFTP), complete the following steps:
     a. In the Import Virtual I/O Server Image window, select **File System**.
     b. Select **Remote NFS Server**, **Remote FTP Server**, or **Remote SFTP Server**.
     c. Enter the required details and click **OK**.

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 7 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 used for logging onto the HMC. A password verifies your user ID and your authority to log in to the console.

To change your password:

1. 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 you want to use, and respecify the new password to confirm in the fields provided.
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 72. For more information about LDAP authentication, see "Manage LDAP" on page 72.

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 7 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 7 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 log on 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 has been reached to re-enter their password. If a password is not re-entered 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 re-enter their password when prompted, if a value was specified in the **Session timeout minutes** field. If the password is not re-entered 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 reaching the maximum number of days of inactivity.
- **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.

The predefined managed resource roles include:
- All System Resources

Note: If you add a customized resource role that includes access to all partitions, you must add the **View managed systems** and **View partitions** tasks to the task role to get access to the views.

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.

Note:

The self-signed certificates on the HMC use 2048-bit RSA encryption. If you are using Certificate Authority (CA) signed certificates, you must use 2048-bit encryption. You can create a new 2048-bit certificate that is signed by the CA by completing the following steps and selecting signed by a CA.

To manage your certificates, 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 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**.
   - 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 will be imported from removable media on the console or from the file system on the system 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.

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.

To configure your HMC so that it uses LDAP authentication, complete the following steps:

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**.

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 do the following:

- View existing KDC servers
- Modify existing KDC server parameters including realm, ticket lifetime, and clock skew
- Add and configure a KDC server on the HMC
- Remove a KDC server
- Import a service key
- Remove a service key

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

Under Kerberos, a client (generally either a user or a service) sends a request for a ticket to the KDC. The KDC creates a ticket-granting ticket (TGT) for the client, encrypts it using the client's password as the

key, and sends the encrypted TGT back to the client. The client then attempts to decrypt the TGT, using its password. If the client successfully decrypts the TGT (i.e., if the client gave the correct password), it keeps the decrypted TGT, which indicates proof of the client's identity.

The tickets have a time availability period. Kerberos requires the clocks of the involved hosts to be synchronized. If the HMC clock is not synchronized with the clock of KDC server, authentication will fail.

A Kerberos realm is an administrative domain, site, or logical network that uses Kerberos remote authentication. Each realm uses a master Kerberos database that is stored on a KDC server and that contains information about the users and services for that realm. A realm might also have one or more slave KDC servers, which store read-only copies of the master Kerberos database for that realm.

To prevent KDC spoofing, the HMC can be configured to use a service key to authenticate to the KDC. Service key files are also known as keytabs. Kerberos verifies the TGT requested was issued by the same KDC that issued the service key file for the HMC. Before you can import a service key file into an HMC, you must generate a service key for the host principal of the HMC client.

Note: For MIT Kerberos V5 *nix distributions, create a service key file by running the `kadmin` utility on a KDC and using the `ktadd` command. Other Kerberos implementations may require a different process to create a service key.

You can import a service key file from one of these sources:

- Removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices. You must use this option locally at the HMC (not remotely), and you must mount the removable media to the HMC before using this option.
- A remote site using secure FTP. You can import a service-key file from any remote site that has SSH installed and running.

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

- You must enable the Network Time Protocol (NTP) service on the HMC and set the HMC and the KDC servers to synchronize time with the same NTP server. You can enable the NTP service on the HMC by accessing the “Change Date and Time” on page 56 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 will always use Kerberos remote authentication, even when the user logs onto the HMC locally.

  Note: You do not need to set all users to use Kerberos remote authentication. You can set some user profiles so that the users can use local authentication only.
- Use of a service key file is optional. Before using a service key file, you must import it into the HMC. If a service key is installed on the HMC, realm names must be equivalent to the network domain name. The following is an example of creating the service key file on a Kerberos server using the kadmin.local command assuming the HMC hostname is hmc1, the DNS domain is example.com, and the Kerberos realm name is EXAMPLE.COM:

  – `# kadmin_local kadmin.local:  ktadd -k /etc/krb5.keytab host/hmc1.example.com@EXAMPLE.COM`

  Using the Kerberos ktutil on the Kerberos server, verify the service key file contents. The output should look like the following:

  –
  ```
  # ktutil
  ktutil:  rkt /etc/krb5.keytab
  ktutil: l
  ```

```
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
 1    9      host/hmc1.example.com@EXAMPLE.COM
 2    9      host/hmc1.example.com@EXAMPLE.COM
```

- The HMC Kerberos configuration can be modified for SSH (Secure Shell) login without a password using GSSAPI. For remote login without a password through Kerberos to an HMC, configure the HMC to use a service key. Once the configuration is completed use `kinit -f` *principal* to obtain forwardable credentials on a remote Kerberos client machine. Then issue the following command to log in to the HMC without having to enter a password: `$ ssh -o PreferredAuthentications=gssapi-with-mic` *user@host*

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** drop down list.
4. When you have completed 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.

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 7 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

This task allows you 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 perform 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 Remote Connections

Learn how to manage remote connections on your Hardware Management Console (HMC).

Note: The HMC's call-home server service must be enabled for you to use this task.

The HMC manages remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, this task allows you to manage the queue manually, if necessary. You can stop transmissions, move priority requests ahead of others, or delete requests.

To manage remote connections, do the following:

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Remote Connections**.
3. From the **Manage Remote Connections** window, a list of transmitting requests being and a list of waiting requests transmitted are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
   - Prioritize a selected request (move it to the top of the queue)
   - Cancel selected requests
   - Cancel all active requests (those being transmitted)
   - Cancel all waiting requests
   - Hold the queue (puts queue on hold after completing current active request)
   - Release the queue
   - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

Manage Remote Support Requests

Learn how to view or manage call-home requests that the Hardware Management Console (HMC) has submitted.

1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Manage Remote Support Requests**.
3. From the **Manage Remote Support Requests** window, a list of active requests and a list of waiting requests are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
   - View all call-home servers
   - Cancel selected requests
   - Cancel all active requests
   - Cancel all waiting requests
   - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

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 have completed 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, do the following:

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 your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
5. Click **OK** and then click **Close** to end the task.

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

Electronic Service Agent Setup Wizard

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

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

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, do the following:

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, *https://www.ibm.com/account/profile*.
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 61.

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 61.

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, do the following:

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:
   - 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 on managing the inbound connectivity.

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 61.

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 Serviceable Event Notification

This task adds email addresses that notify you when problem events occur on your system and configures how you want to receive notification of system events from the Electronic Service Agent.

To set up notification, 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 Serviceable Event Notification**.
3. From the **Manage Serviceable Event Notification** window, you can do the following:
   - Use the **Email** tab to add the email addresses that will be notified when problem events occur on your system.
   - Use the **SNMP Trap Configuration** tab to specify locations for sending Simple Network Management Protocol (SNMP) trap messages for Hardware Management Console application program interface events.
4. Click **OK** when you have completed this task.

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

Manage Connection Monitoring

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 connected to a local HMC, consider the scope of control that you need. A remote HMC defines a specific set of managed objects that are directly controlled by the remote HMC, while a Web browser to a local HMC has control over the same set of

managed objects as the local HMC. The communications connectivity and communications speed is an additional consideration; LAN connectivity provides acceptable communications for either a remote HMC or Web browser control.

Using a remote HMC

A remote HMC gives the most complete set of functions because it is a complete HMC; only the process of configuring the managed objects is different from a local HMC.

As a complete HMC, a remote HMC has the same setup and maintenance requirements as a local Hardware Management Console. A remote HMC needs LAN TCP/IP connectivity to each managed object (service processor) that is to be managed; therefore, any customer firewall that may exist between the remote HMC and its managed objects must permit HMC to service processor communications to occur. A remote HMC may also need communication with another HMC for service and support. Table 10 shows the ports 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), or a dialed connection through a customer-provided switched telephone connection that uses the supplied modem (see “Manage Outbound Connectivity” on page 83). A remote HMC cannot use the supplied modem for communication with a local HMC or a service processor.

Performance and the availability of the status information and access to the control functions of the service processor depends on the reliability, availability, and responsiveness of the customer network that interconnects the remote HMC with the managed object. A remote HMC monitors the connection to each service processor and attempts to recover any lost connections and can report those connections that cannot be recovered.

Security for a remote HMC is provided by the HMC user-login procedures in the same way as a local HMC. As with a local HMC, all communication between a remote HMC and each service processor is encrypted. Certificates for secure communications are provided, and can be changed by the user if desired.

TCP/IP access to the remote HMC is controlled through its internally managed firewall and is limited to HMC related functions.

Using a web browser

If you need occasional monitoring and control of managed objects connected to a single local 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 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 browser access to web server communication

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

Port	Use
TCP 8443	Secure browser access to web server communication
TCP 9960	Browser applet communication
TCP 12443[1]	Remote web browser 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 has been configured to allow web browser access, a web browser gives an enabled user access to all the configured functions of a local HMC, except those functions that require physical access to the HMC, such as those that use the local diskette or DVD media. The user interface presented to the remote web browser user is the same as that of the local HMC and is subject to the same constraints as the local HMC.

The web browser can be connected to the local HMC using a LAN TCP/IP connection and using only encrypted (HTTPS) protocols. Logon security for a web browser is provided by the HMC user-login procedures. Certificates for secure communications are provided, and can be changed by the user.

Performance and the availability of the status information and access to the control functions of the managed objects depends on the reliability, availability, and responsiveness of the network that interconnects the web browser with the local HMC. Because there is no direct connection between the web browser and the individual managed objects, the web browser does not monitor the connection to each service processor, does not do any recovery, and does not report any lost connections. These functions are handled by the local HMC

The web browser system does not require connectivity to IBM for service or support. Maintenance of the browser and system level is the responsibility of the customer.

If the URL of the HMC is specified using the format https://*xxx.xxx.xxx.xxx* (where *xxx.xxx.xxx.xxx* is the IP address) and Microsoft Internet Explorer is used as the browser, a hostname mismatch message is displayed. To avoid this message, a Firefox browser is used or a hostname is configured for the HMC, using the **Change Network Settings** task (see "Change Network Settings" on page 55), and this hostname is specified in the URL instead of an IP address. For example, you can use the format https://*hostname.domain_name* or https://*hostname* (for example, using https://hmc1.ibm.com or https://hmc1).

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, know the TCP/IP address of the HMC to be controlled, and have correctly set up any firewall access between the HMC and the web browser.
- Have a valid user ID and password assigned by the access administrator for HMC web access.

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 have to administer several managed systems, you can achieve consistent results by using the command line interface. The command sequence can be stored in scripts and run remotely.
- When automated operations are required. After you have developed a consistent way to manage the managed systems, you can automate the operations by invoking the scripts from batch-processing applications, such as the **cron** daemon, from other systems.

On a local HMC, you can use the command line interface in a terminal window.

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 machine room where managed systems are located, so you might not have physical access to the HMC. In this case, you can remotely access it using either a remote Web browser or the remote command line interface.

Note: To enable scripts to run unattended between an **SSH** client and an HMC, the SSH protocol must already be installed on the client's operating system.

To enable scripts to run unattended between an **SSH** client and an HMC, do the following:

1. Enable remote command execution. For more information, see "Enable Remote Command Execution" on page 76
2. On the client's operating system, run the SSH protocol key generator. To run the SSH protocol key generator, do the following:
   a. To store the keys, create a directory named $HOME/.ssh (either RSA or DSA keys can be used).
   b. To generate public and private keys, run the following command:
      ```
      ssh-keygen -t rsa
      ```
      The following files are created in the $HOME/.ssh directory:
      ```
      private key: id_rsa
      public key: id_rsa.pub
      ```
      The write bits for both group and other are turned off. Ensure that the private key has a permission of 600.
3. On the client's operating system, use ssh and run the **mkauthkeys** command to update the HMC user's authorized_keys2 file on the HMC by using the following command:
   ```
   ssh hmcuser@hmchostname "mkauthkeys ––add '<the contents of $HOME/ .ssh/id_rsa.pub>' " "
   ```

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

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

To enable password prompting for all hosts that access the HMC through **ssh**, use the **scp** command to copy the key file from the HMC: `scp hmcuser@hmchostname:.ssh/authorized_keys2 authorized_keys2`

Edit the authorized_keys2 file and remove all lines in this file. Then copy it back to the HMC: `scp authorized_keys2 hmcuser@hmchostname:.ssh/authorized_keys2`

Enabling and disabling HMC remote commands

You can enable or disable the remote command line interface access to the 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:
   - 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 PC has LAN connectivity to the desired HMC.
2. From your web browser, enter the URL of the desired HMC, using the format ***https://hostname.domain_name*** (for example: https://hmc1.ibm.com) or ***https://xxx.xxx.xxx.xxx***.

   If this is the first access of the HMC for the current web browser session, you can receive a certificate error. This certificate error is displayed if:

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

   In either case, if you know that the certificate being displayed to the browser is the one used by the HMC, you can continue and all communications to the HMC will be encrypted.

   If you do not want to receive notification of a certificate error for the first access of any browser session, you can configure the browser to trust the HMC or the CA. In general, to configure the browser, use one of the following methods:

   - You must indicate that the browser will permanently trust the issuer of the certificate
   - By viewing the certificate and installing, to the database of trusted CAs, the certificate of the CA that issued the certificate used by the HMC.

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

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 the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

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 8 Release 8.7.0 Maintenance Level 0.

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 at www.ibm.com/legal/copytrade.shtml.

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

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

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

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.

Printed in USA