Power Systems

Managing the Hardware Management Console by using HMC Version 10.2.1030, or later

Note

Before using this information and the product it supports, read the information in "Notices" on page 163.

This edition applies to IBM Hardware Management Console Version 10 Release 3 Maintenance Level 1061 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Managing the HMC by using HMC Version 10.2.1030, or later..... 1
What's new in Managing the HMC by using HMC version 10.2.1030 or later..... 1
Introduction to the HMC..... 2
Logging on to the Hardware Management Console (HMC) when PowerSC MFA is configured on the HMC..... 3
Predefined user IDs and passwords..... 3
Using the web-based user interface..... 4
Overview of menu options..... 5
Tasks and roles..... 6
HMC tasks, user roles, IDs, and associated commands..... 7
Session handling..... 26
Version mismatch state for a managed system..... 27
Systems management for servers..... 28
System content pane..... 28
Add system..... 29
System templates..... 30
Connections and operations..... 31
Firmware..... 41
Service..... 43
System details view..... 48
Serviceability..... 61
Systems Management for Partitions..... 62
Partition content pane..... 62
Partition properties..... 63
Processors..... 64
Memory..... 64
Physical I/O adapters..... 65
Operations..... 65
Console..... 74
Mobility..... 75
Profiles for HMC Version 10.3.1060.0, or later..... 76
Profiles for HMC Version 10.3.1050.0, or earlier..... 77
Delete Partition..... 77
Serviceability..... 78
Virtual I/O..... 79
Tags..... 82
Power enterprise pools..... 82
Templates and OS Images..... 83
System Templates..... 83
Partition Templates..... 84
VIOS Images..... 84
All System Plans..... 88
HMC management tasks..... 89
HMC settings..... 89
Network Settings (for HMC Version 10.3.1061.0, or later)..... 90
Network Settings (for HMC versions between 10.2.1030.0 and 10.3.1060.0)..... 91
Network diagnostic information..... 92
Network topology..... 93
Data replication..... 93
Licenses..... 94
HMC certificates..... 94

Certificate revocation list 96
Update HMC 96
Upgrade HMC 97
Shut down or Restart 98
Backup HMC data 98
Restore HMC data 99
Save HMC upgrade data 100
Restore HMC upgrade data 100
Schedule operations 101
Format media 102
Launch guided setup wizard 102
Cloud Connector 103
Schedule management for HMC Version 10.3.1061.0, or later 104
Performance dashboard 106
Environmental dashboard 107
Call home management for HMC Version 10.3.1060.0, or later 109
Customer information 109
Outbound connectivity 109
Service user authorization 110
Event notification 110
Electronic service agent 110
Connection monitoring 111
Call home management for HMC Version 10.3.1050.0, or earlier 111
Setup electronic service agent 111
Service user authorization 111
Electronic service agent 112
Outbound connectivity 112
Customer information 113
Event notification 113
Connection monitoring 113
Service management tasks for HMC Version 10.3.1061.0, or later 114
Dumps 114
FTP connection 115
Schedule service data 116
Remote support connection 116
Serviceable events 119
Events manager for call home 120
Service actions 120
VIOS images for HMC Version 10.3.1061.0, or later 122
Manage Virtual I/O Server images 122
Manage Virtual I/O Server backup 123
Manage Virtual I/O Server updates 125
User management tasks for HMC Version 10.3.1060.0, or later 126
Active users 126
Running tasks 126
User profiles 127
Resource roles 129
Task roles 130
LDAP 131
KDC 132
MFA 134
User management tasks for HMC Version 10.3.1050.0, or earlier 135
Users and tasks 135
User profiles and access 135
Tasks and resource roles 138
LDAP 138
KDC 139
MFA 142

Enable Remote Command Execution....143
Enable Remote Operation....143
Enable Remote Virtual Terminal....143
Logs....144
Tasks log....144
Console events log....144
Serviceability tasks for HMC versions between 10.2.1030.0 and 10.3.1060.0....144
Serviceable events....145
Events manager for call home....145
Create serviceable event....145
Dumps....146
Transmit service information....147
Remote support connection....148
Remote operations....151
Using a remote HMC....151
Using a web browser....152
Using the HMC remote command line....154
Logging in to the HMC from a LAN-connected web browser....155
Managing OpenBMC-based and BMC-based systems by using the HMC....156
Add Managed Systems....156
Systems Management for Servers....157

Notices....163
Accessibility features for IBM Power servers....164
Privacy policy considerations....165
Programming interface information....166
Trademarks....166
Terms and conditions....166

Managing the HMC by using HMC Version 10.2.1030, or later

Learn how to use the Hardware Management Console (HMC) by using HMC Version 10.2.1030, or later.

About this task

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

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

What's new in Managing the HMC by using HMC version 10.2.1030 or later

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

December 2024

- Added the topic "Backup profile data" on page 52 with information about the latest GUI page for managing backup, delete, and restore operations for the partition data of a managed system.
- Added the topic "Network Settings (for HMC Version 10.3.1061.0, or later)" on page 90 with information about the latest GUI pages for Network settings.
- Added the topic "Schedule management for HMC Version 10.3.1061.0, or later" on page 104 with information about the latest GUI pages for schedule management tasks.
- Added the topic "Service management tasks for HMC Version 10.3.1061.0, or later" on page 114 with information about the latest GUI pages for service management tasks.
- Added the topic "VIOS images for HMC Version 10.3.1061.0, or later" on page 122 with information about the latest GUI pages for VIOS images.
- Updated the topic "Update system firmware" on page 41 with information about the Resume operation.
- Updated the topic "System settings" on page 48 with information about the NPIV validation policy.
- Updated the topics "Delete Partition" on page 77, "Restart partition " on page 68, and "Shutdown partition" on page 69 with information about the latest GUI pages for partition management functions.
- Updated the topics "Licenses" on page 94 and "Format media" on page 102 with information about the latest GUI pages for viewing licenses and formatting the media.
- Updated the topic "HMC certificates" on page 94 with information about the latest GUI page for managing the HMC certificates.
- Updated the topic "Predefined user IDs and passwords" on page 3 with information about the root user ID and password used by the service provider to perform maintenance procedures.

June 2024

- Added the topic "Capacity on Demand for HMC Version 10.3.1060.0, or later" on page 53 with information about the latest GUI pages for Capacity on Demand (CoD) functions.
- Added the topic "Profiles for HMC Version 10.3.1060.0, or later" on page 76 with information about the latest graphical user interface (GUI) page for managing partition profiles.

- Added the topic "Restore HMC upgrade data" on page 100 with information about the new function to restore the HMC upgrade data.
- Added the topic "Call home management for HMC Version 10.3.1060.0, or later" on page 109 with information about the latest GUI pages for Call home management functions.
- Added the topic "User management tasks for HMC Version 10.3.1060.0, or later" on page 126 with information about the latest GUI pages for User management functions.
- Updated the topics "Add system" on page 29, "Reset or remove system connection" on page 35, "Disconnect another management console" on page 35, "Power on system" on page 32,"Rebuild system" on page 33, "Change system password" on page 35 with information about the latest GUI updates for system management functions.
- Updated the topic "Manage system profiles" on page 37 with information about the latest GUI page for managing the system profiles.
- Updated the topic "HMC settings" on page 89 with information about **Maximum webui sessions per user** and **Console maximum webui session**.
- Updated the topics "Upgrade HMC" on page 97, "Save HMC upgrade data" on page 100,"Restore HMC data" on page 99, "Backup HMC data" on page 98 with information about the latest GUI pages for **HMC management** tasks.

November 2023

- Added the topic "Manage identify LED states" on page 46 with information about attention LED and light specific-LEDs.
- Added the topic "Validate and Migrate" on page 75 with information about the new **Validate and Migrate** function.
- Added the topic Upgrade VIOS with information about the new **Upgrade VIOS** function.
- Added the topic "Performance dashboard" on page 106 with information about the new **Performance dashboard**.
- Updated the topic "VMI configuration for eBMC-based managed systems" on page 39 with information about IPv6 support.
- Updated the topic "Partition properties" on page 63.
- Updated the topic Update HMC with information about the new **Update HMC** function.
- Updated the topic "Dumps" on page 146.

Introduction to the HMC

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

You can configure and manage servers on the HMC. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To ensure consistent function, each HMC is shipped preinstalled with the HMC Licensed Machine Code Version 9, Release 1.

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

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

Physical proximity
Before HMC Version 7, at least one local HMC was required to be physically located near the managed systems. As an alternative to the local HMC, you can use a supported device, such as a personal computer that has connectivity and authority to operate through a remotely attached HMC. The

local device must be in the same room as your server and at a distance of 8 m (26 ft) from your server. The local device must have the functional capability that is equivalent to the HMC that it replaces and that is needed by the service representative to service the system. For a virtual HMC, the functional capabilities also include the method of transferring service data, such as firmware updates or diagnostic data, and transferring the log information to and from the HMC.

Redundant or Dual HMCs

A server might be managed by either 1 or 2 Hardware Management Consoles. When two Hardware Management Consoles manage one system, they are peers, and each HMC can be used to control the managed system. The best practice is to attach one HMC to the supported networks or HMC ports of the managed systems. The networks are intended to be independent. Each HMC might be the DCHP server for a service network. Because the networks are independent, the DHCP servers must be set up to provide IP addresses on two unique and nonroutable IP ranges.

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

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

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

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

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

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

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

Notes:

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

Predefined user IDs and passwords

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

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

1. Enter the **Current Password** and the **New Password**.
2. Re-enter the new password in the **Confirmation new password** field.

3. Click **OK**. If the new password complies with the current password policy, the password for the HMC is changed.

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

Table 1. Predefined HMC user IDs and passwords

User ID	Password	Purpose
`hscroot`	`abc123`	The `hscroot` user ID and password are used to log in to the HMC for the first time. They are case-sensitive and can be used only by a member of the super administrator role.
`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, and the menu pod.

With HMC Version 10.2.1040, or later, you can view the HMC dashboard after you log in to the HMC. The dashboard includes the following details:

- **Resource summary**: Displays details about the systems, partitions, and VIOS resources that are available in the HMC, along with the navigation links to systems, partitions, and VIOS resources.
- **HMC details**: Displays details such as the name of the HMC, the level and version of the HMC, the date of the last update, the date of the last reboot, the device type, and the serial number of the HMC.
- **Quick links**: Displays a snapshot of the number of serviceable events, active web users, power enterprise pools, and shared storage pool clusters. Provides navigation links to access Serviceable events, Active web users, Power enterprise pools, and Shared storage pool clusters.
- **Processor and memory summary across all systems**: Displays a snapshot of processor and memory details of the HMC.
- Quick access links to **Refresh** and **HMC settings** pages are also available.

The *title bar*, across the top of the workplace window, identifies the product, search bar, feedback option, help options, notifications, tasks, serviceable events, and information about any user who have logged in to the HMC.

- You can click on the **User** icon to perform the following tasks:
  - **Log out**: Log out of the HMC
  - **Switch to old dashboard**: View the older version of the dashboard.
  - **Change password**: Change your existing password that is used for logging on to the Hardware Management Console (HMC). A password verifies your user ID and your authority to log in to the console.
  - **Request enhancements**: Launches **IBM Power Ideas Portal** where you can request enhancements.
  - **Get started using the app**: Launches the **Getting started** window.
  - **About HMCv10**: Displays the HMC version, name, release, service pack, build level, driver information, machine type, serial number, and model information.

The *navigation area*, in the left portion of the window, contains the primary navigation links for selecting tasks for your System resources, HMC management, User management, Logs, Serviceability, and Call home.

Note: With HMC Version 10.2.1040, or later, you can access the navigation menu options by typing the keywords in the search bar that is available at the top of the *navigation area*.

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

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

You can also select which columns to display by clicking the **Customize columns** icon that is located in the table menu bar. You can refresh the table by clicking the **Refresh** icon. You can export the data of the table by clicking the **Export** icon available in the table menu bar.

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

Overview of menu options

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

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

Table 2. HMC menu options

Menu	Submenu	Options/Tasks
System resources	Partitions	View all partitions
	Virtual I/O Servers	View all Virtual I/O Servers
	Tags	View all tags
	Shared storage pool clusters	View all shared storage pool clusters
	Power enterprise pools	View all power enterprise pools
	System plans	View system plans
	Templates and OS images	View templates and OS images
HMC Management		HMC settings
		Network Settings
		Network diagnostic information
		Network topology
		Data replication
		Licenses
		HMC certificates
		System certificates
		Certificate revocation list

Table 2. HMC menu options (continued)		
Menu	**Submenu**	**Options/Tasks**
User management	Users and tasks	Users and Tasks window
	User profiles and access	User Profiles window
	Tasks and resource roles	Customize User Controls window
	LDAP	LDAP Server Definition window
	KDC	Manage KDC servers
	MFA	Multi Factor Authentication window
Logs	Tasks log	View tasks log window
	Console events log	View console events window
Serviceability	Serviceable events	Serviceable Events Manager window
	Events manager for call home	Events manager for call home window
	Create serviceable events	Create serviceable events window
	Dumps	Manage dumps
	Transmit service information	Transmit service information window
Call home	Setup electronic service agent	Setup electronic service agent window
	Service user authorization	Service user authorization window
	Outbound connectivity	Manage outbound connectivity
	Remote support connection	Manage remote support connection
	Customer information	Manage customer information
	Event notification	Manage serviceable event notification
	Connection monitoring	Manage connection monitoring

Tasks and roles

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

The roles that are discussed refer to HMC users; operating systems that are running on logical partitions have their own set of users and roles. When you create an HMC user, you must assign that user a task role. Each task role allows the user different levels of access to tasks available on the HMC interface. For more information about the tasks each HMC user role can perform, see “HMC tasks, user roles, IDs, and associated commands” on page 7.

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

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

Table 3. Predefined HMC Roles

Role	Description	HMC User ID
Operator	The operator is responsible for daily system operation.	**hmcoperator**
Super administrator	The super administrator acts as the root user, or manager, of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.	**hmcsuperadmin**
Product engineer	A product engineer helps support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.	
Service representative	A service representative is an employee who is at your location to install, configure, or repair the system.	**hmcservicerep**
Viewer	A viewer can view HMC information, but cannot change any configuration information.	**hmcviewer**
Client live update	The client live update role is intended for use when you are using the AIX® Live Update capability on a partition of a managed system. A client live update user has authority that is limited to what is necessary to complete a live update on AIX.	**hmcclientliveupdate**

You can create **customized** HMC roles by modifying predefined HMC roles. Creating customized HMC roles is useful for restricting or granting specific task privileges to a certain user.

HMC tasks, user roles, IDs, and associated commands

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

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

Some tasks have an associated command. For more information about accessing the HMC command line, see “Using the HMC remote command line” on page 154.

Some tasks can only be performed using the command line. For a listing of those tasks, see Table 9 on page 24.

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

Table 4. HMC task groupings

HMC tasks and the corresponding user roles, IDs, and commands	**Associated table**
HMC Management	Table 5 on page 8
Service Management	Table 6 on page 11
Systems Management	Table 7 on page 13
Control Panel Functions	Table 8 on page 23

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 HMC data” on page 98 bkconsdata	X	X		X
Backup Profile Data bkprofdata	X	X		X
Change BMC Certificates chbmccert	X	X		X
Certificate Management chhmccert lshmccert mkhmccert		X		
Date and time chhmc lshmc	X	X		X
Language and locale 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)**
Change HMC Configuration chipsec chpsm chusrtca	X	X		X
"Network Settings (for HMC versions between 10.2.1030.0 and 10.3.1060.0)" on page 91 chhmc lshmc	X	X		X
Change Proxy Configuration chproxy		X		X
Change user password chhmcusr	X	X	X	X
List BMC Certificates lsbmccert	X	X	X	X
List HMC Configuration lsipsec lspsm lsusrtca	X	X	X	X
List HMC Encryption Task lshmcencr	X	X	X	
List System Plan lssysplan		X		
List Proxy Configuration lsproxy	X	X	X	X
"KDC" on page 139 chhmc lshmc getfile rmfile		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)
"LDAP" on page 138 lshmcldap chhmcldap		X		
"Launch guided setup wizard" on page 102		X		
Launch Remote Hardware Management Console	X	X	X	X
Lock HMC Screen	X	X	X	X
Logoff or Disconnect	X	X	X	X
"HMC certificates" on page 94		X		
"Data replication" on page 93	X	X		
"Tasks and resource roles" on page 138 chaccfg lsaccfg mkaccfg rmaccfg		X		
"User profiles and access" on page 135 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		
"Users and tasks" on page 135 lslogon termtask	X	X	X	X
Open 5250 Console	X	X		X
"Enable Remote Command Execution" on page 143 chhmc lshmc	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 Operation" on page 143 chhmc lshmc	X	X	X	X
"Enable Remote Virtual Terminal" on page 143	X	X		X
"Restore HMC data" on page 99	X	X		X
"Save HMC upgrade data" on page 100 saveupgdata	X	X		X
"Schedule operations" on page 101	X	X		
"Shut down or Restart" on page 98 hmcshutdown	X	X		X
"Manage serviceable events" on page 43 lssvcevents	X	X		X
"Licenses" on page 94	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 44		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)**
"Serviceable events" on page 145 chsvcevent cpfile lssvcevents mksvcevent updpmh		X		X
"Format media" on page 102 formatmedia	X	X		X
"Dumps" on page 146 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Transmit service information" on page 147 chsacfg lssacfg	X	X		
"Electronic service agent" on page 112	X	X		X
"Outbound connectivity" on page 112	X	X		X
"Customer information" on page 113	X	X		X
"Service user authorization" on page 111		X		
"Event notification" on page 113 chsacfg lssacfg	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)**
“Connection monitoring” on page 113	X	X	X	X
“Setup electronic service agent” on page 111		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)**
“System settings” on page 48 lshwres	X	X	X	X
lsled	X	X	X	X
lslparmigr	X	X	X	X
lssyscfg	X	X	X	X
chhwres	X	X	X	X
chsyscfg	X	X	X	X
migrlpar	X	X	X	X
optmem	X	X		X
lsmemopt	X	X	X	X
lsrrstartlpar	X	X		
Update Password chsyspwd		X		
Change Default User Interface Settings	X	X	X	X
List CEC Property lscomgmt lsiotopo	X	X	X	X

Table 7. Systems Management tasks, commands, and default user roles (continued)				
HMC Interface Tasks and Associated Commands	**User roles/IDs**			
	Operator (hmcoperator)	**Super Administrator (hmcsuperadmin)**	**Viewer (hmcviewer)**	**Service Representative (hmcservicerep)**
List Utilization Data lslparutil	X	X	X	X
Operations				
"Power off system" on page 31 chsysstate	X	X		X
"Activate partition" on page 66 chsysstate	X	X		X
"Save Current Configuration" on page 77 chsysstate	X	X		X
"Restart partition " on page 68 chsysstate	X	X		X
"Shutdown partition" on page 69 chsysstate	X	X		X
chlparstate	X	X		X
LED Status: Deactivate Attention LED "Manage identify LED states" on page 46 chled	X	X		
LED Status: Identify LED "Manage identify LED states" on page 46	X	X	X	X
LED Status: Test LED "Manage identify LED states" on page 46	X	X	X	X
"Schedule operations for HMC Version 10.3.1060.0, or earlier" on page 33	X	X		
"Launch advanced system management (ASMI)" on page 36 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 system" on page 33 chsysstate	X	X		
"Power management" on page 37 chpwrmgmt lspwrmgmt		X		
"Delete partition" on page 71 rmsyscfg	X	X		X
"Mobility" on page 75 lslparmigr migrlpar	X	X		X
"Manage profiles" on page 77 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
Manage System Plan cpsysplan rmsysplan		X		
Make System Plan mksysplan		X		
Deploy System Plan deploysysplan		X		
Change N_Port Login chnportlogin	X	X		X
RR Start LPAR lsrrstartlpar rrstartlpar	X	X		

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)**
Migrate LPAR migrdbg refdev	X	X		
Make Profile Data mkprofdata	X	X		
Restore Profile Data migrcfg	X	X		
Remove Profile Data rmprofdata	X	X		
Manage Pmem CEC Config: Initialize Profile Data: Restore Profile Data rstprofdata For option "--retainpmemvolume" (access only for hmcsuperadmin)	X	X		
Vios Admin Op: Virtual IO Server Command viosvrcmd For option "--admin" (access only for hmcsuperadmin and hmcoperator)	X	X		X
“Connections and operations” on page 31	X	X	X	X
Configuration				
“Create partition from template” on page 31		X		
“Deploy system from template” on page 31		X		
“Capture configuration as template” on page 38		X		
Change CEC Property chprimhmc	X	X		
Change Trusted System Key chtskey		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)**
"Create partition" on page 30		X		
List LPAR Property lsmigrdbg	X	X	X	X
Hibernate LPAR lsrsdevsize	X	X		
List N_Port Login lsnportlogin	X	X		X
LS Profile Space lsprofspace	X	X	X	X
List Trusted System Key lstskey	X	X	X	X
"Manage profiles" on page 77 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg	X	X	X	X
Manage License Keys chlickey	X	X		
Manage Utilization Data chlparutil	X	X		X
Save Current Configuration "Save Current Configuration" on page 77 mksyscfg	X	X		
ViewSPP lsmemdev	X	X	X	X
Connections				

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)**
"Service processor status" on page 36 lssysconn	X	X	X	X
"Reset or remove system connection" on page 35 rmsysconn	X	X		
Add Connection mksysconn	X	X		
Open V Term mkvterm	X	X		X
Close V Term rmvterm	X	X		X
"Disconnect another management console" on page 35		X		
Hardware (Information)				
"Hardware Operations" on page 62	X	X	X	X
Updates				
"Check readiness" on page 41 updlic		X		X
"View current system firmware levels" on page 41 lslic		X		X
Update HMC updhmc lshmc		X		X
Serviceability				
"Manage serviceable events" on page 78 chsvcevent lssvcevents		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)**
Change SNMP Alerts chspsnmp	X	X		X
"Create serviceable event" on page 44		X		X
"Reference code log" on page 79 lsrefcode	X	X	X	X
"Control Panel Functions" on page 79 lssyscfg	X	X		
"Add FRU" on page 44		X		X
"Add enclosure" on page 46		X		X
"Exchange FRU" on page 45		X		X
"Remove FRU" on page 45		X		X
"Remove enclosure" on page 46		X		X
"Power on/off IO unit" on page 46		X		X
"Dumps" on page 146 dump cpdump getdump lsdump startdump lsfru	X	X		X
"Collect VPD" on page 47	X	X	X	X
"Type, Model, Feature" on page 61		X		
"Setup FSP failover" on page 36 chsyscfg lssyscfg		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)**
"Initiate FSP failover" on page 36 chsysstate		X		
List CEC Property lsprimhmc	X	X	X	X
Capacity on Demand (CoD)				
Enter CoD code chcod		X		
View History Log lscod	X	X	X	X
Change CEC Property chcomgmt	X	X		
CoD Pool Management: Change CoD chcodpool	X	X		
Change CoD mkcodpool		X		
Change VET Code chvet		X		
List CoD Information lscodpool	X	X	X	X
List VET Information lsvet	X	X	X	X
Processor: View Capacity Settings lscod	X	X	X	X
Processor CUoD: View Code Information lscod	X	X	X	X
Processor: On/Off CoD: Manage chcod		X		

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

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)**
PowerVM: View Code Information lscod	X	X	X	X
Enterprise Enablement: Enter Activation Code chcod		X		
Enterprise Enablement: View History Log lscod	X	X	X	X
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				
(21) Activate Dedicated Service Tools chsysstate	X	X		
(65) Disable Remote Service chsysstate	X	X		
(66) Enable Remote Service chsysstate	X	X		
(67) DIsk Unit IOP Reset / Reload chsysstate	X	X		
(68) Concurrent Maintenance Power Off Domain	X	X		
(69) Concurrent Maintenance Power On Domain	X	X		
(70) IOP Control Storage Dump chsysstate	X	X		
(71) Product Engineering Debug Tools pedbg				
(72) PE Shell Access pesh	X	X	X	X

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

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

Command line tasks	User roles/IDs			
	Operator (hmcoperator)	**Super Administrator (hmcsuperadmin)**	**Viewer (hmcviewer)**	**Service Representative (hmcservicerep)**
Change which encryption is used by the HMC to encrypt the passwords of locally authenticated HMC users, or change which encryptions can be used by the HMC Web UI. chhmcencr		X		
List which encryption is used by the HMC to encrypt the passwords of locally authenticated HMC users, or list which encryptions can be used by the HMC Web UI chhmcfs	X	X	X	
Free up space in HMC file systems chhmcfs	X	X		
List HMC file system information lshmcfs	X	X	X	X
Test for removable media readiness on the HMC ckmedia	X	X		X
Obtain required files for an HMC upgrade from a remote site getupgfiles	X	X		X
Provide screen capture on the HMC hmcwin	X	X	X	X
Log SSH command usage logssh	X	X	X	X
Clear or dump partition configuration data on a managed system lpcfgop		X		

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

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

Table 9. Command line tasks, associated commands, and user roles (continued)				
Command line tasks	**User roles/IDs**			
	Operator (hmcoperator)	**Super Administrator (hmcsuperadmin)**	**Viewer (hmcviewer)**	**Service Representative (hmcservicerep)**
Transfer a file from the HMC to a remote system sendfile	X	X	X	X
chsvc	X	X		X
lssvc	X	X	X	X
chstat	X	X		X
lsstat	X	X	X	X
chpwdpolicy		X		
lspwdpolicy	X	X	X	X
mkpwdpolicy		X		
rmpwdpolicy		X		
expdata		X		

Session handling

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

Session limitations

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

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

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

   System management for servers:

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

   System management for partitions:

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

HMC management:

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

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

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

Version mismatch state for a managed system

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

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

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

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

- **Save Area Version Mismatch**

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

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

- **Profile Data Save Area is full**

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

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

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

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

To recover from this state, first start the ASM by selecting the server with the **Version mismatch** and selecting **Connections and operations** and then **Launch advanced system management (ASMI)**.

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

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

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

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

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

- **Connection not allowed**

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

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

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

Systems management for servers

Systems displays tasks to manage servers. 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 and selections are made in the work area.

System content pane

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

The content pane displays all the available systems and the associated information for each system. The system information is displayed in a table view.

In the work pane, the following tabs are available:

Details
When you select the **Details** tab, each partition displays the system name, the current state of the system, state detail, machine type, serial number, attention LED status, reference code, and tags information.

Usage
When you select the **Usage** tab, each system displays the system name, the current state, serial number, CPU usage, memory usage, network I/O usage, and storage I/O usage information.

Resources
When you select the **Resources** tab, each system displays the system name, the current state, serial number, installed CPU, allocated CPU, installed memory, allocated memory, and available memory information.

Levels
When you select the **Levels** tab, each system displays the system name, the current state, serial number, firmware level, activated level, deferred level, and PNOR level information.

All
When you select the **All** tab, all the details of the system are displayed.

Notes:

1. You can search for a system by typing the system name as a keyword in the search bar available at the top of the Systems table.
2. You can customize the columns in the system table by clicking the **Customize columns** icon.
3. You can export the systems data by clicking the **Export** icon. The following formats are supported for exporting option:
   - PNG
   - PDF
   - CSV

You can choose to display the following information:

- Current state
- System name
- ID
- Attention LED
- Reference code
- RMC connection
- OS type
- OS level
- System
- Last activated profile
- Tags
- Description
- IP address
- Partition ID
- Environment
- Data collection
- Processor usage
- Processor peak
- Allocated memory
- Available memory
- Network I/O usage
- Storage I/O usage

Add system

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

For HMC version 10.3.1060.0, or later, to add one or more managed systems to the HMC, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**.
2. Click **Add system**. The **Add system** window opens.
3. To add a managed system, select the **Add system** option and enter the **Hostname or IP address** and **Password** for the managed system. For BMC systems, enter the **Username (BMC system)** of the BMC system.
4. Alternatively, you can select the **Find managed system** option and specify a range of IP addresses and click **Find system** to view a list of systems that were discovered.

   Note: The discovery process can take a long time to complete.

5. Click **Connect** to add the managed system to the HMC.

For HMC version 10.3.1050.0, or earlier, to add one or more managed systems to the HMC, complete the following steps:

1. From the HMC dashboard, click **Connect Systems**.
2. From the **Add Managed Systems** window, you can add a managed system by completing the following fields:
   - **Hostname or IP address**
   - **Username (BMC system)**
   - **Password**

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

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

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

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.

Create partition

You can quickly create partitions with minimum resources.

To create a partition, complete the following steps:

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

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

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

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

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 partition from template** wizard guides you through the deployment process and configuration steps.

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.

Connections and operations

Connections and operations contains the tasks for operating managed systems and to view the Hardware Management Console (HMC) connection status to service processors, reset those connections, connect another HMC to the selected managed system, or disconnect another HMC.

Power off system

Use the **Power off system** task to shut down the managed system. Powering off the managed system makes all partitions unavailable until the system is again powered on.

Before you power off the managed system, ensure that all logical partitions are shut down and that their states have changed from `Running` to `Not Activated`. For more information about shutting down a logical partition, see “Shutdown partition” on page 69

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 might result in data loss and further delays when you activate the logical partitions once more.

To power off a managed system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to power off, and then click **Connections and operations** > **Power off system**. The **Power off system** window opens.
3. Select one of the following options:

   Normal power off
   The Normal power off mode shuts down the system operations in a controlled manner. During the shutdown, programs that are 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.
4. Select **Force power off** to power off a managed system while a dump from the managed system is being offloaded to the HMC. It is recommended to wait until the dump offload operation is complete before powering off. If not, the dump might be corrupted or incomplete.
5. Confirm the system name to be powered off, and click **Power off**.

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

Power on system

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

To power on a managed system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to power on and then click **Connections and operations** > **Power on system**. The **Power on system** window opens.
3. Select one of the following options to power on your managed system:
   - **Normal power on**: Select this option to specify that the HMC uses the current setting for the partition start policy to determine how to power on the managed system. The current setting can be one of the following values:
     - **Auto-Start Always**: This option specifies that the HMC power on logical partitions automatically after the managed system powers on. If powering on the managed system is the result of a user action, the HMC starts all partitions that are configured for automatic startup. If powering on the managed system is the result of an automatic recovery process, the HMC starts only those logical partitions that were running at the time the system is powered off. This option is always available for selection.
     - **Stop at Partition Standby**: This option specifies that logical partition startup is in standby mode after the managed system powers on and the HMC does not start any logical partitions when the managed system powers on. If powering on the managed system is the result of an automatic recovery process and the HMC is used to start a logical partition, the HMC starts all logical partitions that were running at the time the system is powered off. This option is available for selection only when the firmware for the managed system does not support advanced IPL capabilities.
     - **Auto-Start for Auto-Recovery**: This option specifies that the HMC power on logical partitions automatically only after the managed system powers on as the result of an automatic recovery process. This option is available for selection only when the firmware for the managed system supports this advanced IPL capability.
     - **User-Initiated**: This option specifies that the HMC does not start any logical partitions when the managed system powers on. You must start logical partitions manually on the managed system by using the HMC. This option is available for selection only when the firmware for the managed system supports this advanced IPL capability.

     Note: You can set the partition start policy from the **Power On Parameters** page of the **Properties** task for the managed system.
   - **System profile**: Selecting this power-on option specifies that the HMC power on the system and its logical partitions based on a predefined system profile. When you select this power-on option, you must select the partition profile that you want the HMC to use to activate logical partitions on the managed system.
   - **Hardware Discovery**: Selecting this power-on option specifies that the HMC run the hardware discovery process when the managed system powers on. The hardware discovery process captures information about all I/O devices, in particular those devices that are not currently assigned to partitions. When you select the hardware discovery **power on** option for a managed system, the managed system is powered on into a special mode that performs the hardware discovery. After the Hardware Discovery process is complete, the system will be in Operating state with any partitions in the power-off state. The hardware discovery process records the hardware inventory in a cache on the managed system. The collected information is then available for use when you display data for I/O devices or when you create a system plan based on the managed system. This option is available only if the system is capable of using the hardware discovery process to capture I/O hardware inventory for the managed system.
4. Click **Power on** to complete the operation.

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

Rebuild system

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.

To rebuild a managed system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to rebuild, and then click **Connections and operations** > **Rebuild system**. The **Rebuild managed system** window opens.
3. Confirm the system name to rebuild, and click **Rebuild**.

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

Schedule operations for HMC Version 10.3.1060.0, or earlier

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

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

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

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

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

Notes:

- You can specify the number of weeks or months to elapse before performing the scheduled operation again on each selected day.
- With the Hardware Management Console (HMC) Version 10.1.1020, or later, you can specify the interval to be monthly. The scheduled operation is run on the configured time and month. It is also run on the subsequent months based on the number of repetitions and monthly intervals that you have configured.
- For example, if you configure the scheduled operation for 31st of every month with five repetitions, then the scheduled operation is executed every month on 31st, and if a particular month does not have 31st then that repetition is executed on the last day of the month. For example, if you configure the scheduled operation from 31 January with five repetitions, then the operation is executed on 31 January, 28 February, 31 March, 30 April, and 31 May.

From the **Scheduled Operations** window, you can perform the following tasks:

- Schedule an operation to run later.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select one or more managed systems, and then click **Connections and operations** > **Schedule operations**.
3. From the **Scheduled operations** window, click **Options** from the menu bar to display the next level of options:
   - To add a scheduled operation, click **Options** and then click **New**.
   - To delete a scheduled operation, select the operation that you want to delete, point to **Options** and then click **Delete**.
   - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
   - To view a scheduled operation, select the operation that you want to view, point to **View** and then click **Schedule Details...**.

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

4. To close the window, click **Options** and then click **Exit**.

Disconnect another management console

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

About this task

To disconnect another HMC, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server from which you want to disconnect a management console, and then click **Connections and operations** > **Disconnect another management console**.
3. Select an HMC from the list and click **OK**.

   Note: For HMC version 10.3.1060.0, or later, select an HMC from the list and click **Disconnect** to complete the operation.

Change system password

Use this task to change the Hardware Management Console (HMC) access password on the selected managed system.

Note: 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.

To change the system access password, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system for which you want to change the access password, and then click **Connections and operations** > **Change system password**. The **Change system access password** window opens.
3. Enter values for **Current HMC Access password**, **New HMC Access password**, and **Confirm HMC Access password** fields.
4. Click **Save** to complete the operation.

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

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

Reset or remove system connection

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

For HMC version 10.3.1060.0, or later, to reset or remove connections, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to reset, and then click **Connections and operations** > **Reset system connection**. The **Reset system connection** window opens. Confirm the system connection that you want to reset, and click **Reset**.
3. Select the system that you want to remove, and then click **Connections and operations** > **Remove system connection**. The **Remove system connection** window opens. Confirm the system connection that you want to remove, and click **Remove**.

For HMC version 10.3.1050.0, or earlier, to reset or remove connections, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server that you want to reset or remove, and then click **Connections and operations** > **Reset or remove system connection**.
3. Select one of the options from **Reset Connection** or **Remove Connection** and click **OK**.

Launch advanced system management (ASMI)

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 **System resources**, and then select **Systems**.
2. In the content area, select one or more managed systems, and then click **Connections and operations** > **Launch advanced system management (ASMI)**.

Service processor status

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

About this task

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

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to view the service processor connection status and click **Connections and operations** > **Service processor status**.

Setup FSP failover

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

FSP failover is designed to reduce customer outages due to service processor hardware failures. If a redundant service processor is supported for the current system configuration, you can set up FSP Failover for the selected managed system.

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to view the setup FSP failover, and then click **Connections and operations** > **Setup FSP failover**.

Initiate FSP failover

Initiate a secondary service processor if the primary service processor of your managed system fails.

FSP failover is designed to reduce customer outages due to service processor hardware failures.

To start the FSP failover, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to view the setup FSP failover, and then click **Connections and operations** > **Initiate FSP failover**.

Manage system profiles

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

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

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

Use the **Manage system profiles** page 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 edit an existing system profile.
- Set a system profile as the default 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.

  Note: Before you activate a system profile, ensure that all partitions with partition profiles in the system profile are shutdown.

Complete the following steps to access the **System profiles** page:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Select the system for which you want to create a system profile, and then click **Connections and operations** > **Manage system profiles**. The **System profiles** page opens.

   Alternatively, starting from HMC version 10.3.1060.0, or later, you can click the system name for which you want to create a system profile, and then select **System profiles** in the content pane. The **System profiles** page opens.

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

Power management

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

About this task

To enable power saver mode, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to enable the power saver mode, and then click **Connections and operations** > **Power management**.
3. Choose from any of the following Power Saver mode options:

- **Static**: Reduces the power consumption by reducing the processor clock frequency and the voltage to fixed values. This option delivers predictable performance while reducing the power consumption.
- **Dynamic Power Saver mode**: Delivers power savings by varying the processor frequency and voltage that is based on the utilization of the system processors. In Dynamic Power Saver Mode, the system firmware balances performance and power consumption.
- **Maximum Performance mode**: Causes the processor frequency to be set at a specified fixed value. You can set the maximum limit of the processor frequency and power consumption of the system.
- **Dynamic performace mode**: The system firmware defaults to the maximum processor core frequency allowed for a system's environment and configuration. It also reduces frequency only when a system is less used or idle.

Note: If you enable a Power Saver mode, processor frequencies, processor usage will change, and power consumption will change. It also causes varying performance.

4. You can also choose to enable or disable the **Idle power saver** mode. When it is enabled, it reduces the energy consumption when the system is in idle state.

   Note: Setting the Power Saver and Idle Power Saver modes are independent operations.

Manage 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.

To manage the partition availability priority, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage the partition availability priority, and then click **Connections and operations** > **Manage partition availibility priority**.

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

View workload management groups

This task displays 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.

Capture configuration as template

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to view the system information, and then click **Connections and operations**.
3. Click **Capture with physical I/O as template** or **Capture without physical I/O as template**.
4. Enter a template name and description, and then click **OK**.

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

VMI configuration for eBMC-based managed systems

View or modify the Virtualization Management Interface (VMI) configuration settings for eBMC-based managed systems.

About this task

You can use this task to modify the following VMI configuration settings:

- IP Address type
- Network Interface
- IP Type
- IPV4 Address
- IPV6 Address
- Subnet Mask
- Gateway

To view or modify the VMI configuration settings, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select one or more eBMC-based managed systems, and then click **Connections and operations** > **VMI configuration**.
3. From the **VMI Configuration** window, select the IP address for which you want to modify the VMI configuration and then click **Actions** to modify or clear the VMI configuration settings.
4. After you modify the VMI configuration settings, click the **Refresh** icon to view the updated VMI configuration settings.

Manage Partition Data

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

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

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

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

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

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

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

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

Use the Manage Partition Data tasks to complete the following tasks:

- Restore partition data. If you lose partition profile data, use the restore task in one of the following ways:
  - Restore partition data from a backup file. Profile modifications that are completed after the selected backup file was created are lost.
  - Restore merged data from your backup file and recent profile activity. The data in the backup file takes priority over recent profile activity if the information conflicts.
  - Restore merged data from recent profile activity and your backup file. The data from recent profile activity takes priority over your backup file if the information conflicts.
- Initialize partition data. Initializing the partition data for a managed system deletes all of the currently defined system profiles, partitions, and partition profiles.
- Back up a partition profile to a file.
- Back up partition data to a file.

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

Utilization Data

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

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

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

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

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

Firmware

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

Check readiness

Check the readiness status of a selected system from the Hardware Management Console (HMC).

To check the system readiness, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server and click **Firmware** > **Check readiness**.
3. When you have completed this task, click **Close**.

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

View current system firmware levels

View the system firmware information or update the system firmware.

To view the system firmware information, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. To view the firmware information of the system, select the server for which you want to view the firmware information and click **Firmware** > **View current system firmware levels**.
3. After you complete this task, click **Close**.

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

Update system firmware

You can update the firmware levels on the managed system.

To update the system firmware on the selected managed systems, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**.
2. Click **Firmware** > **Update system firmware**. The **Update system firmware** page opens. Complete all the steps that are listed in the page.

   Notes:

   - With HMC 10.3.1061.0, or later, the HMC provides an option to resume previously failed updates. If a previous update failed, you can resume that update from the point of failure. If the **Resume** operation is available during the **Choose firmware type and target level** step, select **Resume** as the update type to resume the previously failed update. You can select **Update** or **Upgrade** as the update type, as applicable, to start a new operation.
   - When you are resuming an update at a power-off or power-on step, the system can be in either state. In all other cases, the state of the system must match the state at the point of failure.
   - If any firmware operation changes the state of the server, such as setting the next IPL side or backing up the firmware level, the resume operation will not be available.

Use the online Help if you need additional information for updating the system firmware.

View current I/O firmware levels

View the current I/O firmware information.

To view the I/O firmware information of the selected managed system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Click **Firmware** > **View current IO firmware levels**.
3. After you complete this task, click **Close**.

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

Update I/O firmware

Update the I/O firmware.

To update the I/O firmware on the selected managed systems, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Click **Firmware** > **Update IO firmware**.
3. After you complete this task, click **Close**.

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

View current SR-IOV firmware levels

View the SR-IOV firmware information.

Note: The SR-IOV adapter must be in shared mode.

To view the SR-IOV firmware information of the system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server and click **Firmware** > **View current SR-IOV firmware levels**.
3. After you complete this task, click **Close**.

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

Update SR-IOV Firmware

Update the driver firmware for shared SR-IOV adapters.

Note: The SR-IOV adapter must be in shared mode.

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. To update the SR-IOV adapters, select the server and click **Firmware** > **Update SR-IOV firmware**.
3. Select the SR-IOV adapters and click **Action** to specify the type of firmware update to start.

   Note: You can update either the adapter firmware or both the adapter driver and adapter firmware. During the firmware update operation, the configured logical ports on the SR-IOV adapter might experience a temporary disruption of network traffic. It might take 2 - 5 minutes to update each SR-IOV adapter. The update operation is performed serially across all the SR-IOV adapters.
4. After you complete this task, click **Close**.

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

Service

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 **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Service**.
3. Select the serviceability task that you want to perform from the list.

Manage serviceable events

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceable events and click **Service** > **Manage serviceable events**.
3. Provide event criteria, error criteria, and FRU criteria. If you do not want the results to be filtered, select **ALL**. Click **Refresh** to refresh the list of serviceable events based on the criteria filter values.

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

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

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

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

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

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

Create serviceable event

This task reports problems that occurred on your Hardware Management Console (HMC) to the service provider (for example, the mouse does not work) or lets you test problem reporting.

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

Reporting a problem

To report a problem on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Create serviceable events**.
2. Enter a brief description of your problem in the **Problem Description** field and then click **Request Service**.

To test problem reporting from the **Create Serviceable Event** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem Description** 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.

Reporting a problem after selecting a system

To report a problem after selecting a system on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Create serviceable event**.
3. In the **Create Serviceable Event** window, you can select a **Problem Type** that describes where the problem occurred or what is the problem.
4. Enter a brief description of your problem in the **Problem Description** field and then click **Request Service**.

To test problem reporting from the **Create Serviceable Event** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem Description** 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.

Add FRU

Locate and add a Field Replaceable Unit (FRU).

To add a FRU to a POWER10 system, complete the following steps:

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

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

Exchange FRU

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

To exchange a FRU, complete the following steps:

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

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

Remove FRU

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

To remove a FRU, complete the following steps:

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

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

Add enclosure

Learn how to locate and add an enclosure.

To add an enclosure, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Add enclosure**.
3. Select an enclosure type, then click **Add**.
4. Click **Launch Procedure**.
5. When you complete the enclosure installation process, click **Finish**.

Remove enclosure

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

To remove an enclosure, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Remove enclosure**.
3. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to **Pending Actions**.
4. Click **Launch Procedure** to begin removing the enclosures that are identified in **Pending Actions** from the selected system.
5. Click **Finish** when you complete the enclosure removal process.

Power on/off IO unit

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

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

To power on or power off an I/O unit, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Power on/off IO unit**.

Manage identify LED states

With HMC Version 10.3.1050, or later, you can view the information about system attention LED and light-specific LEDs to identify a system component on a managed system.

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

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

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

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

Identify LED for an enclosure

If you want to add an adapter to a specific drawer (enclosure), you need to know the machine type, model, and serial number (MTMS) of the drawer. To determine whether, you have the correct MTMS

for the drawer that needs the new adapter, you can activate the LED for a drawer and verify that the MTMS corresponds to the drawer that requires the new adapter.

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

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

Open MES

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

To open MES, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Open MES**.

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

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

Close MES

Close MES order numbers.

To close MES, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Close MES**.

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

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

Collect VPD

Copy Vital Product Data (VPD) to removable media.

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

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

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

- Install or remove a sales feature.
- Upgrade or rollback a model.
- Upgrade or rollback a feature.

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

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

System details view

Displays the tasks that can be performed on the managed system. This information is useful in system and partition planning and resource allocation.

To open the system drill down view, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Click the server for which you want to manage tasks. The system menu pod is displayed.
3. Select the task that you want to perform from the list.

Note: With HMC Version 10.2.1040, or later you can search for a system action that you want to perform by typing the name of the task as a keyword in the search bar that is available under the **System actions** menu.

System settings

Complete the following steps to view or modify the general and advanced settings of the managed system:

1. In the navigation area, click **System resources** > **System**. The **Systems** page opens.
2. Click on a system to view the additional properties.
3. Click **Systems settings**. The **General settings** page opens.

The following tabs are displayed:

- General properties
- Migration
- Power on parameters
- Advanced

General properties

You can view or modify the general properties of the managed system. The **General Properties** tab displays the name of the system, IP address, reference code, machine type, serial number, location of the system, firmware, default configuration, maximum partitions, service partitions, group tags, description, uptime, and power off policy information.

Migration

You can view and modify the partition mobility properties on managed system:

- Inactive profile migration policy

  Select the migration policy that you want to use when you migrate inactive partitions. The following options are available:

  - Partition Configuration: This policy configures the management console to use the partition state that is defined for the logical partition in the hypervisor when you migrate or validate the migration of an inactive logical partition. If the inactive partition that you are migrating is not capable of starting automatically, the management console uses the configuration data that is defined for the partition in the last activated profile.
  - Last Activated Profile: This policy configures the management console to use the memory and processor configuration data that is defined in the last activated profile for the logical partition when you migrate or validate the migration of an inactive logical partition.

- NPIV validation policy

  Select the required NPIV validation policy that you want to use to validate active partition migration. The following options are available:

  – Port validation only: Configures the management console to perform only N_Port ID Virtualization (NPIV) port validation when you validate the active partition migration.
  – Port and Disk validation Configures the management console to perform both NPIV port and disk validation when you validate the active partition migration.

  Note: If the NPIV validation value is already specified during the partition migration validation operation, this policy is not considered.

- Allow Migration with Inactive Source Storage VIOS

  You can perform Live Partition Mobility (LPM) using this option when the source Virtual I/O Server (VIOS) that is hosting the storage adapters is powered off or shutdown. If you enable this option, the storage configuration-related data is collected for all client partitions based on the CEC level preference. The collected data is used to perform LPM on the powered off VIOS.

- Migration Capabilities

  The migration capabilities table displays information about the type of migration that is supported, the number of migrations that are in progress, and the number of migrations that are supported by the managed system. In active migration, you can migrate a running logical partition without shutting down any applications. In inactive migration, you can migrate a logical partition that is powered-off.

Power On parameters

From the **Power On Parameters** tab, you can view or modify the power-on parameters for the next restart.

To modify the power-on parameters, select the required option in the Next value column of the Partition start policy, Power-On Side, and Keylock position fields.

Note: These changes are only valid for the next managed system restart.

Advanced

You can view or modify the advanced settings of the managed system. 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 required memory.

Note: 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.

- Memory mirroring

  This option displays the current mirroring mode and the current system firmware mirroring status. To modify the value and set the next mirroring mode, select the required option from the Next value drop-down list.

- Memory optimization

  This option displays the amount of available mirrored memory on the system. You can specify the additional amount of memory that the system might require. To increase the amount of available mirrored memory, click **Launch Memory Optimization tool**.

- Virtual Trusted Platform Module

Displays the Virtual Trusted Platform Modul (VTPM) settings.

- Supported Hardware Accelerator Types

  Supported hardware accelerator types: You can view the list of supported hardware accelerators for a managed system and the total and available number of Quality of Service (QoS) credits. This section is not displayed if the managed system does not support hardware accelerators. The Supported Hardware Accelerator Types table displays the following information:

  – The type of the hardware accelerator.
  – Maximum QoS credits for a system hardware accelerator.
  – Available QoS credits for a system hardware accelerator.

Processor, Memory, I/O

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

These properties include the following tabs:

Processor

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

- available processor units
- available with stealable processor units
- processing units that are assigned to partitions
- configurable processing units
- installed processing units
- multiple shared processor pools support

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

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

Notes:

- The information about stealable processor units is available only when the managed system is in the standby state or in the operating state.
- If the managed system is licensed with Power® IFL processor and if the firmware level is at FW910, or later, the **Available (with stealable)** field is displayed.
- When a Power10 system is licensed with some IFL processors, the tab also displays the information about the remaining processors that are available for running the AIX or IBM i partitions.

Memory

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

- available memory
- available with stealable memory
- memory assigned to partitions
- assigned persistent memory
- reserved memory
- configurable memory
- installed memory
- active memory sharing support
- memory region size with `Current Value` and `New Value (After System Restart)` fields that specify the current and new value.

Note: You can change the size of the Logical Memory Block (LMB) by changing the values in the `Next Value` field. The changes of this field are applied only after the next managed system restart.

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

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

Physical I/O adapters

The **Physical I/O Adapters** tab displays the physical I/O resources for the managed system. The assignment of I/O slots and partition, the adapter-type, and the slot LP limit information are displayed. The physical I/O resources information is grouped by units.

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

PowerVM

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

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

The PowerVM functions include the following tasks:

- Managing Virtual I/O Servers
- Managing virtual networks
- Managing virtual storage
- Managing hardware virtualized I/O (SR-IOV adapters)
- Managing a reserved processor pool
- Managing shared processor pools
- Managing a shared memory pool

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

Manage system profiles

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

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

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

Use the **Manage system profiles** page 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 edit an existing system profile.
- Set a system profile as the default 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.

  Note: Before you activate a system profile, ensure that all partitions with partition profiles in the system profile are shutdown.

Complete the following steps to access the **System profiles** page:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Select the system for which you want to create a system profile, and then click **Connections and operations** > **Manage system profiles**. The **System profiles** page opens.

   Alternatively, starting from HMC version 10.3.1060.0, or later, you can click the system name for which you want to create a system profile, and then select **System profiles** in the content pane. The **System profiles** page opens.

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

Backup profile data

The partition data includes all configurations, such as the system profile, partition profile, and system configuration details. You can use the **Backup profile data** page to backup, delete, or restore the partition data of a managed system.

The partition data for logical partitions (LPARs) is stored in nonvolatile random access memory (NVRAM) on the Power server. However, this data can be lost during events that require the replacement of the flexible service processor (FSP). This may occur if a system board is replaced on smaller, integrated systems or if the FSP fails on larger systems. Keeping profile data backups can significantly speed up recovery in the event of major hardware repair.

With HMC 10.3.1061.0, or later, complete the following steps to manage the partition data of a managed system:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.

2. Click the system name for which you want to manage backup profiles, then select **Backup profile data** in the content pane. The **Backup profile data** page opens. This page displays the list of existing backup files for the managed system and the time at which each backup file was created.
3. You can perform the following operations to manage backup profile data:
   - Creating a new backup profile file:
     a. Click **Backup profile data**. The **Backup profile data** window opens.
     b. Select the **Create a new backup file** option.
     c. Enter a backup file name, and click **Backup**.

     Note: You can enter up to 31 alphanumeric characters for the backup profile name. The following special characters are allowed: Hyphen (-) and underscore (_).
   - Replacing an existing backup profile file:
     a. Click **Backup profile data**. The **Backup profile data** window opens.
     b. Select the **Replace existing backup file** option.
     c. Select an existing backup file name from the drop down menu, and click **Backup**.
   - Restoring the profile data:
     a. Select the backup file name and click **Restore**. The **Restore profile data** window opens.
     b. Select one of the following options:
        – Full restore from the selected backup file: Restores profile data by using only your backup file. Any profile modifications that are performed after the selected backup files is created will be lost.

          Note: Select this option for a managed system in the recovery state.
        – Backup priority: Merges the stored backup with the recent profile activity. If there is any information conflict, the stored backup data is restored over the recent profile activity.
        – Managed system priority: Merges the recent profile activity with the stored backup. If there is any information conflict, the recent profile activity is restored over the stored backup data.

        Note: You can also select **Force restore partition keystore** to restore the keystore data by ignoring the errors.
     c. Click **Restore**.
   - Deleting backup profile files:
     a. Select the backup file names that you want to delete, and click **Delete**. The **Delete backup profile data** confirmation window opens.
     b. Confirm the backup file names to be deleted, and click **Delete**.

   Notes:

   - You can search for a specific backup profile by entering a search keyword in the search bar.
   - The default backup file is also listed in the table. You cannot delete the default backup profile file.
   - You cannot create a backup profile file when the managed system is in the recovery state.

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

Capacity on Demand for HMC Version 10.3.1060.0, or later

With Capacity on Demand (CoD) offerings you can dynamically activate one or more resources on your server as your business peaks dictate.

Capacity on Demand also gives you the option to temporarily activate capacity to meet intermittent performance needs, to activate extra capacity on a trial basis, and to access capacity to support operations in times of need.

Capacity on Demand resources

Learn about the different Capacity on Demand (CoD) resources that are available for your system.

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

To view the **CoD resources** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view CoD details.
3. Click **CoD resources** in the content pane menu.

   Note: Click **Enter activation code** to enter the CoD activation codes that you have for your system. If you get an error that the code is not valid, ensure that the code you are entering was generated for that specific managed system.

The **CoD processor capacity** section displays the total number of processors, processors that are active, and those processors that can be activated by using CoD.

- **Inactive processors**: Displays the total number of inactive processors on your managed system.
- **Permanently activated processors**: Displays the total number of permanently activated processors on your managed system.
- **Temporarily activated processors**: Displays the number of processors that are temporarily activated on your managed system
- **Installed processors**: Displays the total number of processors that are installed on your managed system. This number includes both active processors and inactive processors.

The **CoD memory capacity** section displays the available memory, amount of active memory, and memory available for activation by using CoD.

- **Inactive memory**: Displays the total number of inactive memory units on your managed system.
- **Permanently activated memory**: Displays the total number of permanently activated memory units on your managed system.
- **Temporarily activated memory**: Displays the number of memory units that are temporarily activated on your managed system
- **Installed memory**: Displays the total number of memory units that are installed on your managed system.

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

Elastic CoD

You can view the total number of Elastic Capacity on Demand (Elastic CoD) memory units that are temporarily activated on your managed system. You can activate memory units that are already installed on your managed system for a specified number of days as your business peaks demand. You are charged for the total number of memory days that the Elastic CoD memory remains activated.

To view the **Elastic CoD** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view Elastic CoD details.
3. Click **Elastic CoD** in the content pane menu.
4. Click **Enter activation code** to enter the CoD activation codes that you have for your system. If you get an error that the code is not valid, ensure that the code you are entering was generated for that specific managed system. The **Processors** and **Memory** sections display the state of the Elastic CoD.
5. Click **View activation code information** to view information about the CoD activation code.

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

Trial CoD

You can view the total number of Trial Capacity on Demand (Trial CoD) processors and memory that are temporarily activated on the managed system. You can activate the inactive processors and memory that are installed on the managed system for a trial period (that is, a defined number of days).

To view the **Trial CoD** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view Trial CoD details.
3. Click **Trial CoD** in the content pane menu.
4. Click **Enter activation code** to enter the CoD activation codes that you have for your system. If you get an error that the code is not valid, ensure that the code you are entering was generated for that specific managed system. The **Processors** and **Memory** sections display the state of the Trial CoD.
5. Click **View activation code information** to view information about the CoD activation code.

Use the online Help if you need additional information about Trial CoD.

CoD history log

The Capacity on Demand (CoD) history log contains information about the CoD events that occurred on your system. The entries are shown in chronological order, starting with the most recent entry. You can see the timestamp and the log entry that contains a description for each event that occurred.

After the history log reaches the maximum number of entries for your system, subsequent entries cause the history log to wrap, that is, the newest entry overlays the oldest entry.

To view the **CoD history log** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view CoD history log details.
3. Click **CoD history log** in the content pane menu. A table with timestamp and log entries is displayed.

Use the online Help if you need additional information about CoD history log.

Licensed capabilities

You can view the licensed capabilities that are supported on your managed system.

To view the **Licensed capabilities** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view licensed capabilities details.
3. Click **Licensed capabilities** in the content pane menu.
4. Click **Enter activation code** to enter the CoD activation codes that you have for your system. If you get an error that the code is not valid, ensure that the code you are entering was generated for that specific managed system.

The **PowerVM licensed capabilities** section displays the runtime capabilities that are supported by the managed system.

- **Active memory sharing**: When the managed system is Active Memory Sharing capable, you can configure multiple partitions to share system memory. Partitions can share the memory in the shared memory pool by using the PowerVM Active Memory Sharing technology (or shared memory).
- **Live partition mobility**: You can migrate AIX, IBM i, and Linux® logical partitions from one system to another. The mobility process transfers the system environment that includes the processor state, memory, attached virtual devices, and connected users.
- **Micro-partitioning**: When the managed system is Micro-Partitioning® capable, a logical partition can use fractions of processors from a shared processor pool.
- **PowerVM partition remote restart**: When the managed system is PowerVM Partition Remote Restart capable, you can remotely restart logical partitions. Use this feature to recover the partitions quickly during a source server failure.

- **Partition suspend**: When the managed system is Partition Suspend capable, you can suspend processing for a logical partition and save its state to a suspend file. Suspending the logical partition frees up system resources for use by other activities. When you resume the logical partition, the partition operates again from the point at which it was suspended
- **SR-IOV (logical port limit)**: When the managed system is single root I/O virtualization (SR-IOV) capable, the SR-IOV adapter can be configured in the shared mode and can be shared by multiple logical partitions. If this capability is not supported, the SR-IOV adapter can be configured in the shared mode but can be used by only one logical partition.
- **Virtual I/O server**: When the managed system is Virtual I/O Server capable, you can create Virtual I/O Server logical partitions on the managed system.

The **Other licensed capabilities** section displays the following information:

- **Active memory expansion**: When the managed system is Active Memory Expansion capable, you can expand memory on the server beyond the physical limits of the server and beyond the capacity of the true physical memory that is assigned to an AIX partition. By using this feature, you can enable a partition to do more work with less memory. You can also expand the memory capability of the server to run more partitions.
- **Active memory mirroring for hypervisor**: When the managed system is Active Memory Mirroring for Hypervisor capable, two identical copies of the system hypervisor are maintained in memory always. Both copies are simultaneously updated with any changes. If there is a memory failure on the primary copy, the second copy is automatically called, eliminating platform outages due to uncorrectable errors in system hypervisor memory. Active Memory Mirroring for hypervisor is designed to ensure that system operation continues even in the unlikely event of an uncorrectable error that is occurring in main memory that is used by the system hypervisor. The feature permanently activates the Active Memory Mirroring for hypervisor capability.
- **AIX enablement for 256-core partition**: When the managed system is AIX Enablement for 256-Core Partition capable, the feature permanently enables greater than 128 cores and up to 256 cores per dedicated processor partition. Without this feature, the largest partition that can be created is up to 128 cores. Micropartitions, which are not affected by this feature, can be created with a maximum of 128 virtual processors.
- **Coherent accelerator processor interface (CAPI)**: When the managed system is CAPI enabled, an I/O adapter can be used as a coherent accelerator to participate in memory coherency domain to accelerate system workloads.
- **Dynamic platform optimization**: When the managed system is Dynamic Platform Optimization (DPO) capable, you can dynamically optimize the placement of partitions. This function increases the processor-memory affinity of the partitions to improve the performance. To enable this function, certain systems require a DPO activation code. You can click Enter Activation Code to activate the DPO code.
- **IBM i 5250 application**: When the managed system is IBM i 5250 Application capable, you can run 5250 applications on the IBM i partitions of the managed system. 5250 applications include all 5250 sessions (such as 5250 emulation, Telnet, and screen scrapers), interactive system monitors, and twin axial printer jobs.
- **IBM i native I/O**: When the managed system is not IBM i native I/O capable, IBM i I/O must be virtualized by using the Virtual I/O Server, and the Restricted I/O Partition setting must be enabled for all IBM i partitions. The management console does not know the IBM i native I/O capability of a managed system with firmware level 850 or below so the capability is not displayed.

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

Licensed capabilities history log

The licensed capabilities history log contains information about the history log of the licensed functions on your system. The history log contains information about the activations of Capacity on Demand (CoD) advanced functions that occurred on your system.

CoD advanced functions include PowerVM Enterprise Edition, PowerVM Standard Edition, Live Partition Mobility Trial, Enterprise Enablement, WWPN Renewal, Active Memory Expansion, AIX Enablement for 256-core LPAR, and Active Memory Mirroring for Hypervisor. A log entry is created each time an activation

code is entered successfully, and each time a CoD advanced function trial expires. For each entry in the CoD advanced functions activation history log, this table shows the timestamp on the system when the entry was logged and a description of the log entry. The entries are shown in chronological order, starting with the most recent entry.

To view the **Licensed capabilities history log** page, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**. The **Systems** page opens.
2. Click the system for which you want to view licensed capabilities history log.
3. Click **Licensed capabilities history log** in the content pane menu. A table with timestamp and log entries is displayed.

Use the online Help if you need additional information about Licensed capabilities history log.

Capacity on Demand for HMC Version 10.3.1050.0, or earlier

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

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

Capacity on Demand functions

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

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

The **CoD processor capacity** functions include the following tasks:

- – Inactive processors
  - Permanently activated processors
    - Linux or VIOS only
    - Any
  - Temporarily activated processors
  - Installed processors

The **CoD memory capacity** functions include the following tasks:

- – Inactive memory
  - Permanently activated memory
  - Temporarily activated memory
  - Installed memory
- Temporarily activated memory

The **Elastic CoD** functions include the following tasks:

- Enter activation code
- Elastic CoD processors
- Elastic CoD memory

The **Trial CoD** functions include the following tasks:

- Enter activation code
- Trial CoD processors
- Trial CoD memory

The **CoD history log** contains information about the CoD events that occurred on the system. A description about the event is displayed with a timestamp.

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

Licensed Capabilities

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

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

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

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

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

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 **Logs**, and then select **Tasks log**.

   Note: Alternatively, you can access **Tasks log** by clicking **System resources** > **Systems** and then click the system for which you want to view the tasks log. The **Tasks log** task is displayed menu pod.
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.

Reference code log

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Click the server for which you want to manage serviceability tasks and then click **Reference code log** in the menu pod.
3. Select a specific reference code to view the details.

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

RIO configuration

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

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

To view the hardware topology, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and then click **Rio configuration** in the menu pod.
3. View the hardware topology information.

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

PCI configuration

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and click **PCI configuration** in the menu pod.
3. View the PCIe hardware topology.

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

Topology diagrams

Learn how to view the topology diagrams of the selected system.

You can use the Hardware Management Console (HMC) to view the topology diagrams of the selected system, including the virtual and physical components.

Virtual networking diagram

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

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

displayed in a click card. Alternatively, you can hover over the label of a resource area to display the name of the resource as a tooltip.

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Virtual networking diagram** in the menu pod.
3. 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.
4. 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.
5. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the virtual networking diagram.

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

Virtual storage diagram

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and click **Virtual Storage Diagram** in the menu pod.

   Note: To view the virtual storage diagrams of a single partition in a particular system, select the partition of your choice and then click **Partition virtual storage diagram** in the menu pod.
3. 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.
4. 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.
5. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the virtual storage diagram.

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

SR-IOV vNIC diagram

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the server for which you want to manage serviceability tasks and click **SR-IOV vNIC diagram** in the menu pod.
3. 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.
4. 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.
5. In the upper-right corner of the work pane, click the **Legend** icon to view an explanation of the symbols that are used in the SR-IOV and vNIC diagram.

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

Serviceability

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

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

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

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

Type, Model, Feature

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

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

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

Hardware Operations

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

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

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

Prepare for Hot Repair or Upgrade

Provides a summary of required actions to be performed to isolate a particular hardware component as part of a service procedure.

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

Systems Management for Partitions

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

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

Partition content pane

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

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

In the work pane, the following tabs are available:

Details
When you select the **Details** tab, each partition displays the partition name, the current state of the partition, partition ID, attention LED status, IP address, reference code, RMC connection status, OS type, OS level, last activated profile, tags, and description information.

Usage
When you select the **Usage** tab, each partition displays the partition name, the current state, processor usage, network I/O usage, and storage I/O usage information.

Resources
When you select the **Resources** tab, each partition displays the partition name, the current state, allocated processors,allocated virtual processors, processor mode, processor weight, allocated memory, and memory mode information.

All
When you select the **All** tab, all the details of the partition are displayed.

Notes:

1. You can search for a partition by typing the partition name as a keyword in the search bar that is available at the top of the Partitions table.
2. You can customize the columns in the partitions table by clicking the **Customize columns** icon.
3. You can export the partition data by clicking the **Export** icon. The following formats are supported for exporting option:

- PNG
- PDF
- CSV

You can choose to display the following information:

- Current state
- System name
- ID
- Attention LED
- Reference code
- RMC connection
- OS type
- OS level
- System
- Last Activated profile
- Tags
- Description
- IP address
- Partition ID
- Environment
- Data collection
- Processors
- Memory
- Network I/O usage
- Storage I/O usage

Partition properties

Partition properties display properties of the selected partition. These properties include:

You can view the partition's name, IP address, resource configuration, version of the operating system that is installed on the partition, the system on which the partition is located, the description of the partition, group tags, and partition uptime.

Notes:

- On Power10 processor-based systems, the image date of the OS that is installed on the partition and the expiration date of the AIX Update Access Key (UAK) for the managed system are displayed for AIX and AIX/Linux partitions.
- If the managed system supports virtual serial numbers, the Virtual Serial Number is displayed.

Virtualized trusted platform module settings

Click **Virtualized trusted platform module settings** to enable the AIX environment of the logical partition to use Trusted Boot capability.

Advanced settings

Click **Advanced settings** to view additional properties of the partition, including the list of supported hardware accelerators for a logical partition and Quality of Service (QoS) credits for a specific hardware accelerator if the managed system supports hardware accelerators.

Notes:

- If the managed system supports Platform KeyStore, you can select the value of the **Platform KeyStore Size** option in the range 4 KB - 64 KB. The value of 0 KB for the **Platform KeyStore Size** option indicates that the platform keystore function is disabled for the logical partition.
- With HMC version 10.3.1060.1, or later, you can enable the **KVM capable** option to run Kernel-based Virtual Machine (KVM) in a PowerVM LPAR. This new feature of PowerVM enables the use of KVM, a popular Linux virtualization technology, utilizing common Linux virtualization administration skills and tools. This technology enables expanded open source-based innovations and solutions on the Power platform.

Processors

The **Processor** displays the properties of the logical partition that uses shared or dedicated processors. You can assign the logical partition to be either in Capped or Uncapped mode.

Note: A capped logical partition cannot use more processing units than are committed to the logical partition. An uncapped logical partition can use idle processing units when the logical partition needs more processing units.

To view and edit the processor details, complete the following steps:

1. In the navigation area, click **System resources** > **Partitions**. The Partitions page opens. Alternatively, in the navigation area, click **System resources** > **Systems**. Click the system in which the logical partition is located. The Partitions page is displayed.
2. Click the partition for which you want to view the properties. The partitions details page opens.
3. Click **Processors** in the content pane. The **Processors** page opens. The Processor mode and the available number of processors are displayed.
4. Select the required values to set the **Virtual Processors** and **Processing Units** for the logical partition. You can view the **Maximum**, **Allocated**, and **Minimum** numbers of processing units for the logical partition. Use the **Virtual Processors** slider or **Processing Units** slider to adjust the number of processors that you want to assign. This value can be set only for the partition that is running or stopped in the shared mode.
5. You can use the **Force** option to change the processor and memory value, or the physical I/O configuration for an AIX, Linux, or VIOS partition that is in running state and that does not have an RMC connection to the management console. You can use the **Force** option to change the configuration and specify a timeout value for the operation in the **Timeout (Minutes)** field. A default value of 120 minutes is used for memory remove operations, and a default value of 5 minutes is used for all other operations.
6. In the **Advanced Settings** section, you can map the capabilities of your managed system with the type and version of the operating system of the logical partition.

Use the online Help if you need additional information about processors.

Memory

The Memory page displays the properties of the running logical partition that is using the dedicated or the shared memory. To view and edit the memory details, complete the following steps:

1. In the navigation area, click **System resources** > **Partitions**. The Partitions page opens. Alternatively, in the navigation area, click **System resources** > **Systems**. Click the system in which the logical partition is located. The Partitions page is displayed.
2. Click the partition for which you want to view the properties. The partitions details page opens.
3. Click **Memory**. On the **Memory** page, you can view the properties of the running logical partition that is using the dedicated or the shared memory.
4. Assign the required amount of dedicated or shared memory to a logical partition. You can also assign the **Maximum**, **Allocated**, and **Minimum** numbers of memory for the logical partition in **GB** or **MB** memory units.

5. You can use the **Force** option to change the processor and memory value, or to change the physical I/O configuration for an AIX, Linux, or VIOS partition that are in the running state and that does not have an RMC connection to the management console. You can use the **Force** option to change the configuration and specify a timeout value for the operation in the **Timeout (Minutes)** field. A default value of 120 minutes is used for memory remove operations, and a default value of 5 minutes is used for all other operations.
6. In the **Advanced Settings**, you can configure the following settings:
   a. Click **Enable Active Memory Expansion** to expand memory on the server beyond the physical limits of the server and beyond the capacity of the true physical memory that is assigned to an AIX or a Linux partition.
   b. Specify the **Minimum**, **Allocated**, and **Maximum** number of pages of **Huge Page Memory** for the partition.

      Note: If the managed system does not have the specified number of pages of huge page memory available when you activate the partition profile, the managed system does not activate the logical partition. You can commit less huge page memory to the logical partition only by changing the value and reactivating the partition profile. The **Allocated** field specifies the number of pages that you can assign to partitions on the managed system. This number of pages specified includes the pages that are assigned to the partitions on the system.

Use the online Help if you need additional information about Memory.

Physical I/O adapters

The **Physical I/O adapters** page lists the physical location code, partner location code, and a description for each physical I/O adapter that is assigned to the logical partition.

To view and edit the **physical I/O adapter** details, complete the following steps:

1. In the navigation area, click **System resources** > **Partitions**. The **Partitions** page opens. Alternatively, in the navigation area, click **System resources** > **Systems**. Click the system in which the logical partition is located. The Partitions page is displayed.
2. Click the partition for which you want to view the properties. The partitions details page opens.
3. Click **Physical I/O adapter**.
4. Click **Add adapter** to add a physical I/O adapter to the logical partition.
5. To remove an adapter, select the physical I/O adapter from the list, click **Action** > **Remove Adapter**.
6. In the **Options** sections, you can use the Force option to change the processor and memory value, or the physical I/O configuration for an AIX, Linux, or VIOS partition that are in running state and that does not have an RMC connection to the management console.

Note:

- For an IBMi partition, you can use the Force option to remove the physical I/O configuration. Before saving the value, you can use the Force option to change the configuration and set a timeout value for the overall operation. If timeout option is not specified, a default value of 120 minutes is used for memory remove operations, and a default value of 5 minutes is used for all other operations.
- If you select to add or remove an adapter that has an associated partner adapter, by default, the partner adapter is also automatically selected to be added or removed from the partition.

Use the online Help if you need additional information about physical I/O adapters.

Operations

Operations contains the tasks for operating partitions.

About this task

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to manage operations tasks. In the content pane, click **Operations** and select the task that you want to perform from the list.

Note: With HMC Version 10.2.1040, or later you can search for a partition action that you want to perform by typing the name of the task as a keyword in the search bar that is available under the **Partition actions** menu.

Activate partition

Select the required partition profile from the list of profiles and click **Activate** to activate a partition profile on your managed system that is in the **Not Activated** state.

On the **Advanced activation settings** tab, select the **No VSI Profile** check box to activate the partition without VSI profiles.

Specify the **Boot mode** and the **Keylock position** and click **Activate**.

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.

Schedule operations

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

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

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

The Schedule 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 **Schedule operations** window you can perform the following operations:

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

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

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

Notes:

- You can specify the number of weeks or months to elapse before performing the scheduled operation again on each selected day.

- With the Hardware Management Console (HMC) Version 10.1.1020, or later, you can specify the interval to be monthly. The scheduled operation is run on the configured time and month. It is also run on the subsequent months based on the number of repetitions and monthly intervals that you have configured.
- For example, if you configure the scheduled operation for 31st of every month with five repetitions, then the scheduled operation is executed every month on 31st, and if a particular month does not have 31st then that repetition is executed on the last day of the month. For example, if you configure the scheduled operation from 31 January with five repetitions, then the operation is executed on 31 January, 28 February, 31 March, 30 April, and 31 May.

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

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

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

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

Backup I/O Configuration
Schedules a backup I/O configuration operation for a selected Virtual I/O Server.

To schedule operations on the HMC, complete the following steps:

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

Network boot

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

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

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

Restart partition

You can restart a partition and the associated partition profile by using the Hardware Management Console (HMC). Restarting a logical partition shuts down the logical partition and then starts it again.

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

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

Complete the following steps to restart partitions:

1. In the navigation area, click **System resources** > **Partitions**.

   Alternatively, you can click **System resources** > **Systems**. Click a system from the list. Click **Partitions**. The **Partitions** page is displayed.
2. Select a single partition or multiple partitions that you want to restart.
3. Click **Operations** > **Restart Partition**. The **Restart Partition** page is displayed.
4. Select one of the following options:

Dump	The HMC shuts down the logical partition and initiates a main storage or a 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. **Note:** This option is available only if the partition is in a running state or open firmware state.
Operating System	The HMC shuts down the logical partition normally by issuing the shutdown `-r` command to AIX or Linux logical partitions, and PWRDWNSYS OPTION(*CNTRLD)RESTART(*YES) command to IBM i logical partitions. After the shutdown is complete, the logical partition is immediately restarted. **Note:** This option is available in AIX or Linux systems, only if the Resource Monitoring Control (RMC) state is active. For IBM i systems, this option is available only if the partition is in a running state.
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 the data is partially updated. Use this option only after a controlled end is unsuccessfully attempted.

Operating System Immediate	The HMC shuts down the logical partition immediately by issuing the shutdown **-Fr** command to AIX or Linux logical partitions, and PWRDWNSYS OPTION(*IMMED)RESTART(*YES) command to IBM i logical partitions. After the shutdown is complete, the logical partition is immediately restarted. **Note:** This option is available in AIX or Linux systems, only if the RMC state is active. For IBM i systems, this option is available only if the partition is in a running state.
Dump Retry	The HMC retries a main storage or system memory dump on the logical partition. After the retry is complete, the logical partition is shut down and restarted. Use this option only if you have previously tried the **Dump Retry** option without success. **Note:** This option is available only in IBM i logical partition.

Note:

- For all partitions except the IBM i partition, the Resource Monitoring and Control (RMC) state must be active to select the **Operating System** or the **Operating System Immediate** options.
- It is recommended to use either the **Operating System** or the **Operating System Immediate** option to restart an IBM i logical partition. The IBM i logical partition must have the code level IBM i 7.2 TR 1 or IBM i 7.1 TR 9, or later. If these options are not available, it is recommended you issue the PWRDWNSYS OPTION(*CNTRLD) RESTART(*YES) or PWRDWNSYS OPTION(*IMMED) RESTART(*YES) command in the command-line interface of the operating system. Using the other options to restart an IBM i logical partition results in an abnormal Initial program load (IPL).

5. Confirm the partitions that you want to restart, and click **Restart**.

   Note:

   - You can view the progress of the restart operation with the progress bar and through the task notifications.
   - If the partition restart operation is not successful, an error message is displayed.

Shutdown partition

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

For IBM i logical partitions, use this page only if you cannot shut down the IBM i logical partition from the command line of the operating system. Using this page to shut down an IBM i logical partition results 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 message is displayed, indicating that you must shut down the client partitions before you shut down the VIOS partition.

Complete the following steps to shutdown partitions:

1. In the navigation area, click **System resources** > **Partitions**.

   Alternatively, you can click **System resources** > **Systems**. Click a system from the list. Click **Partitions**. The **Partitions** page is displayed.

2. Select a single partition or multiple partitions that you want to shutdown.
3. Click **Operations** > **Shutdown Partition**. The **Shutdown Partition** page is displayed.
4. Select one of 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, the shutdown operation ends 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 the data is partially updated. Use this option only after a controlled shutdown is unsuccessfully attempted.
Operating System	The HMC shuts down the logical partition normally by issuing the shutdown command to AIX or Linux logical partitions, and PWRDWNSYS OPTION(*CNTRLD) command to IBM i logical partitions. **Note:** This option is available in AIX or Linux systems, only if the RMC state is active. For IBM i systems, this option is available only if the partition is in a running state.
Operating System Immediate	The HMC shuts down the logical partition immediately by issuing the shutdown **-F** command to AIX or Linux logical partitions, and PWRDWNSYS OPTION(*IMMED) command to IBM i logical partitions. **Note:** This option is available in AIX or Linux systems, only if the RMC state is active. For IBM i systems, this option is available only if the partition is in a running state.

Note:

- For all partitions except the IBM i partition, the Resource Monitoring and Control (RMC) state must be active to select the **Operating System** or the **Operating System Immediate** options.
- It is recommended to use either the **Operating System** or the **Operating System Immediate** option to shut down an IBM i logical partition. The IBM i logical partition must have the code level IBM i 7.2 TR 1 or IBM i 7.1 TR 9, or later. If these options are not available, it is recommended you issue the PWRDWNSYS OPTION(*CNTRLD) or PWRDWNSYS OPTION(*IMMED) command in the command-line interface of the operating system. Using the **Delayed** or **Immediate** options to shut down an IBM i logical partition results in an abnormal Initial program load (IPL).

5. Confirm the partitions that you want to shutdown, and click **Shutdown**.

Note:

- You can view the progress of the shutdown operation with the progress bar and through the task notifications.

- If the partition shutdown operation is not successful, an error message is displayed.

Turn on/off LPAR attention LED

Use this task to activate or deactivate the partition attention LED for a logical partition.

To activate or deactivate the partition attention LED, select a managed partition from the table and click **Operations** > **Turn on/off LPAR attention LED**.

From the **Turn on/off LPAR attention LED** window, select **Activate Virtual LED** or **Deactivate Virtual LED** from the **Action** menu.

The system attention LED icon is indicated by a yellow triangle with an exclamation mark (!). When this icon appears, check the attention light on the physical system to verify that the LED is on:

- When the system attention LED icon appears above a server icon on the HMC interface, it indicates that a problem may exist on the selected system.
- When the system attention LED icon appears above the partition icon, it indicates that the partition requires service.

Note: Alternatively, you can turn on or turn off the partition attention LED by toggling the **LED on/off** option under **Attention LED** column in the content pane.

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

Partition Templates

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

Capture partition as a template

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

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to capture as a template, and click **Operations** > **Capture partition as a template**.
3. Enter a template name and description.
4. Click **OK**.

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

Delete partition

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

The Delete partition 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.

Update VIOS

Use this task to update VIOS from the HMC. You can select the source from where the VIOS image file needs to be copied. You can also save the downloaded image file for future use.

About this task

Note:

- This task might require the virtual I/O server to be rebooted. You can select the **Restart the VIOS if required** checkbox to reboot the system.
- You cannot save more than three image files at a time.
- Virtual I/O Server update operation can take up to two hours to complete.

To update VIOS, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then click **Virtual I/O servers**.
2. Select a virtual I/O server from the list.
3. Click **Operations** and from the menu, click **Update VIOS**.
   - To update the VIOS image file from an HMC, complete the following steps:
     a. Select **HMC** as the image file location.
     b. Choose an image from the displayed list.
   - To update the VIOS image file from a remote server, complete the following steps:
     a. Select **Remote Server** as the update image file location.
     b. Select **NFS Server** or **SFTP Server** as the server type.
     c. Enter the required details.
     d. Select the **Save update image to HMC** checkbox to save the downloaded update image file for future use. Provide a name for the update image file.

        The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   - To update the VIOS image file from the IBM website, complete the following steps:
     a. Select the **IBM website** as the update image file location.
     b. Select an update file image from the displayed list.
     c. Select the **Save update image to HMC** checkbox to save the downloaded update image file for future use.
   - To update the VIOS image file from a USB device, complete the following steps:
     a. Select **USB** as the update image file location.
     b. Select a USB device from the **USB Input** list.
     c. Enter the required details.
     d. Select the **Save update image to HMC** checkbox to save the downloaded update image file for future use. Provide a name for the update image file.

        The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
4. Click **Update**.

Upgrade VIOS

About this task

Use this task to upgrade Virtual I/O Server (VIOS) from the Hardware Management Console (HMC). You can select the source from where you need to copy the VIOS image file. You can also save the downloaded VIOS image file for future use.

What to do next

Notes:

- Ensure that the VIOS has a minimum memory of 10 GB.
- Ensure that the HMC has sufficient disk space to save the new VIOS image file. You can remove the old installation images to free-up extra memory.
- The **Upgrade VIOS** operation is available only when the VIOS is in the running state with an active Resource Monitoring and Control (RMC) connection.
- Before you run the **Upgrade VIOS** operation, make sure that you rename the VIOS that has volume groups with *altinst_rootvg* or *old_rootvg* names.
- The upgrade VIOS operation can take up to two hours to complete.

1. In the navigation area, click **System resources** > **Virtual I/O servers**.
2. Select a partition from the table. The **VIOS properties** page is displayed.

   Note: Alternatively, you can select a partition from the table and click **Operations** > **Upgrade HMC**.
3. Click **Virtual IO Server actions** and from the menu, click **Upgrade VIOS**. The **Upgrade VIOS** window opens.
4. In the **Choose disk space** step, select a disk from the displayed list.
5. Click **Next** to view the **Choose image location** step.
   a. To upgrade the VIOS image file from an HMC, complete the following steps:
      i) Select **HMC** as the image file location.
      ii) Select an image from the displayed list.
   b. To upgrade the VIOS image file from a remote server, complete the following steps:
      i) Select either **NFS Server** or **SFTP Server** as the server type.
      ii) Enter the details such as **Remote server hostname or IP address**, **Mount location**, **username**, and **password**.
      iii) Select the **Save install image to HMC** checkbox to save the downloaded upgrade image file for future use. Provide a name for the upgrade image file.

      Note: The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-), and the underscore (_) characters.
   c. To upgrade the VIOS image file from a USB device, complete the following steps:
      i) Select **USB** as the location for the upgrade image file.
      ii) Select a USB device from the **USB Input** list.
      iii) Enter the details such as **Remote server hostname or IP address**, **Mount location**, **username**, and **password**.
      iv) Select the **Save install image to HMC** checkbox to save the downloaded upgrade image file for future use. Provide a name for the upgrade image file.

      Note: The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-), and the underscore (_) characters.
6. Click **Next**. The **Summary** step displays the chosen disk space and upgrade image files.
7. Click **Upgrade**.

Validate Maintenance Readiness and Prepare

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

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

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

You can click **Prepare for Maintenance** in the upper-right corner of the **Validate Maintenance Readiness** window to prepare the VIOS for maintenance. You can select the **Continue with prepare even if there are errors/warnings** checkbox to prepare the VIOS for maintenance even when there are errors and warning.

The **Prepare for Maintenance** task unconfigures the virtual SCSI and virtual Fibre Channel devices in the VIOS to switch the path of the redundant virtual SCSI and the virtual Fibre Channel storage. It also changes the high availability mode of the redundant Shared Ethernet Adapter (SEA) of the VIOS to the Standby state. This task also performs the failover of the vNIC by activating the vNIC backing device that is on an another VIOS. Any failures during these steps are reported at the end of the procedure.

You can click **View System VIOS** in the upper-right corner of the **Validate Maintenance Readiness** window to view information about the Virtual I/O Server of the managed system.

Console

Console contains the tasks to open a virtual terminal window or close a virtual terminal connection for AIX or Linux logical partitions.

About this task

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to manage console tasks. In the content pane, click **Console** and select the task that you want to perform from the list.

Open terminal window

Use this task to open an HMC virtual terminal window locally.

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to open a virtual terminal window, and click **Console** > **Open terminal window**. The virtual terminal window opens.
3. You can modify the font name or font size used in the virtual terminal window by selecting the options from the **Font Name** or **Font Size** lists.

Close terminal connection

Use this task to close a virtual terminal connection.

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to close the virtual terminal connection, and click **Console** > **Close terminal connection**. This option terminates the already opened virtual terminal session.

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.

Validate and Migrate

You can validate the settings for moving the partitions from the source system to the destination system by using the HMC. You can also migrate partitions to another managed system.

To validate and migrate partitions to another system in the HMC Version 10.3.1050, or later, complete the following steps:

1. In the navigation area, click **System resources** and then select **Systems**.
2. In the content pane, select the system and click **Partitions**. Alternatively, you can directly access the partitions by clicking **System resources** > **Partitions**.
3. In the content pane, select the partitions that you want to validate and migrate to another system.
4. Click **Mobility** > **Validate and Migrate**. The **Migrate Partitions** wizard opens.
5. Complete the steps for validation and migration in the **Migrate Partitions** wizard.

Recover

Recover this partition from a migration that did not complete.

About this task

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

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select the system and click **Partitions**. Alternatively, you can access the partitions directly by clicking **System resources** > **Partitions**.
3. In the content pane, select the partition that you want to recover.
4. Click **Mobility** > **Recover**. The Migration Recovery window opens.
5. Complete the information as necessary and click **Recover**.

Validate

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

About this task

To validate the settings for moving the partition from the source system to the destination system in HMC Versions 10.2.1030 and 10.2.1040, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select the system and click **Partitions**. Alternatively, you can access the partitions directly by clicking **System resources** > **Partitions**.
3. In the content pane, select the partition for which you want to validate the settings.
4. Click **Mobility** > **Validate**. The Partition Migration Validation window opens.
5. Fill in the information in the fields, and click **Validate**.

Migrate

Migrate a partition to another managed system.

About this task

To migrate a partition to another system in HMC Versions 10.2.1030 and 10.2.1040, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select the system and click **Partitions**. Alternatively, you can access the partitions directly by clicking **System resources** > **Partitions**.
3. In the content pane, select the partition that you want to migrate to another system.
4. Click **Mobility** > **Migrate**. The Partition Migration wizard opens.
5. Complete the steps in the Partition Migration wizard and click **Finish**.

Profiles for HMC Version 10.3.1060.0, or later

You can manage the partition profiles for your logical partitions by using the Hardware Management Console (HMC). You can change the resource specifications that are stored in your partition profiles as your needs change.

About this task

A partition profile is a record on the Hardware Management Console (HMC) that specifies a possible set of resource allocations and activation settings for a logical partition. To activate a logical partition, you must activate one of the partition profiles for that logical partition. The managed system uses the partition profile to configure the resources for the logical partition. The partition profile is a separate entity from the logical partition. Changing the partition profile properties does not automatically change the resource allocations for an active logical partition. Similarly, changing the resource allocations for an active logical partition does not automatically change the properties for any partition profile.

Use the **Partition profiles** page to complete the following tasks:

- Create new partition profiles.
- Create a copy of a partition profile.
- View the properties of a partition profile. From this task, you can view or edit an existing partition profile. You can modify the processor, memory, and adapter assignments for a profile by editing the profile
- Set a default partition profile.
- Save the current configuration of a logical partition to a new partition profile. This procedure is useful if you change the configuration of a logical partition using dynamic logical partitioning and you do not want to lose the changes when you restart the logical partition. You can perform this procedure at any time after you initially activate a logical partition.
- Delete a partition 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.
- Activate a partition profile.

Complete the following steps to access the **Partition profiles** page:

1. In the navigation area, click **System resources** > **Partitions**. The **Partitions** page opens.

   Alternatively, in the navigation area, click **System resources** > **Systems**. Click the system in which the logical partition is located. The **Partitions** page is displayed.
2. Click **Partition profiles** in the content pane. The **Partition profiles** page opens.

Alternatively, select the partition for which you want to manage profiles, and then click **Profiles** > **Manage profiles**. The **Partition profiles** page opens.

Profiles for HMC Version 10.3.1050.0, or earlier

Learn about the tasks that are available in the **Profiles** menu for HMC Version 10.3.1050.0, or earlier.

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.

Change Default Profile

Change the default profile for the partition.

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

Manage profiles

Use the **Partition profiles** page 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, logical ports, power control, 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.

Select **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.

Delete Partition

You can delete a partition and the associated partition profile by using the Hardware Management Console (HMC). A partition can be deleted from either a single system or multiple systems. When you delete a partition, all hardware resources that are assigned to that partition become available to other partitions.

Note:

- You cannot delete a partition if it is the service partition of your managed system.
- To delete a partition, ensure that it is in the **Not activated** state. If the partition is in a Running state, shutdown the partition and then delete the partition.

Complete the following steps to delete partitions:

1. In the navigation area, click **System resources** > **Partitions**.

   Alternatively, you can click **System resources** > **Systems**. Click a system from the list. Click **Partitions**. The **Partitions** page is displayed.
2. Select a single partition or multiple partitions that you want to delete.
3. Click **Operations** > **Delete Partition**. The **Delete Partition** page is displayed.
4. Confirm the partitions that you want to delete, and click **Delete**.

   Note:

- **Clean up associated virtual I/O server mappings** and **Delete associated virtual disks** options are only applicable for VIOS.
- By default, both **Clean up associated virtual I/O server mappings** and **Delete associated virtual disks** options are selected.

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

Serviceability

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

These problems are reported to you as serviceable events. Use the **Serviceable events** 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 events** task to report the problem to your service provider.

Manage serviceable events

Problems on your managed partitions are reported to the Hardware Management Console (HMC) as serviceable events. You can view the problem, manage problem data, call home the event to your service provider, or repair the problem.

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system for which you want to manage serviceable events.
3. Click **System actions** > **Service** > **Manage serviceable events**.
4. Provide event criteria, error criteria, and FRU criteria. If you do not want the results that are filtered, select **ALL**. Click **Refresh** to refresh the list of serviceable events based on the criteria filter values.

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

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

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

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

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

- **Add PMH Comment**: Add a comment to a PMH for a selected serviceable event. If a PMH number does not exist for a given problem, the Add PMH Comment option is not available.

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

Reference code log

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

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

Control Panel Functions

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

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

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

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

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

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

Virtual I/O

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

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

Virtual networks

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

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

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to manage virtual networks, and then click **Virtual networks** from the partition details page.

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

Virtual NICs

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

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

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

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

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to manage virtual NICs, and then click **Virtual NICs** from the partition details page.

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

Virtual storage

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

To view the virtual storage capacity of a partition by using the Hardware Management Console (HMC), complete the following steps:

1. In the navigation area, click **System resources** > **Partitions**.
2. Select a partition to view the **Partition properties** page.
3. Click **Virtual storage**.

Note:

- In the Virtual Storage work panel, you can use the left and right arrow key buttons to switch between the Storage and Adapter views.
- You can add virtual storage resources to a partition. You can use the Adapter View to create and view the adapter configuration of the virtual storage devices that are allocated for the logical partition.
- Click **Storage View** to view and manage the storage capability of the logical partition.

Virtual SCSI

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

You can add the virtual storage resources to a partition.

1. Click **Adapter View** to create, view the adapter configuration of the virtual storage devices that are allocated for the logical partition.
2. Click **Storage View** to view and manage the storage capacity of the logical partition.

Physical Volume

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

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

You can perform actions such as **View Device Mapping**, **Modify Connections**, **Rename Device** and **Remove** in the Virtual SCSI panel.

1. To perform each action, select a **Virtual Target Device** > **Action**.
2. To rename the virtual target device, select **Action** > **Rename Device** and change the name in the **New Virtual Target Device Name** option. Click **Ok**.
3. To remove the virtual target device, select **Action** > **Remove**. Click **Ok**.

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

Virtual Fibre Channel

You can view virtual Fibre Channel resources that are assigned to the logical partition of the PowerVM configuration. The physical port on each physical Fibre Channel adapter is identified using a Worldwide Port Name (WWPN). The virtual Fibre Channels that are assigned to the PowerVM configuration are displayed. You can add the required type of virtual Fibre Channel to a partition.

You can perform actions such as **View Device Mapping**, **Remove**, **Log In** and **Log Off** in the Virtual Fibre Channel panel.

1. Select a **Virtual I/O server** on which you want to perform an action.
2. To view the device mapping of a virtual I/O server, click **Action** > **View Device Mapping**.
3. To remove a virtual I/O server, click **Action** > **Remove** > **Ok**.
4. To log in to WWPN, click **Action** > **Log In**.
5. To log out of WWPN, click **Action** > **Log Off**.

Virtual Optical Device

You can view the virtual optical devices that are available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

You can perform actions such as **View Device Mapping**, **Load and Unload of Virtual Optical Medians**, **Rename Device** and **Remove** in the Virtual Optical Device panel.

1. Select a **Device** on which you want to perform an action.
2. To check the virtual optical device association with the VIOS, click **Action** > **View Device Mapping**.
3. To load the virtual optical media from the media repository, click **Action** > **Load**.
4. To unload the virtual optical media from the virtual optical device, click **Action** > **Unload**.
5. To rename the virtual optical device, click **Action** > **Rename Device**.
6. To remove the virtual optical device that is associated with the logical partition, select **Action** > **Remove**.

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

Hardware virtualized I/O

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

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

1. In the navigation area, click **System resources**, and then select **Partitions**.
2. Select the partition for which you want to manage serviceability tasks and click **Hardware virtualized I/O** in the partition details page.
3. You can add an SR-IOV logical port to the partition or change the settings of the SR-IOV logical ports. In the **SR-IOV logical port** table, you can also view the information about the logical ports that can be migrated and the information about the backing device that is configured for the logical ports.

   Notes:

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

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

Tags

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

Tags may be nested to create customized system resources view.

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

To create a new group, complete the following steps:

1. In the navigation pane, click **System resouces** > **Tags** > **Create tags**.
2. In the **Create tags** window, specify a tag name and description for the tag.
3. Select one or more resources (example: servers, partitions, or Virtual I/O Servers) that you want to include in the tag that you want to work with.
4. Click **Add** to save the changes and to close the window.

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

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

Power enterprise pools

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

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

- Add processors or memory to a server.

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

Templates and OS Images

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

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

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

To access the Template Library, complete the following steps:

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

System Templates

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

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

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

Partition Templates

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

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

Notes:

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

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

VIOS Images

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

You can access the following tasks:

Manage Virtual I/O Server Images

You can import Virtual I/O Server (VIOS) images from a DVD, a USB, or a remote server and store the images on the HMC. The stored VIOS images can be used for VIOS installation. You must be an HMC super administrator (hmcsuperadmin) to install the VIOS image.

About this task

To manage or to import the VIOS image repository, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, select the **VIOS Images** tab, and then click **Manage Virtual I/O Server Images**.
3. In the **Virtual I/O Server Image Repository** window, click **Import New Virtual I/O Server Image**.
4. In the **Import Virtual I/O Server Image** window, choose to import the VIOS images from a DVD, USB device, or a file system.
   - To import VIOS images from a DVD to the HMC, complete the following steps:
     a. In the **Import Virtual I/O Server Image** window, select **Management console DVD**.
     b. In the **Name** field, enter the name of the VIOS image that you want to import from the DVD.
   - To import VIOS images from a USB device to the HMC, complete the following steps:
     a. In the **Import Virtual I/O Server Image** window, select **Management console USB**.

b. In the **Name** field, enter the name of the VIOS image that you want to import from the USB device.

c. In the **USB Partition** list, select your USB device.

- To import VIOS images from a Network File System (NFS), File Transfer Protocol (FTP), or Secure Shell File Transfer Protocol (SFTP), complete the following steps:

  a. In the **Import Virtual I/O Server Image** window, select **File System**.

  b. Select **Remote NFS Server**, **Remote FTP Server**, or **Remote SFTP Server**.

  c. Enter the required details.

5. Click **OK**.

Manage Virtual I/O Server Backups

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

About this task

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

Procedure

1. In the navigation area, click **System resources**, and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, select the **VIOS Images** tab, and then click **Manage Virtual I/O Server Backups**.
3. In the **Manage Virtual I/O Server Backups** window, select the **Virtual I/O Server Configuration Backup** tab. A table is displayed that lists all the backup files of the VIOS configuration that is taken by the HMC. Additionally, you can view the time at which the configuration file was last edited.

   a) To take the backup of the input/output configuration file of a VIOS, click **Backup I/O configuration**. In the **Backup I/O configuration** window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

   You can enable the **Overwrite Existing File** checkbox to overwrite the existing file name.

   The file name that you specify must consist of 1 - 40 characters including file extension **`.tar.gz`**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

   b) To rename an existing backup file that is stored in the HMC, select a configuration file from the table and click **Action** > **Rename**.

   The file name that you specify must consist of 1 - 40 characters including file extension **`.tar.gz`**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

   c) To restore the VIOS input/output configuration, select a backup file which contains the I/O configuration of the VIOS that you want to restore, and click **Action** > **Restore**.

   Note: This action might require the Virtual I/O Server to be rebooted. You can select the **If required, reboot Virtual I/O Server** checkbox to reboot the VIOS.

   The file name that you specify must consist of 1 - 40 characters including file extension **`.tar.gz`**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

   d) To export the VIOS backup files to the remote system, select one or more backup files that are saved on the HMC. Click **Action** > **Export** and then complete the following steps:

   i) Specify credentials of the remote server where backup files are copied.

   ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

e) To import the backup files from the remote system, click **Import** and then complete the following steps:

i) Specify credentials of the remote server, and then select the VIOS where backup files are imported.

ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

4. In the **Manage Virtual I/O Server Backups** window, click the **Virtual I/O Server Backup** tab. A table is displayed that list all the VIOS image backup that are taken in the HMC. You can also view the name and size of the VIOS image, the time when the VIOS image file was last edited, the managed system and the VIOS from which the image was captured.

a) To take the backup of the VIOS image, click **Create Backup**. In the **Create Backup** window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

The file name that you specify must consist of 1 - 40 characters including file extension **.tar**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

You can enable the **Overwrite Existing File** checkbox to overwrite the existing file name. You can select **NIMOL resources**, **Media repository content**, and **Volume groups structure** to include the selected resources into your backup file.

b) To rename an existing VIOS image backup file that is stored in the HMC, select a backup file from the table and click **Action** > **Rename**.

The file name that you specify must consist of 1 - 40 characters including file extension **.tar**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

c) To remove a VIOS image backup file from the HMC, select a backup file which contains the VIOS configuration that you want to remove from the table, and click **Action** > **Remove**.

d) To export the Virtual I/O Server backup files to the remote system, select one or more backup files that are saved on the HMC. Click **Action** > **Export** and complete the following steps:

i) Specify credentials of the remote server where backup files are copied.

ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

e) To import the backup files from the remote system, click **Import** and complete the following steps:

i) Specify credentials of the remote server, and then select the target Virtual I/O Server where backup files are imported.

ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

5. In the **Manage Virtual I/O Server Backups** window, click the **Shared Storage Pool Cluster Backup** tab. A table is displayed that lists all the VIOS image backups that are taken in the HMC. Additionally, you can also view the **Managed System, Virtual I/O Server**, and **Backup Created time**.

a) To take a backup of the VIOS Shared Storage Pool Cluster (SSP) configuration, click **Backup SSP Cluster Configuration**. In the **Backup SSP Cluster Configuration** window, select the managed system and the Virtual I/O Server that the backup is created for, and then specify a name for it.

The file name that you specify must consist of 1 - 40 characters including file extension **.tar.gz**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

You can enable the **Overwrite Existing File** checkbox to overwrite the existing file name.

b) To restore the Shared Storage Pool Cluster configuration, select the backup file that contains the configuration of the SSP cluster that you want to restore, and click **Action** > **Restore**.

Note: This action might require the Virtual I/O Server to be rebooted. You can select the **If required, reboot Virtual I/O Server** checkbox to reboot the VIOS.

c) To rename one of the existing SSP cluster configuration backup files, select a configuration from the table and click **Action** > **Rename**.

The file name that you specify must consist of 1 - 40 characters including file extension **.tar.gz**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

d) To remove the SSP cluster configuration backup, select a backup file which contains the SSP cluster configuration that you want to remove, and click **Action > Remove**.

e) To export the Virtual I/O Server backup files to the remote system, select one or more backup files that are saved on the HMC. Click **Action** > **Export** and complete the following steps:

i) Specify credentials of the remote server where the backup files are copied.

ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

f) To import backup files from the remote system, click **Import** and complete the following steps:

i) Specify credentials of the remote server, and then select the target Virtual I/O Server where the backup files are imported.

ii) Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

6. Click **Apply**.

Manage Virtual I/O Server Updates

With HMC version 10.2.1030, or later, you can manage the Virtual I/O Server (VIOS) updates. You can use the update image files that are available on the HMC or copy the VIOS update image files that are uploaded on other resources to the HMC. You can rename the existing VIOS update image file name or delete the older update image files to free up disk space.

About this task

To manage the VIOS update images that are stored in the HMC, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Templates and OS Images**.
2. From the **Templates and OS Images** window, select the **VIOS Images** tab, and then click **Manage Virtual I/O Server Updates**.
3. In the **Manage Virtual I/O Server Update Images** window, the **Virtual I/O Server Update Images** tab displays the list of all the VIOS image files that are stored in the HMC.

a) To rename an existing image file that is stored in the HMC, select a file from the table and click **Action** > **Rename**.

The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

b) To remove one or more VIOS image files from the HMC, select the files from the list and click **Action** > **Remove**.

c) To import the image files from a remote system, click **Import**. In the **Copy Update Image** window, you can copy and import the VIOS image file from the NFS server, SFTP Server, or a USB device.

- To import VIOS image files from the NFS server to the HMC, complete the following steps:

i) In the **Copy VIOS image** window, select **NFS Server**.

ii) In the **Name** field, enter the VIOS update image file name that you want to import.

iii) Enter the required details.

- To import VIOS images from the SFTP server to the HMC, complete the following steps:

i) In the **Copy VIOS image** window, select **SFTP Server**.

ii) In the **Name** field, enter the VIOS update image file name that you want to import.

iii) Enter the required details.

- To import VIOS images from a USB device to the HMC, complete the following steps:

i) In the **Copy VIOS image** window, select **USB**.

ii) In the **Name** field, enter the VIOS update image file name that you want to import.

iii) Enter the required details.

Note: The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

4. Click **Apply**.

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.

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 that are assigned to your user ID, you might not have access to all the tasks. See Table 3 on page 7 for a listing of the tasks and the user roles that are allowed to access them.

HMC settings

You can view the HMC information and change the HMC settings.

1. In the navigation area, click **HMC management**.
2. In the content pane, click **HMC settings**.
3. You can view the HMC information under the **HMC details** section.
4. You can update the following settings for the HMC:

HMC settings

You can configure the following user settings:

- **Idle Time Out** : Specify idle time out settings for an HMC session in minutes.
- **Session Time out**: Specify session time out settings for an HMC session in minutes.
- **Max Web UI Login Attempts** : Specify the maximum number of failed login attempts that are allowed within the login suspend time before your user account is temporarily suspended and disabled from logging in to the HMC. The suspension lasts for the login suspend time. You can enter the maximum number of login attempts in the range 3 - 50.

  Note: For HMC Version 10.3.1050.0, or later, this field is displayed as **Maximum login attempts**.
- **Web UI Suspend Time**: Specify the number of minutes for which a user account is suspended after the maximum number of failed login attempts is reached within this same amount of time. You can enter a value in the range 1 - 1440 minutes. After the maximum number of failed login attempts is reached, the account is suspended for the number of specified minutes in the `Web UI Suspend Time` field.

  Note: For HMC Version 10.3.1050.0, or later, this field is displayed as **Login suspend time**.

With HMC Version 10.3.1060.0, or later, you can configure the following user settings:

- **Maximum webui sessions per user**: Specify the maximum number of web user interface sessions that are allowed for a logged in user. By default, 100 web user interface sessions are allowed for a user. The value for maximum webui sessions ranges between 50-200.
- **Console maximum webui session**: Specifies the maximum number of web user interface sessions that are allowed in the HMC. By default, 1000 web user interface sessions are allowed in the HMC. This is a read-only parameter that cannot be modified.

Note: Web user interface sessions include sessions that are created through both graphical user interface (GUI) and REST API.

Certificate validity
You can specify the number of days for which the certificate is valid.

Remote control
You can configure the following options for the remote control:

- **Remote web access**: You can allow the HMC to be accessed at a remote workstation through a web browser.
- **Remote virtual terminal connections**: A Remote Virtual Terminal connection is a terminal connection to a logical partition from another remote HMC. You can use this task to enable Remote Virtual Terminal access for remote clients.
- **Remote command execution through SSH**: You can enable remote command execution by using the ssh facility.

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

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

Note: A maximum of 8192 characters is allowed.

Globalization setting
You can specify the language and locale and date and time for the HMC.

Note: The HMC must be rebooted for Language and locale, Date, and time changes to take effect

Language and locale

This task sets the language and location for the HMC. After you select a language, you can select a locale that is associated with that language.

The language and locale settings determine the language, the character set, and other settings specific to the country or region (such as formats for date, time, numbers, and monetary units). Changes that are made in the **Language and locale** section 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.

Date and time

Change the date and time of the battery-operated Hardware Management Console (HMC) clock and add or remove time servers for the Network Time Protocol (NTP) service.

Use this task in the following situations:

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

Note: The time setting adjusts automatically for Daylight Saving Time in the time zone that you select.

5. Click **Save** when you complete this task.

Network Settings (for HMC Version 10.3.1061.0, or later)

You can view the current network information for the HMC and modify network settings.

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Network Settings**.

3. In the **Network settings** page, you can view and modify the following options:

   Console identification
   Displays the console name and domain name.

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

   LAN adapters
   Displays a summarized list of all (visible) local area network (LAN) adapters. You can select a LAN adapter from the list and click the edit icon to open a window to modify addressing, routing, other LAN adapter characteristics, and firewall settings.

   Bond adapters
   You can create or delete a Bond LAN adapter. A Bond LAN adapter combines two Ethernet interfaces into a single logical link. To change the settings of the Bond LAN adapter, click the edit icon. You can change the IP address, IP network mask, gateway, and firewall settings of the Bond LAN adapter.

   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** as the option.

4. Click **Save** 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.

Network Settings (for HMC versions between 10.2.1030.0 and 10.3.1060.0)

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

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Network Settings**.
3. From the **Customize Network Settings** window, you can work with the following tabs:

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

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

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

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

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

The **Gateway address** is the route to all networks. The default gateway address (if defined) informs this HMC where to send data if the target station does not reside on the same subnet as the source. If your p10jauhine 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.

Network diagnostic information

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 **HMC management**.
2. In the content pane, click **Network diagnostic information**.
3. From the **Network diagnostic information** 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.

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 **HMC management**.
2. In the content pane, click **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.

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:

- User profiles data
  - User identification
  - Authentication methods
  - Resource roles and task roles that are managed by the user
  - Logon session properties
  - Remote access settings

  Note: When you configure **User profiles data**, the auto manage authentication method is not considered for data replication as the user will be generated at the secondary HMC automatically during the authentication process.
- Group data
  - All user-defined group definitions

  Note: When you configure **Group Data**, the complete group data is transferred from the source HMC and replaced on the secondary HMC. If the secondary HMC does not have a resource that is part of a group, the resource is not shown in that particular group.
- Multi-Factor Authentication data
  - PowerSC MFA hostname that is used by the HMC for Multi-Factor Authentication.
- Kerberos configuration data
  - Key Distribution Center (KDC), realm, and hostname that is used by the HMC for Kerberos authentication
- LDAP configuration data

  - LDAP server name and distinguished name tree that is used by the HMC for LDAP authentication.
  - Configured attributes of LDAP (such as hmcuserpropsattribute, automanage, searchfilter, scope, groupattribute, and memberattribute)
- Password policy configuration data
  - Password policy name
  - Password policy description
  - Configured attributes of the password policy (such as min_pwage, pwage, min_length, hist_size, warn_pwage, min_digits, min_uppercase, min_lowercase, and min_special_chars)
- Outbound connectivity data
  - Information for dialing out (such as whether to enable the local system as a call-home server, or whether to allow dialing to use the local modem, the dial prefix, or phone numbers)

Note: Customizable console data is accepted from other HMCs only after specific HMCs and their associated allowable customizable data types are configured.

To manage data replication, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Data replication**.
3. From the **Configure Customizable 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.

Licenses

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

You can view the licenses at any time.

With HMC 10.3.1061.0, or later, to view licenses, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, you can either click **Third party license agreement** or **Additional license agreement** to view more information.

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

With HMC 10.3.1060.0, or earlier, to view licenses, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Licenses**.
3. Click any of the license links to view more information.

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

HMC certificates

Use this task to manage the certificates used on your Hardware Management Console (HMC). It provides the capability of getting information on the certificates that are used on the console. You can 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 that is required for all remote access to the HMC, a certificate is required to provide the keys for this encryption. The HMC provides a self-signed certificate that allows this encryption to occur.

To manage your certificates by using HMC 10.3.1061.0, or later, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **HMC certificates**. The **HMC certificate** page opens. This page displays the HMC certificate that is enabled on the HMC and also the archived certificate if it is available.
3. In the **HMC certificate** section, click **Actions** and select any of the following options to manage HMC certificates:
   - **View issuer**: You can view all HMC certificates with hierarchy. You can view the issuer details used to sign the certificate in use by the HMC.
   - **Edit**: You can modify the existing certificate information that is enabled for the console.

     Note: You cannot edit a certificate that is signed by a certificate authority (CA). You can edit a self-signed certificate or create a new certificate.
   - **Create**: You can create a new HMC certificate that will be enabled for the console. You can choose between a self-signed and CA-signed certificate.
   - **Import certificate**: You can import a server certificate or signing certificate files that are received from the CA to the HMC from the following locations:
     - **Local filesystem**: You must upload the HMC certificate file. Optionally, you can also upload the signing certificate files in the order of intermediate certificate first, followed by the root certificate.
     - **HMC**: You must specify the CA-signed certificate name. Optionally, you can also specify the signing certificate names in the order of intermediate certificate first, followed by the root certificate.
     - **SFTP server**: You must specify the CA-signed certificate name. Optionally, you can also specify the signing certificate names in the order of intermediate certificate first, followed by the root certificate.

     Click **Import** to complete the operation.

     Note: HMC will restart to import the HMC certificate.
   - **Import repository**: You can import a certificate repository to the HMC.
   - **Archive**: You can archive a certificate or delete it from the current status.

     Note: You can reuse the archived certificate in future.
4. The **Archived certificate** section displays the archived certificate if available. Click **Actions** and select any of the following options to manage the archived certificates:
   - **View issuer**: You can view all HMC certificates with hierarchy. You can view the issuer details used to sign the archived certificate.
   - **Apply**: You can apply the displayed archived certificate as the HMC certificate.

To manage your certificates by using HMC 10.3.1060.0, or earlier, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **HMC certificates**.
3. Use the menu bar from the **Certificate Management** window for the actions that you want to take with the certificates:
   - To create a new certificate for the console, click **Create**, then select **New Certificate**. Determine whether your certificate will be self-signed or signed by a Certificate Authority (CA), then click **OK**.
   - To modify the property values of the self-signed certificate, click **Selected**, then select **Modify**. Make the appropriate changes, then click **OK**.

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

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

- To work with existing and archived certificates or signing certificates, click **Advanced**. Then you can choose the following options:
  - Delete existing certificates
  - Work with archived certificates
  - Import certificates
  - View issuer certificates

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

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

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

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

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

Update HMC

Learn how to update the internal code of the Hardware Management Console (HMC).

To update the HMC, complete the following steps:

1. In the navigation area, click **HMC management** > **HMC actions** > **Update HMC**. The **Update HMC** page opens.
2. Follow the steps in the **Update HMC** page to complete the update HMC operation.

Note: If the HMC update operation requires a restart, click **Restart the HMC if required**.

Use the online Help if you need additional information about updating the HMC.

Upgrade HMC

About this task

Learn how to upgrade the Hardware Management Console (HMC) data.

To upgrade the HMC, complete the following steps:

Procedure

1. In the navigation area, click **HMC management**.
2. In the work pane, click **HMC actions** > **Upgrade HMC**. The **Upgrade HMC** window opens.
3. In the **Save HMC upgrade data** step,
   a. Select one of the following options for restoring the data:
      - **Save HMC upgrade data and restore after upgrade:** You can save the configuration data. This data will be restored after the HMC upgrade process completes. The HMC configuration data consists of files that were created or customized with the current software level. You can also save the HMC data on a media before upgrading the HMC.
      - **Do not save HMC upgrade data (clean install):** You can skip to save the HMC upgrade data if the configuration data is not needed after the upgrade operation.

   b. Select one of the following location options to save the HMC upgrade data:
      - **HMC only:** You can save the HMC configuration data to a nonvolatile area on the HMC hard disk drive.
      - **FTP server:** You can save the HMC configuration data to an FTP remote server.

        Note: This option is displayed as **HMC and FTP server** in HMC Version 10.3.1050.0.
      - **SFTP server:** You can save the HMC configuration data to an SFTP remote server.

        Note: This option is displayed as **HMC and SFTP server** in HMC Version 10.3.1050.0.
      - **USB** You can save the HMC configuration data to a Universal Serial Bus (USB) device.

        Note: This option is displayed as **HMC and USB** in HMC Version 10.3.1050.0.

   Note: With HMC Version 10.3.1050.0, you must click **Save HMC upgrade data** to save the configuration data. This additional step is not needed if you are using HMC Version 10.3.1060.0, or later.
4. Click **Next**.
5. In the **Download upgrade files** step, you can download the network installation files for the HMC upgrade operation. You can select the location from where you want to download the files from the following options:
   - **HMC server:** You can download the upgrade files from the HMC directory by entering the location where the network installation files are saved. If files are saved in the home directory, you can leave the HMC directory field blank.
   - **FTP server:** You can download the HMC upgrade files from the remote FTP server. Enter the FTP server hostname or IP address, User ID, and Password to download the HMC upgrade files.
   - **SFTP server:** You can download the HMC upgrade files through the SFTP server. Enter the SFTP server hostname or IP address, User ID, and Password to download the HMC upgrade files. Also select an **Authentication type**. The Authentication type field is available only when the SFTP

protocol type is selected. You can choose password-based authentication or Secure Shell (SSH) key-based authentication.

- **NFS server:** You can download HMC upgrade files through the NFS server. Enter the NFS server hostname or IP address and Mount location to download upgrade files.
- **IBM website:** You can download the HMC update files from the IBM website. The IBM website option allows the HMC to contact the IBM service website and directly download service files from the location.

  Note: IBM website option is available only with HMC Version 10.3.1060.0, or later.

Note: With HMC Version 10.3.1050.0, you must click **Download upgrade files** to download the HMC upgrade files from the selected location. This additional step is not needed if you are using HMC Version 10.3.1060.0, or later.

6. Click **Next**.
7. In the **Summary** step, the summary information of the following choices is displayed:
   - Restored data settings and saved location of HMC upgrade data
   - Downloaded location and server hostname or IP address of downloaded upgrade files

   Note: The list of users who are using the HMC is displayed in the table.
8. Click **Restart HMC and upgrade**. HMC will restart after the upgrade operation is completed.

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 **HMC management**, and then select **HMC actions** > **Shut down or Restart**.
2. From the **Shut Down or Restart** window, you can:
   - Select **Restart the HMC** to automatically restart the HMC once the shut down has occurred.
   - Do not select **Restart the HMC** if you do not want to automatically restart the HMC.
3. Click **OK** to proceed with the shut down, otherwise click **Cancel** to exit the task.

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

Backup HMC data

You can back up or archive the data that is stored on your Hardware Management Console (HMC) hard disk that is critical to support HMC operations.

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

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

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

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

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

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

1. In the navigation area, click **HMC management**, and then select **HMC actions** > **Backup HMC data**. The **Backup HMC data** window opens.
2. Select the **Exclude Network data** option to exclude network-related files in the backup data.

   Note: This option is not available in HMC version 10.3.1060.0, or later.
3. Select the **Include Performance and Capacity Monitoring (PCM) data** option to back up the performance and capacity monitoring data that is collected for the managed system.
4. Choose the archive option that you want to use, and follow the instructions that are associated with that option.
5. For HMC Version 10.3.1050.0, or earlier, click **OK** to continue with the backup process. For HMC Version 10.3.1060.0, or later, click **Backup** to compete the backup process.

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

Note:

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

Restore HMC data

You can select a remote repository for restoring critical backup data for the HMC.

For HMC Version 10.3.1060.0, or later, complete the following steps to restore the HMC data:

1. In the navigation area, click **HMC management**.
2. In the work pane, click **HMC actions** > **Restore HMC data**. The **Restore HMC data** window opens.
3. In the **Restore file location** step, select **Restart HMC after download** to automatically restart the HMC after the download is completed to restore the data.
4. Next, select a file location from the following options:
   - **SFTP server:** Select this option to restore the critical backup data by using the Secure Shell File Transfer Protocol (SFTP) server. Select an **Authentication type**. The **Authentication type** field is available only when the SFTP server is selected. You can choose password-based authentication or Secure Shell (SSH) key-based authentication. Enter the SFTP server hostname or IP address, User ID, Password, and Backup file name.
   - **NFS server:** Select this option to restore the critical backup data from the remote Network File System (NFS) server. Enter the NFS server hostname or IP address, Mount location, and Backup file name.
   - **USB:** Select this option to restore the critical backup data by using a Universal Serial Bus (USB) flash memory device.
5. Click **Restore HMC** to download the critical HMC data from the selected file location.
6. In the **Restore HMC** step, the progress of the download is displayed. Click **Restart HMC** to restore and restart the HMC with all the critical data.

For HMC Version 10.3.1050.0, or earlier, complete the following steps to restore the HMC data:

1. In the navigation area, click **HMC management**, and then select **HMC actions** > **Restore HMC data**.
2. From the **Restore HMC Data** window, click **Restore from a remote Network File System (NFS) server**, **Restore from a remote File Transfer Protocol (FTP) server**, **Restore from a remote Secure Shell File Transfer Protocol (SFTP) server**, or **Restore from a remote removable media**.
3. Click **Next** to proceed or **Cancel** to exit the task without making any changes.

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

Save HMC upgrade data

Use this task to save the HMC upgrade data on the preferred location.

This data is restored after the HMC upgrade process is completed. The HMC configuration data consists of files that were created or customized with the current software level. You can also save the HMC upgrade data on a media before you upgrade the HMC. You can skip the **Save data for HMC migration** option if the user configuration data is not needed after the upgrade operation.

Note: To save the HMC upgrade data, you must have access as an operator, a super administrator, or a service representative.

For HMC Version 10.3.1060.0, or later, complete the following steps to save the HMC upgrade data:

1. In the navigation area, click **HMC Management**.
2. In the work pane, select **HMC actions** > **Save HMC upgrade data**. The **Save HMC upgrade data** window opens.
3. Select the **Save data for HMC migration** option to include data for migrating this HMC to another HMC.
4. Select the **Include Network data** option to include network-related files in the data.
5. Select the **Include Performance and Capacity Monitoring Data** option to save the performance and capacity monitoring data that is collected for the managed system.
6. Next, select a save location from the following options:
   - **HMC:** Select this option to save the HMC configuration data to a nonvolatile area on the HMC hard disk drive.
   - **USB:** Select this option to save the HMC upgrade data to a Universal Serial Bus (USB) flash memory device on the local system.

     Note: To use this option, ensure that your USB flash memory device is formatted.
   - **SFTP server:** Select this option to access the Secure Shell File Transfer Protocol (SFTP) server to save the HMC upgrade data.
7. Click **Save** to complete the task.

For HMC Version 10.3.1050.0, or earlier, complete the following steps to save the HMC upgrade data:

1. In the navigation area, click **HMC Management**, and then select **HMC actions** > **Save upgrade data**.
2. From the **Save Upgrade Data** window, this wizard takes you through the steps that are required for saving your data. Select the type of media that you want to save your data to, then click **Next** to proceed through the task windows.
3. Click **Finish** when you have completed the task.

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

Restore HMC upgrade data

With HMC Version 10.3.1060.0, or later, you can select the repository to download and then restore the Hardware Management Console (HMC) upgrade data for your HMC.

Complete the following steps to restore the HMC upgrade data:

1. In the navigation area, click **HMC management**.
2. In the work pane, click **HMC actions** > **Restore HMC upgrade data**. The **Restore HMC upgrade data** window opens.
3. In the **Download location** step, select the **Restart HMC after download** option to automatically restart the HMC after the download is completed to restore the HMC upgrade data.

4. Next, select the **Restore data for HMC migration** option to download the data for migrating data from another HMC to this HMC.
5. Next, select a download location from the following options:
   - **SFTP server:** Select this option to restore the HMC upgrade data by using the Secure Shell File Transfer Protocol (SFTP) server. Select an **Authentication type**. The **Authentication type** field is available only when the SFTP server is selected. You can choose password-based authentication or Secure Shell (SSH) key-based authentication. Enter the SFTP server hostname or IP address, User ID, Password, and Backup file name.
   - **USB:** Select this option to restore the HMC upgrade data by using a Universal Serial Bus (USB) flash memory device.
6. Click **Restore** to download the HMC upgrade data from the selected download location.
7. In the **Restore** step, the progress of the download is displayed. Click **Restart** to complete the process.

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

Schedule operations

Create a schedule for certain operations to be performed on the Hardware Management Console (HMC) itself without operator assistance.

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

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

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

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

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

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

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

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

The operation that can be scheduled for the HMC is:

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

To schedule operations on the HMC, complete the following steps:

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

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

Format media

You can format a USB Flash Drive Memory Key.

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

With HMC 10.3.1061.0, or later, to format a USB Flash Drive Memory Key, complete the following steps:

1. In the navigation area, click **HMC management**, and then select **HMC actions** > **Format media**. The **Format media** panel opens.
2. From the **Format media** panel, select the device that you want to format from the **Available devices** table.
3. Select the type of file system to format. The available values are `ext4` and `vfat`.
4. Enter a label to assign to the device. The specified label is converted to uppercase and truncated to 11 characters. If you do not enter a label, a blank label is assigned.
5. Ensure that your media is correctly inserted, then click **Format**.

With HMC 10.3.1060.0, or earlier, to format a USB Flash Drive Memory Key, complete the following steps:

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

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

Launch guided setup wizard

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

1. In the navigation area, click **HMC management**, and then select **HMC actions** > **Launch guided setup wizard**.
2. From the **Launch Guided Setup Wizard - Welcome** window it is recommended that you have certain prerequisites on hand. Click **Prerequisites** in the **Launch Guided Setup Wizard - Welcome** window

for the information. When you have completed that, this wizard takes you through the following tasks required to set up your system and HMC. As you complete each task, click **Next** to proceed.

a. Change HMC Date and Time

b. Change HMC passwords

c. Create additional HMC users

d. Configure HMC Network Settings (This task cannot be performed if you are accessing the **Launch Guided Setup Wizard** remotely.)

e. Specify contact information

f. Configure connectivity information

g. Authorize users to use the Electronic Service Agent software tool and configure notification of problem events.

3. Click **Finish** when you have completed all the tasks in the wizard.

Cloud Connector

Cloud connector is a service that runs on Hardware Management Console (HMC) and sends system resource usage data to IBM Cloud Management Control (CMC) continuously. The HMC Cloud Connector supports either a direct outbound connection or a connection through proxy server to IBM CMC portal. The Cloud Connector supports basic authentication protocol and other authentication protocols, such as Kerberos, LDAP, and Digest-MD5 to connect to the proxy server.

The following steps can be completed on the Cloud Connector task:

1. To enable the Cloud Connector, you need a key from the IBM CMC Portal. To obtain the key, visit your IBM CMC Portal, click **Cloud Connector** > **Settings**.
2. To run the Cloud Connector, complete the following steps:

   a. In the navigation area, click **HMC management**.

   b. In the content panel, click **Cloud connector**. The **State**, **Authentication Type**, **HTTP Proxy**, and **Sock Proxy** of the Cloud Connector is displayed.

   c. To start the Cloud Connector, click **Start cloud connector** and follow the steps in the wizard.

3. To stop the Cloud Connector, complete the following steps:

   a. To stop the Cloud Connector, click **Stop cloud connector**.

   b. Select the **Purge all data** checkbox, and all the data that is associated with the HMC in the CMC Cloud Storage is purged when the Cloud Connector is stopped. The HMC Cloud Connector stops collecting and sending data to the CMC Cloud Storage.

   c. Click **Stop**.

   Note: Alternatively, if you do not select the **Purge all data** checkbox, the HMC Cloud Connector will be stopped but the historical data that is associated with the HMC will be retained in the CMC Cloud Storage.

4. To restart the Cloud Connector, click **Restart cloud connector** and follow the steps in the **Restart cloud connector** wizard.
5. To refresh the Cloud Connector status, click **Refresh**. The updated HMC Cloud Connector status is displayed.

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

Schedule management for HMC Version 10.3.1061.0, or later

You can create a schedule for certain operations to be performed on the managed system without any operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitive processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation.

The **Schedule management** page provides filtering options based on the resource type. You can schedule operations for the managed system, partitions, virtual I/O servers (VIOS), and console. Complete the following steps to manage scheduled operations:

1. In the navigation area, click **Schedule management**. The **Scheduled management** page opens. The **Schedule management** table displays the information about scheduled tasks. You can filter the list of scheduled tasks based on the resource type by selecting any one of the following tabs:
   - **All**: When you select the **All** tab, you can view all the list of scheduled operations irrespective of the resource type. You can view the name of the scheduled task, resource name, resource type, the time of the scheduled operation, the number of remaining repetitions, and repeat interval.
   - **System**: When you select the **System** tab, you can view the name of the scheduled task, name of the system, the time of the scheduled operation, the number of remaining repetitions, and repeat interval.
   - **Partition**: When you select the **Partition** tab, you can view the name of the scheduled task, name of the partition, name of the system, the time of the scheduled operation, the number of remaining repetitions, and repeat interval.
   - **VIOS**: When you select the **VIOS** tab, you can view the name of the scheduled task, Virtual I/O Server name, name of the system, the time of the scheduled operation, the number of remaining repetitions, and repeat interval.
   - **Console**: When you select the **Console** tab, you can view the name of the scheduled task, name of the console, the time of the scheduled operation, the number of remaining repetitions, and repeat interval.
2. Click **Schedule**. The **Schedule** panel opens. Select any one of the following tasks based on the resource type:

Table 10. Schedule management operations

Resource type	Tasks
System	**Activate system profile**: Activates all partitions that are associated with the system profile. **Backup profile data**: Backs up the profile data to a disk and allows it to be restored to the Hardware Management Console (HMC). **Power Off System**: Powers off the managed system, making all partitions unavailable until the system is powered on again. **Power On System**: Powers on the system and its partitions according to the Partition Start Policy. **Edit shared processor pool**: Schedules an operation for modifying a shared processor pool. **Move partition to different pool**: Schedules an operation for moving a partition to a different processor pool. **Edit power saver mode for system**: Schedules an operation for changing the power saver mode for a managed system. **Monitor/Perform Dynamic Platform Optimize**: Schedules an optimization operation and sends an email alert.
Partition	**Activate partition profile**: Schedules the activation of the selected partition profile. **Dynamic reconfiguration**: Schedules a dynamic reconfiguration task for a partition. **Operating system shutdown on a partition**: Schedules an operating system shutdown on a partition.
VIOS	**Activate VIOS profile**: Schedules the activation of the selected VIOS profile. **Dynamic reconfiguration**: Schedules a dynamic reconfiguration task for a VIOS. **Operating system shutdown on a VIOS**: Schedules an operating system shutdown on a VIOS. **Backup IO configuration**: Schedules a backup of the IO configuration. **Backup SSP configuration**: Schedules a backup of the SSP configuration. **Backup VIOS**: Schedules a backup of the VIOS.

Table 10. Schedule management operations (continued)	
Resource type	**Tasks**
Console	**Backup HMC data**: Schedules a backup of HMC data. **Run ILMT scan and upload**: Schedules a Run ILMT scan and upload operation.

3. To view the detailed information of a scheduled task, click **View**.
4. To delete scheduled operations, select the scheduled tasks that you want to delete, and click **Delete**.

Notes:

- You can specify the number of weeks or months to elapse before performing the scheduled operation again on each selected day.
- You can specify the interval to be monthly. The scheduled operation is run on the configured time and month. It is also run on the subsequent months based on the number of repetitions and monthly intervals that you have configured.
- For example, if you configure the scheduled operation for 31st of every month with five repetitions, then the scheduled operation is executed every month on 31st, and if a particular month does not have 31st then that repetition is executed on the last day of the month. For example, if you configure the scheduled operation from 31 January with five repetitions, then the operation is executed on 31 January, 28 February, 31 March, 30 April, and 31 May.
- You can schedule an operation to occur once or you can schedule it to repeat. You must provide the time and date that you want the operation to occur. If you want the operation to repeat, you are asked to select the following options:
  - The day or days of the week that you want the operation to occur.
  - The interval, or time between each occurrence.
  - The total number of repetitions.
- You can search for any data within the table by typing a relevant keyword in the search bar.
- To refresh the list of scheduled operations, click the **Refresh** icon.
- You can export the scheduled operations data by clicking the **Export** icon. The following formats are supported for the exporting option:
  - PNG
  - PDF
  - CSV
- For more information about managing scheduled operations with HMC 10.3.1060.0, or earlier, see "Schedule operations for HMC Version 10.3.1060.0, or earlier" on page 33

Use the online Help if you need additional information for schedule management.

Performance dashboard

Starting with HMC Version 10.3.1050, or later, you can view the **Performance dashboard** by accessing it from the navigation area. The **Performance dashboard** displays the allocation and usage data for virtualized server resources. It displays data in the form of charts, graphs, and tables.

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

The **Performance dashboard** captures data only from the systems for which you choose to enable data collection.

You can access the **Performance dashboard** page in multiple ways. Complete any one of the following steps to view the **Performance dashboard** page:

- From the HMC dashboard, complete the following steps:
  1. Click **Performance dashboard** in the left navigation window.
  2. Select a system and click **Launch**.
- From the left navigation window, complete the following steps:
  1. Click **System resources** > **Systems**.
  2. Select a system from the list and click any one of the following:
     a. **Performance** > **View performance dashboard**.
     b. **i icon** > **Go to performance dashboard**.

To enable data collection for one or more systems, complete the following steps:

1. In the navigation area, click **System resources** > **Systems**.
2. In the **Systems** page, click **Performance** > **Turn on/off performance data collection**. Alternatively, you can click **Usage** tab in the **Systems** page and click the toggle switch in the **Data collection** column.
3. Specify the number of days for which you want to store performance data by typing the number from 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 upto 366 days.
4. Click the toggle switch in the **Collection** column next to the name of the system for which you want to collect data. Alternatively, you can click **All On** to enable data collection for all the servers in your environment that is managed by the HMC.

   Note: You might be prevented from collecting data from all the managed systems in your environment because the storage space is limited. The HMC prohibits you from enabling data collection from more systems when the HMC determines that it might run out of the 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 dashboard** page.

Environmental dashboard

Starting with HMC Version 10.3.1060.0, you can view the Environmental dashboard by accessing it from the navigation area. The Environmental dashboard displays the sustainability metrics to provide insights into the environmental impacts of the selected system. It displays data in the form of graphs.

The Environmental dashboard gathers data and provides specific information and trends about the following parameters:

- Power usage
- Inlet temperature
- Carbon footprint
- Core Usage percentage

It also provides the historical trends for the same parameters over a specific time. This information can help you to effectively monitor energy consumption and carbon emissions that are generated by the selected systems.

The System details section of the Environmental dashboard displays information that is associated with the selected system. The System details section displays the following parameters:

- State

- Machine type*Serial number
- Number of partitions
- Number of Virtual I/O Server (VIOS)

In addition, the Power trends graphs are useful for tracking energy consumption, assessing environmental impact, and making data-driven decisions to promote sustainability. The Power trends graph is customisable based on a timeline and date range. For more information about the Environmental dashboard, see Using the Environmental dashboard.

The Environmental dashboard captures data only from the selected systems for which you choose to enable data collection. You can also export the Environmental dashboard data metrics that are displayed in the Environmental dashboard into a folder on your local system.

You can access the Environmental dashboard page in multiple ways. Complete any one of the following steps to view the Environmental dashboard page:

- From the HMC dashboard, complete the following steps:
  1. Click **Environmental dashboard** in the left navigation window.
  2. Select a system and click **Launch**.
- From the left navigation window, complete the following steps:
  1. Click **System resources** > **Systems**.
  2. Select a system from the list and click any one of the following options:
     a. **Performance** > **View environmental dashboard**.
     b. **i icon** > **Go to environmental dashboard**.
- From the left navigation window, complete the following steps:
  1. Click **System resources** > **Systems**.
  2. Click a system from the list.
  3. Click **System actions**.
  4. Click **View environmental dashboard**.

You can enable data collection in multiple ways for one or more servers. Complete any one of the following methods to enable data collection:

- From the HMC dashboard, complete the following steps:
  1. In the navigation window, click **System resources**.
  2. Click **Systems**.

     The **Systems** page is displayed.
  3. Click **Usage**.
  4. If the Data collection is not enabled for any particular system, under the Data collection column, click **On**. The green tick mark indicates that the Data collection is enabled for that particular system.
- From the Environmental dashboard, complete the following steps:
  1. In the HMC dashboard, click Environmental dashboard in the left navigation window.

     The **Systems** page is displayed.
  2. Select a **system** from the available list and click **Launch**.
  3. In the Environmental dashboard, if the Data collection is not enabled, click **Turn data collection on** in the notification message to enable data collection for the selected system.

  Note: The **Data collection** toggle switch shows the current status of data collection. You can change it by toggling the switch.

Call home management for HMC Version 10.3.1060.0, or later

The tasks that are available on the HMC Version 10.3.1060.0, or later, for the **Call home management** tasks are described.

Note: Depending on the task roles that are assigned to your user ID, you might 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 that are allowed to access them.

Customer information

Use this task 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 "Data replication" on page 93.

To customize your customer information, complete the following steps:

1. In the navigation area, click **Call home management**, and then select **Customer information**.
2. Provide the appropriate information in **Administrator information**, **System information**, and **Account information** sections.
3. Click **Save** when you have completed the task.

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

Outbound connectivity

You can 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 by using the **Manage Data Replication** task, the data that is specified in this task might change depending on automatic replication from other HMCs configured on your network. For more information about data replication, see "Data replication" on page 93.

You can configure this HMC to attempt connections through the 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 conducting automated service operations. HMC can initiate the connection. IBM Service Support System cannot and never attempts to initiate a connection to the HMC.

You can configure this HMC to attempt connections through the Internet, Internet Virtual Private Network (VPN), or through a remote pass-through system. Remote service is a two-way communication between the HMC and your support system for conducting automated service operations. The connection can only be initiated by the HMC.

To customize your connectivity information, complete the following steps:

1. In the navigation area, click **Call home management**, and then select **Outbound connectivity**.
2. In the **Local console configuration** section, click **Configure** to launch the **Configure local console** window. You can configure the HMC as a call home server and configure the proxy settings that the HMC uses to contact the service provider for call home and firmware updates. Click **Configure** to complete the local console configuration.
3. In the **Call home server consoles** section, click **Add** to specify an IP address or hostname that you want to add to the list of call home server consoles.
4. When you complete all the necessary fields, click **Save** to save your changes.

Use the online Help if you need additional information for customizing outbound connectivity information.

Service user authorization

You can 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 service provider ID, complete the following steps:

1. In the navigation area, click **Call home management**, and then select **Service user authorization**.
2. Enter a service provider ID that is registered with the Electronic Service Agent. If you need a user ID, you can register at the IBM Registration website. Click **Add ID**.
3. Click **Save**.

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

Event notification

You can add email addresses that notify you when problem events occur on your system and configure the method of notification about system events from the Electronic Service Agent.

To set up notification, complete the following steps:

1. In the navigation area, click **Call home management**, and then select **Event notification**.
2. You can complete the following tasks:
   - In the **Email notification** section, select **Enable email notification for problem events** to enable notifications about problem events on your system and scheduled operations.
   - Click **Add email address** to add the email addresses that are notified when problem events occur on your system and when scheduled operations are planned for your system.
   - In the **SNMP trap configuration** section, specify locations for sending Simple Network Management Protocol (SNMP) trap messages for Hardware Management Console application programming interface events.
3. Click **Save** when you complete this task.

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

Electronic service agent

You can enable or disable the call-home state for managed systems.

Note: If Customizable Data Replication is enabled on this HMC by using the **Manage Data Replication** task, the data that is specified in this task might change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see "Data replication" on page 93.

By enabling the call-home state for a managed system, the console automatically contacts 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 systems:

1. In the navigation area, click **Call home management**, and then select **Electronic service agent**.
2. Set **State** to **Enabled** or **Disbaled** for the managed systems.

3. Click **Save** when you complete the task.

Use the online Help if you need additional information for enabling the Electronic service agent.

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 **Call home management**, and then select **Connection monitoring**.
2. Adjust the timer settings. Set **Notifications** to **Enabled** or **Disabled**.
3. Click **Save** when you complete the task.

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

Call home management for HMC Version 10.3.1050.0, or earlier

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

Note: Depending on the task roles that are assigned to your user ID, you might 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 that are allowed to access them.

Setup electronic service agent

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

About this task

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

Procedure

1. In the navigation area, click **Call home**, then select **Setup electronic service agent**.
2. The Electronic Service Agent wizard opens. Follow the instructions in the wizard to configure call-home tasks.

Service user authorization

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

To register a user ID, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Service user authorization**.
2. 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.

3. Click **OK**.

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

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 "Data replication" on page 93.

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 **Call home**, and then select **Electronic service agent**.
2. From the **Enable Electronic Service Agent** window, select a system or systems you want to enable or disable the call-home state.
3. Click **OK** when you have completed the task.

Use the online Help if you need additional information for enabling the Electronic service agent.

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 "Data replication" on page 93.

You can configure this HMC to attempt connections through the 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.

You can configure this HMC to attempt connections through the Internet, Internet Virtual Private Network (VPN), or through a remote pass-through system. Remote service is a two-way communication between the HMC and your support system for the purpose of conducting automated service operations. The connection can only be initiated by the HMC.

To customize your connectivity information, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Outbound connectivity**.
2. In the **Manage Outbound Connectivity** window, click **Configure** to launch the **Local Console Configuration** window. You can configure the HMC as a call home server and configure the proxy settings that the HMC uses to contact the service provider for call home and firmware updates.
3. Click **Add** to specify an IP address or host name that you want to add to the list of call home server consoles.
4. 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.

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 "Data replication" on page 93.

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

- Administrator and System
- Account

To customize your customer information, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Customer information**.
2. From the **Manage Customer Information** window, provide the appropriate information in the **Administrator and System** tab.

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

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

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 **Call home**, and then select **Event notification**.
2. From the **Manage Event Notification** window, you can complete the following tasks:
   - Use the **Email** tab to add the email addresses that are notified when problem events occur on your system and when scheduled operations are planned for your system.
   - Use the **SNMP Trap Configuration** tab to specify locations for sending Simple Network Management Protocol (SNMP) trap messages for Hardware Management Console application programming interface events.
3. Click **OK** when you complete this task.

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

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 **Call home**, and then select **Connection monitoring**.
2. From the **Manage Connection Monitoring** window, adjust the timer settings, if required, and enable or disable the server.
3. Click **OK** when you have completed the task.

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

Service management tasks for HMC Version 10.3.1061.0, or later

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

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.

Dumps

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

To manage a dump with HMC 10.3.1061.0, or later, complete the following steps:

1. In the navigation area, click **Service management** and then select **Dumps**.
2. Select a system to view the list of existing dumps for the system. You can also select **All** in the **System** drop-down list to view the entire list of existing dumps for the HMC.
3. You can view the list of dumps in the content pane. You can perform the following tasks:
   - Modifying the system dump settings: Click **Edit system dump settings** to display and alter the dump settings.

     Note: This option is available only for the flexible service processor (FSP) based systems.
   - Initiating a dump: Click **Initiate dump** to perform the following tasks:
     - Initiate a resource dump.
     - Initiate a system controller dump.
     - Initiate a system dump.
4. Select dump files in the Dumps table to perform the following tasks:
   - **Call home**: Use the call home feature to transmit the dump to your service provider.
   - **Delete dump**: Delete the selected dump files from the HMC.
   - **Save to media**: Copy the dump file to the media.
   - **Save to remote system**: Copy the dump file to a remote system.

Notes:

- You can search for a dump by typing a keyword in the search bar that is available at the beginning of the **Dumps** table.
- You can click the **Refresh** icon to update and redisplay the data in the dump table.
- You can export dumps data by clicking the **Export** icon. The following file formats are supported for the **Export** option:
  - PNG
  - PDF
- You can customize the columns in the Dumps table by clicking the **Customize columns** icon.

FTP connection

You can provide configuration data to allow the use of File Transfer Protocol (FTP) to offload the service information. If your network includes a company firewall, you must specify the configuration information about the firewall for you to use an FTP site to offload the service information.

To configure an FTP connection, complete the following steps:

1. In the navigation area, click **Service management**.
2. In the content pane, click **FTP connection**. The **FTP connection** page opens.
3. Select the option **Enable FTP transmission of service information**.
4. Configure the following **Server** properties:
   a. Select one of the following types of file transfer:
      - **SFTP**: Select this option to use Secure File Transfer Protocol (SFTP) for the transmission of service information.
      - **FTP**: Select this option to use the FTP for the transmission of service information.
   b. Select one of the following modes:
      - **Passive**: Select this option to allow the server to assign an IP address and port number on its side, while the client initiates a connection to the server.
      - **Active**: Select this option to have the client request that the server initiate a data connection and terminate it at an IP address and port number that is chosen by the client, with the server connecting to the client.
   c. Enter the **Server hostname or IP address** of the remote server.
   d. Enter the **Port** number of the remote server.
   e. Enter the **User name** and the **Password** to access the remote server.
   f. You can also enter the **Directory**. This is an optional field.
5. Provide the configuration information about the firewall for you to use an FTP site to offload the service information.
   a. Select the **Enable FTP firewall configuration settings** option.
   b. Select one of the following modes:
      - **Passive**: Select this option to allow the server to assign an IP address and port number on its side, while the client initiates a connection to the server.
      - **Active**: Select this option to have the client request that the server initiate a data connection and terminate it at an IP address and port number that is chosen by the client, with the server connecting to the client.
      - **Optional**: Select this option to first try the **Passive** mode followed by the **Active** mode.
   c. Enter the **Server hostname or IP address** of the remote server.
   d. Enter the **Port** number of the remote server.
   e. Select the **Authentication format** from the drop-down list.
   f. Optionally, you can enter an **Exclusion list** that specifies the domains or hosts where the firewall should not be applied. For example, if you do not want the firewall to affect FTP connections to hosts in your own **probe.net** domain, set this field to `probe.net`. To specify multiple domains or hostnames, separate them with commas. The special token `localdomain`is used for unqualified hostnames, so include it in your list if you want hosts without explicit domain names to bypass the firewall.
   g. Enter the **User name** of the firewall .
   h. Enter the firewall **Password** that is associated with the firewall username.

      Note: When you set the password, you must change the permissions on the file so that no one can view your password, except a superuser.

6. Click **Test connection** to test the connection.
7. Click **Save** to complete the FTP configuration.

Schedule service data

You can schedule when to transmit service information for use for problem determination to your service provider.

To schedule service information, complete the following steps:

1. In the navigation area, click **Service management**, and then select **Schedule service data**.
2. On the **Schedule service data** page, configure the types of service information that you want to enable for regular transmissions by toggling the **Schedule service data** option and specifying the interval in days and the time to schedule repeating transmissions:
   - **Disk health data**: Disk health information such as idle time, power on hours, reassigned sectors, and soft errors is collected and sent when you transmit Disk Health Log information.
   - **Fix level recommendation tool data**: Fix Level Recommendation Tool (FLRT) information for the AIX and Virtual I/O Server (VIOS) operating systems is collected and sent. The data includes update and upgrade recommendations. Provides a report with data to aid system administrators with service planning.
   - **Hardware service data**: Hardware service information is collected and sent when you transmit the Vital Product Data (VPD) log.
   - **Operational heartbeat data**: Operational test (heartbeat) information is collected and sent when you transmit the Problem Event log.

     Note: Operational heartbeat data collection is always enabled.
   - **Software service data**: Software service information is collected and sent for all software running on the selected partitions when you send the VPD log.
   - **Update access key**: As update access keys expire, they need to be replaced. This option checks whether a new update access key needs to be downloaded for the system.
   - **AIX update access key**: As update access keys expire, they need to be replaced. This option checks whether a new AIX update access key needs to be downloaded for the system.
3. Click **Save** to save the schedule information.

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

Remote support connection

Manage the service connection that securely accesses the remote system.

To manage the connection that service uses to securely access the system remotely, complete the following steps:

1. In the navigation area, click **Service management**, and then select **Remote support connection**.
2. In the **Remote support connection** page,
   a. Click Open to keep the connection open. When you select the Open option, you must specify the Connection timeout (minutes) period.
   b. Click `Close` to close the remote support connection.
3. When you complete all the necessary fields, click **Save** to save your changes.

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

Prerequisites for managing a Remote support connection

Learn about the prerequisites for enabling remote access for your Hardware Management Console (HMC).

About this task

Notes:

- IBM can remotely connect to your system to perform maintenance actions by using remote access. Remote access can be enabled as needed for a specified time limit up to 2 days.
- It is recommended that you install and configure the **Remote Support Proxy** service to simplify firewall configurations. One **Remote Support Proxy** can be used by multiple systems and by other management consoles.

Step 1. Configuring a firewall rule

Before you begin

With a Remote Support Proxy server

Use the following information to configure a firewall rule after you install and configure the Remote Support Proxy server:

Source	IP address of the Remote Proxy Server
Target	129.33.206.139 and 204.146.30.139
Port	443
Protocol	https
Direction	Outbound only

Note: You also need to configure the IP address of the Remote Support Proxy server into the system.

Without a Remote Support Proxy server

If the Remote Support Proxy server is not installed and configured, use the following information to configure a firewall rule:

Source	The service IP address of every management console that is running the remote support center service
Target	129.33.206.139 and 204.146.30.139
Port	22
Protocol	ssh
Direction	Outbound only

Step 2. Installing Remote Support Proxy

About this task

The Remote Support Proxy utility must be installed in the following situations:

- Your system does not have internet access.
- You want to route multiple systems to the support center through a single system. This way, firewall restrictions need to be disabled only for a single system.

- All nodes in your system have service IP addresses configured in IPv6 format. In this case, the Remote Support Proxy needs to listen on an IPv6 interface, which needs to be defined on your system as a support center.

To download and install the Remote Support Proxy utility, complete these steps:

Procedure

1. On the Linux computer where you plan to run the proxy utility, download the Remote Support Proxy utility installation package and Release Notes from the Fix Central website.
2. Assign the downloaded file execution permissions by running the following command:

   ```
   chmod +x file_name.bin
   ```

   where **file_name.bin** is the name of the installation package.
3. Install the Remote Support Proxy utility by using the following command:

   ```
   ./file_name.bin
   ```

   where **file_name.bin** is the name of the installation package for the system.
4. A software license is displayed.
5. Follow the instructions and accept the license. The installation program installs an RPM package that is named supportcenter_proxy and then exits.

   Note: Occasionally, the license is not displayed and the application ends unexpectedly. The license cannot be displayed when the **bzip2** package is missing on the system. Use the Linux package manager to reinstall the **bzip2** package to the system and try again.

   The following files are installed on the local system:

/usr/bin/supportcenter_proxy	The binary executable file.
/etc/supportcenter/proxy.conf	The configuration file. You must update this file before you start the Remote Support Proxy service.
/etc/init.d/supportcenter_proxy	The system service for starting and stopping the Remote Support Proxy. The service is configured to start when the server boots. It does not start automatically after installation.
/usr/share/supportcenter/syslog-logger	The logger program that can be modified to integrate with the existing logging and monitoring systems.
/usr/share/doc/proxy-version/license	The directory that contains the accepted software license for the Remote Support Proxy in multiple languages. In the directory path, version is the product version.
/usr/share/supportcenter/proxy_id_rsa	A cryptographic file that is used by the configuration-retrieval function.

Step 3. Configuring Remote Support Proxy

Before you begin

After you install the Remote Support Proxy on the system, you must configure it. The Remote Support Proxy is required when remote support assistance is configured on systems that do not have direct access to the internet.

To configure the Remote Support Proxy service with the system, change the following required parameters in the **/etc/supportcenter/proxy.conf** file:

ListenInterface	Specifies the IPv4 address, IPv6 address, or interface name on which the proxy service must listen for incoming connections from the system (for example, 192.0.2.1, 2001:DB8:0:0:0:0:0:0, or eth0). • If you specify an IPv4 or IPv6 address, the proxy service listens on only the specified IP address. • If you specify an interface name, the proxy service listens on all allowed addresses. You can configure which addresses are allowed by setting the **UseIPv4**, **UseIPv6,** and **UseIPv6LinkLocalAddress** parameters. By default, the proxy service listens on both IPv4 and IPv6 addresses. • If you specify the interface name, the name must be the same as the output from the **ifconfig** command. **Important:** The storage system must have access to the system that runs the Remote Support Proxy as defined by this interface name or IP address.
ListenPort	The TCP port on which the Remote Support Proxy must listen for incoming connections from the system. For example: 8988. **Important:** The storage system must have access to the system running the Remote Support Proxy as defined by this port.

ServerAddress	The TCP port on which the Remote Support Proxy must listen for incoming connections from the system. Add the following strings to the configuration file:
	`ServerAddress1 129.33.206.139`
	`ServerPort1 443`
	`ServerAddress2 204.146.30.139`
	`ServerPort2 443`

Step 4. Starting Remote Support Proxy

Procedure

After you update the Remote Support Proxy configuration file, start the Remote Support Proxy service. To start the Remote Support Proxy service, run the following command:

```
service supportcenter_proxy start
```

Note: If the proxy service does not start correctly, examine the log file for errors. The default log file is **/var/log/supportcenter_proxy.log**.

Serviceable events

Use this page to view and manage serviceable events.

To manage serviceable events, complete the following steps:

1. In the navigation area, click **Service management**, and then select **Serviceable events**. The **Serviceable events** page opens. You can view serviceable events from the Hardware Management Consoles (HMCs) that are listed.
2. You can modify the event criteria, error criteria, and FRU criteria to refine the list of serviceable events that you want to view.
3. Click **Refresh** to refresh the list of events that are based on the selected filter values.
4. Select the serviceable events that match your selection criteria and click **Action** to manage the selected serviceable events. Click **Action** > **View details** to view the details of the serviceable events.
5. Click **View** to change the view of the table from compact to full.

   Compact
   Displays fewer details for the serviceable events in the table.

   Full
   Displays more details for the serviceable events in the table.

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

Events manager for call home

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

1. In the navigation area, click **Service management**, 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.
3. 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.
4. Click **Refresh** to refresh the list.
5. Select an event and click **Action** to choose any of the following options to manage the selected event:
   - **View Details**: Displays the details of this event.
   - **View Files**: Displays the files that are associated with this event.
   - **View Reference Code Description**: Displays the description of the reference code associated with the selected serviceable event. This option is not be available if the reference code has no description.
   - **Approve Call Home**: Approve the call home of this event. This option is only available if the event has not been approved already.
6. Click **Save** to save the filter values.

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

Service actions

You can create a serviceable event or send service data.

Create serviceable events

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.

Reporting a problem

To report a problem on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **Service management**.
2. Click **Service actions** > **Create serviceable event**. The **Create serviceable events** window opens.
3. Enter a brief description of your problem in the **Problem description** field and then click **Request service**.

To test problem reporting from the **Create serviceable events** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem description** 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.

Reporting a problem after selecting a system

To report a problem after selecting a system on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **Systems**.
2. In the content pane, select a managed system and click **Service** > **Create serviceable event**.
3. In the **Create Serviceable Event** window, you can select a **Problem type** that describes where the problem occurred or what is the problem.
4. Enter a brief description of your problem in the **Problem description** field and then click **Request service**.

To test problem reporting from the **Create Serviceable Event** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem description** 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.

Send service data

Service data is a set of program and event traces and storage dumps that can assist you in servicing the system. The data in selected service categories is collected in a file or group of files for transmission to your Service Provider.

Before you begin

Send service data only when requested by your service representative. The call home server and remote service must be enabled before you can send information to the service support system.

Procedure

1. In the navigation area, click **Service management**.
2. Click **Service actions** > **Send service data**. The **Send service data** panel opens.
3. Enter the required fields, and click **Send**.

VIOS images for HMC Version 10.3.1061.0, or later

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

Manage Virtual I/O Server images

You can import Virtual I/O Server (VIOS) images from a USB device or a remote server and store the images on the HMC. The stored VIOS images can be used for VIOS installation. You must be an HMC super administrator (hmcsuperadmin) to install the VIOS image.

About this task

To manage or to import the VIOS image repository, complete the following steps:

Procedure

1. In the navigation area, click **VIOS images**. The **VIOS images** page opens.
2. Click **Import**. In the **Import VIOS image** panel, complete the following steps:
   - Enter a name for the VIOS image.
     a. Select the import location from the following options:
        - **SFTP server**: Select this option to import the VIOS images from a Secure Shell File Transfer Protocol (SFTP) server. You must specify **Password** or **Keyfile** as the authentication type.

          Note: The **Authentication type** field is available only when the SFTP server is selected.

          - For password authentication, the following fields are mandatory:
            - **Remote server hostname or IP address**: Enter the remote server hostname or IP address of the remote SFTP Server.
            - **User ID**: Enter the username of the remote SFTP Server.
            - **File names**: Enter the ISO file names.

            Optionally, you can enter remote directory information.
          - For keyfile authentication, the following fields are mandatory:
            - **Remote server hostname or IP address**: You must enter the remote server hostname or IP address of the remote SFTP Server.
            - **Keyfile**: Enter the SSH Keyfile name.
            - **File names**: Enter the ISO filename.

            Optionally, you can enter remote directory and passphrase information.
        - **NFS server**: Select this option to import the VIOS images from a Network File System (NFS) server. The following fields are mandatory:
          - **Remote server hostname or IP address**: Enter the remote server hostname or IP address of the remote NFS server.
          - **Mount location**: Enter the mount location of the remote NFS server.
          - **File names**: Enter the ISO file names.

          Optionally, you can enter information about remote directory and other mount options.

- **USB**: Select this option to import VIOS images from the Universal Serial Bus (USB) flash memory device. Select the USB device from the **USB input** drop-down list.

b. To import VIOS images from a Secure Shell File Transfer Protocol (SFTP) server, enter the server hostname or IP address,

- Select the import location from the following options:

a. Select the import location from the following options:

- **SFTP server**: Select this option to import the VIOS images from a Secure Shell File Transfer Protocol (SFTP) server. You must specify **Password** or **Keyfile** as the authentication type.

  Note: The **Authentication type** field is available only when the SFTP server is selected.

  - For password authentication, the following fields are mandatory:
    - **Remote server hostname or IP address**: Enter the remote server hostname or IP address of the remote SFTP Server.
    - **User ID**: Enter the username of the remote SFTP Server.
    - **File names**: Enter the ISO file names.

    Optionally, you can enter remote directory information.
  - For keyfile authentication, the following fields are mandatory:
    - **Remote server hostname or IP address**: You must enter the remote server hostname or IP address of the remote SFTP Server.
    - **Keyfile**: Enter the SSH Keyfile name.
    - **File names**: Enter the ISO filename.

    Optionally, you can enter remote directory and passphrase information.
- **NFS server**: Select this option to import the VIOS images from a Network File System (NFS) server. The following fields are mandatory:
  - **Remote server hostname or IP address**: Enter the remote server hostname or IP address of the remote NFS server.
  - **Mount location**: Enter the mount location of the remote NFS server.
  - **File names**: Enter the ISO file names.

  Optionally, you can enter information about remote directory and other mount options.
- **USB**: Select this option to import VIOS images from the Universal Serial Bus (USB) flash memory device. Select the USB device from the **USB input** drop-down list.

- To import VIOS images from a Secure Shell File Transfer Protocol (SFTP) server, enter the server hostname or IP address.

3. Click **Import** to import the VIOS images.

   Note: You can also rename an existing VIOS image. In the **VIOS images** page, select an existing image and click **Rename**. Enter the new name of the file in the **New image name** field, and click **Save**

Manage Virtual I/O Server backup

You can manage the I/O configuration of Virtual I/O Servers (VIOS) and manage the backup of the VIOS image on the management console.

About this task

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

Procedure

1. In the navigation area, click **VIOS images**.
2. In the content pane, click **VIOS backups**. The **Manage Virtual I/O Server Backups** window opens. The **Virtual I/O Server Configuration Backup** tab displays a table that lists all the backup files of the VIOS configuration that is taken by the HMC. Also, you can view the time at which the configuration file was last edited.
   - To take the backup of the input/output configuration file of a VIOS, click **Backup I/O configuration**. In the Backup I/O configuration window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

     You can enable the **Overwrite Existing File** checkbox to overwrite the existing file name.

     The file name that you specify must consist of 1 - 40 characters including the file extension **.tar.gz**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   - To rename an existing backup file that is stored in the HMC, select a configuration file from the table and click **Action** > **Rename**.

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

     Note: This action might require the Virtual I/O Server to be rebooted. You can select the **If required, reboot Virtual I/O Server** checkbox to reboot the VIOS.

     The file name that you specify must consist of 1 - 40 characters including file extension **.tar.gz**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   - To export the VIOS backup files to the remote system, select one or more backup files that are saved on the HMC. Click **Action** > **Export** and then complete the following steps:

     a. Specify the credentials of the remote server where backup files are copied.

     b. Select **NFS Server** or **SFTP Server** as the server type and enter the required details.
   - To import the backup files from the remote system, click **Import** and then complete the following steps:

     a. Specify credentials of the remote server, and then select the VIOS where backup files are imported.

     b. Select **NFS Server** or **SFTP Server** as the server type and enter the required details.
3. In the Manage Virtual I/O Server Backups window, click the **Virtual I/O Server Backup** tab. A table is displayed that lists all the VIOS image backups that are taken in the HMC. You can also view the name and size of the VIOS image, the time when the VIOS image file was last edited, the managed system and the VIOS from which the image was captured.
   - To take the backup of the VIOS image, click **Create Backup**. In the Create Backup window, select the managed system and the VIOS for which the back up is created, and then specify a name for the backup file.

     The file name that you specify must consist of 1 - 40 characters including the file extension **.tar**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

     You can enable the **Overwrite Existing File** checkbox to overwrite the existing file name. You can select **NIMOL resources**, **Media repository content**, and **Volume groups structure** to include the selected resources into your backup file.

- To rename an existing VIOS image backup file that is stored in the HMC, select a backup file from the table and click **Action** > **Rename**.

  The file name that you specify must consist of 1 - 40 characters including the file extension **.tar**. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
- To remove a VIOS image backup file from the HMC, select a backup file that contains the VIOS configuration that you want to remove from the table, and click **Action** > **Remove**.
- To export the Virtual I/O Server backup files to the remote system, select one or more backup files that are saved on the HMC. Click **Action** > **Export** and complete the following steps:
  a. Specify the credentials of the remote server where backup files are copied.
  b. Select **NFS Server** or **SFTP Server** as the server type and enter the required details.
- To import the backup files from the remote system, click **Import** and complete the following steps:
  a. Specify the credentials of the remote server, and then select the target Virtual I/O Server where backup files are imported.
  b. Select **NFS Server** or **SFTP Server** as the server type and enter the required details.

4. Click **Apply**.

Manage Virtual I/O Server updates

You can manage the Virtual I/O Server (VIOS) updates. You can use the update image files that are available on the HMC or copy the VIOS update image files that are uploaded on other resources to the HMC. You can rename the existing VIOS update image file name or delete the older update image files to free up disk space.

About this task

To manage the VIOS update images that are stored in the HMC, complete the following steps:

Procedure

1. In the navigation area, click **VIOS images**.
2. In the content pane, click **VIOS updates**. The **Manage Virtual I/O Server Update Images** window opens. The **Virtual I/O Server Update Images** tab displays the list of all the VIOS image files that are stored in the HMC.
   - To rename an existing image file that is stored in the HMC, select a file from the table and click **Action** > **Rename**. The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.
   - To remove one or more VIOS image files from the HMC, select the files from the list and click **Action** > **Remove**.
   - To import the image files from a remote system, click **Import**. In the Copy Update Image window, you can copy and import the VIOS image file from the NFS server, SFTP Server, or a USB device.
     a. To import VIOS image files from the NFS server to the HMC, complete the following steps:
        i) In the **Copy VIOS image** window, select **NFS Server**.
        ii) In the **Name** field, enter the VIOS update image file name that you want to import.
        iii) Enter the required details.
     b. To import VIOS images from the SFTP server to the HMC, complete the following steps:
        i) In the Copy VIOS image window, select **SFTP Server**.
        ii) In the **Name** field, enter the VIOS update image file name that you want to import.
        iii) Enter the required details.

c. To import VIOS images from a USB device to the HMC, complete the following steps:

i) In the Copy VIOS image window, select **USB**.

ii) In the **Name** field, enter the VIOS update image file name that you want to import.

iii) Enter the required details.

Note: The file name that you specify must consist of 1 - 40 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, the dot (.), the dash (-) and the underscore (_) characters.

3. Click **Apply**.

User management tasks for HMC Version 10.3.1060.0, or later

Learn about User management tasks that are available for HMC Version 10.3.1060.0, or later.

Note: Depending on the task roles that are assigned to your user ID, you might 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 that are allowed to access them.

Active users

The **Active users** page displays the list of users that are logged on to the Hardware Management Console (HMC).

1. In the navigation area, click **User management** > **Active users**. In the **Active users** page, the following information is displayed:
   - The username that is logged in to the HMC
   - The session identification number linked to the user logged in to the HMC
   - The number of tasks that are running
   - The log-in time of the user
   - The access location of the user
   - The login mode of the user
   - Additional information about the active user session
2. If you are assigned required task role permissions, you can select the usernames from the Active users list and click **Log off** to log off the users.

Notes:

- You can search for any data within the table by typing a relevant keyword in the search bar.
- You can customize the columns in the active users table by clicking the **Customize columns** icon.
- You can export the active users data by clicking the **Export** icon. The following formats are supported for exporting option:
  - PNG
  - PDF
  - CSV

Running tasks

The **Running tasks** page displays the list of currently running tasks for the user.

1. In the navigation area, click **User management** > **Running tasks**. In the **Running tasks** page, the following information is displayed:
   - The name of the task that is running
   - The task identification number that is associated with the running task

- The session identification number that is associated with the user ID that is running the task
- The user ID that is logged in to the HMC
- The object names that are targeted for the running task
- The time at which the task was started

2. If you are assigned required task role permissions, you can select the tasks that you want to close from the running tasks list, and click **Close task window**.

Notes:

- You can search for any data within the table by typing a relevant keyword in the search bar.
- You can customize the columns in the running tasks table by clicking the **Customize columns** icon.
- You can export the running tasks data by clicking the **Export** icon. The following formats are supported for exporting option:
  - PNG
  - PDF
  - CSV

User profiles

You can use the **User profiles** page to manage the user profiles for the system users that log in to the Hardware Management Console (HMC). A user profile is a combination of a user ID, server authentication method, permissions, and a text description. Permissions represent the authority levels that are assigned to the user profile for the objects that the user has permission to access.

Users can be authenticated by using local authentication on the HMC, by using Kerberos remote authentication, or by using LDAP authentication. For more information on setting up Kerberos authentication on the HMC, see “KDC” on page 132. For more information about LDAP authentication, see “LDAP” on page 131.

Users who remotely authenticate through Kerberos or Lightweight Directory Access Protocol (LDAP) must have their profiles set. 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 in to the HMC locally.

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

If you are using local authentication, the user ID and password are used to verify a user’s authorization to log on the HMC. The user ID must start with an alphabetic character and consist of 1 to 32 characters. The password has the following rules:

- Must begin with an alphanumeric character.
- Must contain at least 8 characters, however, this limit can be changed by your system administrator.
- The characters must be standard 7-bit ASCII characters.
- Valid characters to use for the password can be: A-Z, a-z, 0-9 and special characters (~ ! @ # $ % ^ & * ( ) _ + - = { } [ ] \ : " ; ’).

If you are using Kerberos authentication, specify a Kerberos remote user ID.

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.

If you are using 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 task roles include:

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

You can perform the following operations in the **User profiles** page:

- Creating a new user profile
- Copying an existing user profile for a user
- Editing a user profile
- Deleting user profiles

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

1. In the navigation area, click **User management** > **User profiles**.
2. In the work pane, complete the following steps:
   - To create a new user profile, click **Create**. The **Create profile** window opens. Enter the necessary information and click **Create**.
   - To create a user profile with the same attributes as an existing profile, select a user ID, and click **Copy**. The **Copy profile** window opens. Enter the necessary information and click **Copy**.

     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.
   - To change the attributes of an existing user profile, select a user ID and click **Edit**. The **Edit profile** window opens. Enter the necessary information and click **Edit**.
   - To delete user profiles, select one or more user IDs, and click **Delete**. The **Delete user profile** window opens. A confirmation message is displayed for the deletion of selected user profiles. Click **Delete** to delete the user profiles that are displayed.

   Note: From the **Create profile**, **Copy profile**, and **Edit profile** windows, you can modify the following attributes:

   - **User ID**: Enter the user ID for the user profile that 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 expiration in days**: Specify the number of days a password is valid before it expires.
   - **Session settings**: Specify the session properties for the user profile.
   - **Allow remote access via the web**: Select this option to enable remote web server access for the user profile.
   - **Allow remote access via the SSH**: Select this option to enable remote web server access through SSH for the user profile.
   - **Task roles**: Displays the task roles that are currently available. Select one task role for this user ID.

- **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.

Notes:

- You can search for any data within the table by typing a relevant keyword in the search bar.
- You can customize the columns in the user profiles table by clicking the **Customize columns** icon.
- You can export the user profiles data by clicking the **Export** icon. The following formats are supported for exporting option:
  - PNG
  - PDF
  - CSV

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

Resource roles

You can use this task to define and customize managed resource 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 that are 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 **User profiles and access** task to create new users with their own permissions.

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

The predefined managed resource roles include:

- All System Resources

You can perform the following operations in the **Resource roles** page:

- Creating a resource role
- Editing an existing resource role
- Copying an existing managed resource role to a new managed resource role
- Deleting existing resource roles

To customize managed resource roles, complete the following steps:

1. In the navigation area, click **User management** > **Resource roles**.
2. In the work pane, complete one of the following steps:
   - To create a new resource role, click **Create**. The **Create resource role** window opens. Enter the necessary information and click **Create**.
   - To create a resource role with the same attributes as an existing resource role, select a resource role, and click **Copy**. The **Copy resource role** window opens. Enter the necessary information and click **Copy**.
   - To change the attributes of an existing resource role, select a resource role and click **Edit**. The **Edit resource role** window opens. Enter the necessary information and click **Edit**.
   - To delete resource roles, complete the following steps:
     - Select one or more resource roles and click **Delete**. The **Delete resource role** confirmation window opens.

- Select the **Force** option, if the resource role needs to be deleted even if it has an associated user.
- Click **Delete** to complete the delete operation.

Notes:

- You can search for any data within the table by typing a relevant keyword in the search bar.
- You can customize the columns in the resource roles table by clicking the **Customize columns** icon.
- You can export the resource roles data by clicking the **Export** icon. The following formats are supported for exporting option:
  - PNG
  - PDF
  - CSV

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

Task roles

You can use this task to define and customize task roles.

Notes:

- You cannot edit the task role objects that are defined by the system.
- Each new task role is based on another task role and the newly defined task role cannot have more authority than the one on which it is based.

You can perform the following operations in the **Task roles** page:

- Creating a task role
- Editing an existing task role
- Copying an existing managed resource role for a new task role
- Deleting existing task roles

To add or customize a task role, complete the following steps:

1. In the navigation area, click **User management** > **Task roles**.
2. In the work pane, complete one of the following steps:
   - To create a new task role, click **Create**. The **Create task role** window opens. Enter the necessary information and click **Create**.
   - To create a task role with the same attributes as an existing task role, select a task role, and click **Copy**. The **Copy task role** window opens. Enter the necessary information and click **Copy**.
   - To change the attributes of an existing task role, select a task role and click **Edit**. The **Edit task role** window opens. Enter the necessary information and click **Edit**.
   - To delete task roles, complete the following steps:
     - Select one or more task roles and click **Delete**. The **Delete task role** confirmation window opens.
     - Select the **Force** option, if the task role needs to be deleted even if it has an associated user profile.
     - Click **Delete** to complete the delete operation.

Notes:

- You can search for any data within the table by typing a relevant keyword in the search bar.
- You can customize the columns in the task roles table by clicking the **Customize columns** icon.
- You can export the task roles data by clicking the **Export** icon. The following formats are supported for exporting option:

- PNG
- PDF
- CSV

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

LDAP

Configure your Hardware Management Console (HMC) so that it uses Lightweight Directory Access Protocol (LDAP) authentication.

Before you begin

When you log in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote LDAP server for the user authentication. Configure your HMC so that it uses LDAP remote user authentication.

Note: Before you configure the HMC so that it uses LDAP authentication, you must make sure that a working network connection exists between the HMC and the LDAP servers.

About this task

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

Procedure

1. In the navigation area, click **User management** > **LDAP**. The **LDAP** window opens.
2. Set **Enable authentication** to on to enable LDAP authentication on the HMC by using LDAP servers that are listed for the primary and the backup URI.
3. Define an LDAP server to use for authentication in the **Primary URI** field. Specify a primary URI for the LDAP server that you want to use.
   For example: Microsoft Active Directory, Tivoli®, and Open LDAP).
4. You can also define a backup LDAP server to use for authentication in the **Backup URI** field.
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. Specify the search scope in the **Specify search page** field. You can limit the search of the LDAP server for the user ID. The two options that are available are:
   - one
   - sub

   The default value is **one**.
7. Select **Enable TLS Encryption (STARTTLS)** to enable Transport Layer Security (TLS) on the connection between the HMC and the LDAP server. TLS provides data confidentiality (third parties cannot read the data) or data integrity protection (protection from tampering).
8. Select the **Use non-anonymous binding** option, if the LDAP server does not support anonymous binding. Enter **Bind DN** and **Bind password**.
9. Define the **Distinguished name tree for search**, also known as the search base, for the LDAP server. You can use this field to specify the search criteria for the LDAP server that is used to locate the user record to authenticate the user. For example, **dc=example, dc=com**. Click **Add** to add one or more distinguished name trees to the LDAP server. All the distinguished name trees that are added by the user are displayed. If you want to delete any distinguished name tree, click **X** icon that is displayed next to the distinguished name tree.
10. Complete the following steps to configure LDAP for remote user management:
    a. Select **Enable LDAP for remote user management**.

b. Define the LDAP attribute that locates and retrieves the role and authorization properties of the user being authenticated in the **LDAP attribute to retrieve user properties** field.

c. You can also specify a value for the **LDAP group log in** field so that you can retrieve the group login information for a specific user from the LDAP server when required.

d. You can specify a value for the **Attributes for group members** field so that you can retrieve the member information for a specific user when required.

e. You can specify a filter to use to limit the search of the LDAP server for the user ID of the user being authenticated in the **Additional search filter** field.

f. Select **Use Kerberos for user authentication** option to specify that the remote user is to be authenticated by Kerberos.

g. You can specify an LDAP attribute to locate and retrieve the remote authentication name from the LDAP server in the **LDAP attribute to retrieve remote user ID** field.

Note: For more information about configuring the HMC so that it uses LDAP remote user management, see Configuring the HMC so that it uses LDAP remote user management.

11. Click **Save**.

What to do next

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

KDC

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

Before you begin

- 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 **Date and time** task from **HMC management**, and then selecting **HMC settings**.
- Set the user profile of each remote user to use Kerberos remote authentication instead of local authentication. A user that is set to use Kerberos remote authentication always uses Kerberos remote authentication, even when the user logs on to the HMC locally.

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

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

  Using the Kerberos ktutil on the Kerberos server, verify the file content of the service key. The output looks like the following example:

  – `# ktutil`

  ```
  ktutil: rkt /etc/krb5.keytab
  ktutil: l
  slot KVNO Principal
  ---- ----
  ---------------------------------------------------------------------
  ```

```
1 9 host/hmc1.example.com@EXAMPLE.COM
2 9 host/hmc1.example.com@EXAMPLE.COM
```

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

About this task

From this task, you can complete the following tasks:

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

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

Under Kerberos, a client (either a user or a service) sends a request for a ticket to the KDC. The KDC creates a ticket-granting ticket (TGT) for the client, encrypts it using the client's password as the key, and sends the encrypted TGT back to the client. The client then attempts to decrypt the TGT, by using its password. If the client successfully decrypts the TGT (for example, if the client gave the correct password), it keeps the decrypted TGT, which indicates proof of the client's identity.

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

A Kerberos realm is an administrative domain, site, or logical network that uses Kerberos remote authentication. Each realm uses a primary 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 secondary KDC servers that store read-only copies of the primary Kerberos database for that realm.

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

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

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

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

To use KDC remote authentication for the HMC, complete the following steps:

Procedure

1. In the navigation area, click **User management** > **KDC**. The **Key distribution center configuration** page opens.

2. Select **Enable authentication**.
3. Complete the following steps to configure KDC servers:
   a) **Default realm**: Specify the default Kerberos realm that you want to use for this HMC. A realm is an authentication administrative domain. Normally, realms always appear in uppercase letters. It is good practice to create a realm name that is the same as your DNS domain (in uppercase 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.
   b) **Ticket lifetime**: Specify the number of seconds for which a ticket that is issued by the KDC server must be valid. The default ticket lifetime is 24000 seconds (6 hours and 40 minutes). Ticket lifetime sets the lifetime for credentials. The format is an integer number followed by one of the following options: **s** seconds, **m** minutes, **h** hours, or **d** days.
   For example: Enter a Kerberos ticket lifetime string such as *2d4h10m*.
   c) **Clock skew**: Specify the maximum number of seconds that the HMC time is allowed to differ from the KDC server time for a successful authentication. This allows users to authenticate successfully even when the HMC time and the KDC server time differ slightly. 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 the number of seconds. The default value for clock skew is 120 seconds.
   d) **Authentication timeout**: Specify the maximum number of seconds after an online authentication request to KDC server is aborted from HMC. The default value for authentication timeout is 6 seconds.
4. Complete the following steps to configure KDC service key:
   a) Click **Import service key** to import a KDC service key. After you import a service-key file into the HMC, you must restart the HMC for the change to take effect.
   b) To remove a service-key file from this HMC, click **Remove service key**. Restart the HMC after you delete a service-key file from the HMC.
5. Complete the following steps to manage KDC servers:
   a) To add a KDC server, complete the following steps:
      i) Click **Add KDC server**. The **Add KDC server** window opens.
      ii) Enter **Hostname or IP Address** and **Realm**.
      iii) Click **Add KDC server**.
   b) To edit an existing KDC server, select a KDC server from the list and click **Edit**.
   c) To delete KDC servers, select KDC servers from the list and click **Delete**.
6. Click **Save**.

What to do next

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

MFA

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

Notes:

- By default, MFA is disabled on the HMC.
- For HMC graphical user interface (GUI) login, when MFA is enabled and the user is configured on the PowerSC MFA server, enter the Cache Token Credential (CTC) code in the password field.
- For Secure Shell (SSH) login, when MFA is enabled, all users that login through SSH are prompted for a CTC code. If the user is configured on the PowerSC MFA server, then you can enter the CTC code at the prompt. If the user is not configured on the PowerSC MFA server, press `Enter` when prompted for CTC code, and then enter the password of the user at the prompt.

- When PowerSC MFA is enabled, all users are prompted for PowerSC MFA authentication process. To exempt any user from the PowerSC MFA authentication process when they login to the HMC through the command-line interface (CLI) or SSH, add the user to the PowerSC MFA **allowlist** in the HMC.

To enable MFA, complete the following steps:

1. In the navigation area, click **User management** > **MFA**.
2. Select **Enable authentication**.
3. Enter the following information:
   - **Server hostname or IP address** of the authentication server.
   - **Port** of the authentication server.
4. Click **Save**.

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

User management tasks for HMC Version 10.3.1050.0, or earlier

The tasks that are available on the HMC for User management are described.

Note: Depending on the task roles assigned to your user ID, you might 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 that are allowed to access them.

Users and tasks

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

1. In the navigation area, click **User management**, and then select **Users and tasks**.
2. In the **Users and Tasks** window, the following information displays:
   - User you are logged in as
   - Time you logged in
   - Number of tasks running
   - Your access location
   - Information about tasks that are running:
     - Task ID
     - Task name
     - Targets (if any)
     - Session ID
3. Choose to log off or disconnect from a session that is currently running by selecting the session from the Users **Logged On** list, then click **Logoff** or **Disconnect**.

   Alternately, you can choose to switch to another task or end a task by selecting the task from the **Running Tasks** list, then click **Switch To** or **Terminate**.
4. When you have completed this task, click **Close**.

User profiles and access

Manage your system users that log on to the HMC. A user profile is a combination of a user ID, server authentication method, permissions, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

Users can be authenticated using local authentication on the HMC, by using Kerberos remote authentication, or by using LDAP authentication. For more information on setting up Kerberos

authentication on the HMC, see "KDC" on page 139. For more information about LDAP authentication, see "LDAP" on page 138.

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

If you are using local authentication, the user ID and password are used to verify a user's authorization to log on the HMC. The user ID must start with an alphabetic character and consist of 1 to 32 characters. The password has the following rules:

- Must begin with an alphanumeric character.
- Must contain at least 8 characters, however, this limit can be changed by your system administrator.
- The characters must be standard 7-bit ASCII characters.
- Valid characters to use for the password can be: A-Z, a-z, 0-9 and special characters (~ ! @ # $ % ^ & * ( ) _ + - = { } [ ] \ : " ; ').

If you are using Kerberos authentication, specify a Kerberos remote user ID.

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

The user profile includes managed resource roles and task roles that are assigned to the user. The *managed resource roles* assign permissions for a managed object or group of objects and the *task roles* define the access level for a user to perform on a managed object or group of objects. You can choose from a list of available default managed resource roles, task roles, or customized roles that are created by using the **Manage Task and Resource Roles** task.

See "HMC tasks, user roles, IDs, and associated commands" on page 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, click **User management**, and then select **User profiles and access**.
2. Complete one of the following steps:
   - From the **User Profiles** window, if you are creating a new user ID, point to **User** on the menu bar and when its menu is displayed, click **Add**. The **Add User** window is displayed.
   - From the **User Profiles** window, if 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.

3. Complete or change the fields in the window, click **OK** when you are done.

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

Adding, Copying, or Modifying User Profiles

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

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

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

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

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

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

User Properties

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

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

Timeout Values

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

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

Inactivity Values

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

Tasks 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 **User profiles and access** task to create new users with their own permissions.

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

The predefined managed resource roles include:

- All System Resources

The predefined task roles include:

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

To customize managed resource roles or task roles:

1. In the navigation area, click **User Management**, and then select **Tasks and resource roles**.
2. From the **Customize User Controls** window, select either **Managed Resource Roles** or **Task Roles**.
3. To add a role, click **Edit** from the menu bar, then click **Add** to create a new role.

   or

   To copy, remove, or modify an existing role, select the object you want to customize, click **Edit** from the menu bar, then click **Copy**, **Remove**, or **Modify**.
4. Click **Exit** when you are have completed the task.

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

LDAP

Configure your HMC so that it uses LDAP (Lightweight Directory Access Protocol) authentication.

Before you begin

When you log in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote LDAP server for the user authentication. You must configure your HMC so that it uses LDAP remote user 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.

About this task

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

Procedure

1. In the navigation area, click **User management**, and then select **LDAP**. The **LDAP Server Definition** window opens.
2. Select **Enable LDAP**.
3. Define an LDAP server to use for authentication.
   Example: Microsoft Active Directory, Tivoli, and Open LDAP).
4. 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.
5. Define the distinguished name tree, also known as the search base, for the LDAP server. You can use this field to specify the search criteria for the LDAP server that is used to locate the user record to authenticate the user. For example, **dc=example, dc=com**. Click **Add** to add more than one distinguished name tree to the LDAP server. All the distinguished name trees that are added by the user is displayed in a list. If you want to delete an entry in the list, select the distinguished name tree and click **Remove**.
6. Specify the search scope for limiting the search of the LDAP server for the user ID of the user being authenticated. The two options that are available are:
   - one
   - sub

   The default value is **one**.
7. For more information about configuring the HMC so that it uses LDAP remote user management, see Configuring the HMC so that it uses LDAP remote user management.
8. Click **OK**.

What to do next

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

KDC

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

From this task, you can complete the following tasks:

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

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

Under Kerberos, a client (generally either a user or a service) sends a request for a ticket to the KDC. The KDC creates a ticket-granting ticket (TGT) for the client, encrypts it using the client's password as the key, and sends the encrypted TGT back to the client. The client then attempts to decrypt the TGT, by using its password. If the client successfully decrypts the TGT (for example, if the client gave the correct password), it keeps the decrypted TGT, which indicates proof of the client's identity.

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

A Kerberos realm is an administrative domain, site, or logical network that uses Kerberos remote authentication. Each realm uses a primary 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 secondary KDC servers that store read-only copies of the primary Kerberos database for that realm.

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

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

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

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

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

- You must enable the Network Time Protocol (NTP) service on the HMC and set the HMC and the KDC servers to synchronize time with the same NTP server. You can enable the NTP service on the HMC by accessing the **Date and time** task from **HMC management**, and then selecting **HMC settings**.
- You must set the user profile of each remote user to use Kerberos remote authentication instead of local authentication. A user that is set to use Kerberos remote authentication always uses Kerberos remote authentication, even when the user logs on to the HMC locally.

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

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

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

  –
  ```
  # ktutil
  ktutil: rkt /etc/krb5.keytab
  ktutil: l
  slot KVNO Principal
  ---- ----
  ---------------------------------------------------------------------
  1 9 host/hmc1.example.com@EXAMPLE.COM
  2 9 host/hmc1.example.com@EXAMPLE.COM
  ```
- The HMC Kerberos configuration can be modified for SSH (Secure Shell) login without a password by using GSSAPI. For remote login without a password through Kerberos to an HMC, configure the HMC to use a service key. After the configuration is completed, use `kinit -f principal`

to obtain forwardable credentials on a remote Kerberos client machine. You can then enter the following command to log in to the HMC without having to enter a password: `$ ssh -o PreferredAuthentications=gssapi-with-mic user@host`.

To manage the KDC, complete the following steps:

1. In the navigation area, click **User management**, and then select **KDC**.
2. From the **Manage KDC** window, select the appropriate task from the available options under the **Actions** menu.
3. When you complete the task, click **OK**.

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

View KDC Server

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

To view existing KDC Servers on your HMC, click **User management**, and then select **KDC**. 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, click **User management**, and then select **KDC**.
2. Select a KDC Server.
3. Select a value to modify:
   - **Realm**. A realm is an authentication administrative domain. Normally, realms always appear in upper case letters. It is good practice to create a realm name that is the same as your DNS domain (in upper case letters). A user belongs to a realm if and only if the user shares a key with the authentication server of that realm. Realm names must be equivalent to the network domain name if a service key file is installed on the HMC.
   - **Ticket Lifetime**. Ticket lifetime sets the lifetime for credentials. The format is an integer number followed by one of **s** seconds, **m** minutes, **h** hours, or **d** days. Enter a Kerberos lifetime string such as *2d4h10m*.
   - **Clock skew**. Clock skew sets the maximum allowable amount of clock skew between the HMC and the KDC server before Kerberos considers messages invalid. The format is an integer number that represents number of seconds.
4. Click **OK**.

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, click **User management**, and then select **KDC**.
2. From the **Actions** drop down list, select **Add KDC Server**.
3. Enter the host name or IP address of the KDC server.
4. Enter the KDC server realm.
5. Click **OK**.

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, click **User management**, and then select **KDC**.
2. Select the KDC server from the list.
3. From the **Actions** drop down list, select **Remove KDC Server**.
4. Click **OK**.

Import Service Key

Before you can import a service key file into an 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, click **User management**, and then select **KDC**.
2. From the **Actions** drop down list, select **Import Service Key**.
3. Select from one of the following:
   - **Local** - The service key must be located on removable media currently mounted on the HMC. You must use this option locally at the HMC (not remotely), and you must mount the removable media to the HMC before using this option. Specify the full path of the service key file on the media.
   - **Remote** - The service key must be located on a remote site available to the HMC via secure FTP. You can import a service key file from any remote site that has SSH (Secure Shell) installed and running. Specify the hostname of the site, a user ID and password for the site, and the full path of the service key file on the remote site.
4. Click **OK**.

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

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, click **User management**, and then select **KDC**.
2. From the **Actions** drop down list, select **Remove Service Key**.
3. Click **OK**.

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

MFA

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

Notes:

1. Multi-Factor Authentication is disabled on the HMC by default.

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

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

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

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

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

Enable Remote Command Execution

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

1. In the navigation area, click **Users and Security**, 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, click **Users and Security**, 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, click **Users and Security**, 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.

Logs

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

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 **Logs**, and then select **Tasks log**.

   Note: Alternatively, you can access **Tasks log** by clicking **System resources** > **Systems** and then click the system for which you want to view the tasks log. The **Tasks log** task is displayed menu pod.
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 log

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 logs, complete the following steps:

1. In the navigation area, click **Logs**, and then select **Console events log**.
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.

Serviceability tasks for HMC versions between 10.2.1030.0 and 10.3.1060.0

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.

Serviceable events

This task allows you to select the criteria for the set of serviceable events you want to view. When you finish selecting the criteria, you can view the serviceable events that match your specified criteria.

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

1. In the navigation area, click **Serviceability**, and then select **Serviceable events**.
2. You can modify the event criteria, error criteria, and FRU criteria to refine the list of serviceable events that you want to view.
3. Click **Refresh** to refresh the list of events that are based on the selected filter values.
4. Select the serviceable events that match your selection criteria and click **Action** to manage the selected serviceable events.
5. Click **View** to see the complete details of the serviceable events.

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

Events manager for call home

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

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

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

Create serviceable event

This task reports problems that occurred on your Hardware Management Console (HMC) to the service provider (for example, the mouse does not work) or lets you test problem reporting.

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

Reporting a problem

To report a problem on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Create serviceable events**.
2. Enter a brief description of your problem in the **Problem Description** field and then click **Request Service**.

To test problem reporting from the **Create Serviceable Event** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem Description** 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.

Reporting a problem after selecting a system

To report a problem after selecting a system on your Hardware Management Console, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select a managed system and click **Service** > **Create serviceable event**.
3. In the **Create Serviceable Event** window, you can select a **Problem Type** that describes where the problem occurred or what is the problem.
4. Enter a brief description of your problem in the **Problem Description** field and then click **Request Service**.

To test problem reporting from the **Create Serviceable Event** window, complete the following steps:

1. Select **Test problem reporting** and enter *This is just a test* in the **Problem Description** 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.

Dumps

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

To manage a dump for HMC Versions 10.2.1030 and 10.2.1040, complete the following steps:

1. In the navigation area, click **Serviceability** and then select **Dumps**.
2. From the **Manage Dumps** window, select a dump-related task.

   Click **Action** to perform the following tasks:

   - View dump details.
   - Copy the dump to the media.
   - Copy the dump to a remote system.
   - Use the call home feature to transmit the dump to your service provider.
   - Delete a dump.

   Click **Initiate Dump** to perform the following tasks:

   - Initiate a resource dump.
   - Initiate a system controller dump.
   - Initiate a system dump.
3. Click **Refresh** to update and redisplay the data in the dump table.
4. Click **System Dump Parameters** to display and alter the dump parameters.

   Note: This option is available only for the flexible service processor (FSP) based systems.

To manage a dump for the HMC Version 10.3.1050, or later, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Dumps**.
2. In the content pane, select a dump-related task to perform the following tasks:

- Use the call home feature to transmit the dump to your service provider.
- Delete a dump.
- Save the dump to the media.
- Save the dump to a remote system.

Click **Initiate dump** to perform the following tasks:

- Initiate a resource dump.
- Initiate a system controller dump.
- Initiate a system dump.

3. Click **Refresh** icon to update and redisplay the data in the dump table.
4. Click **Edit system dump settings** to display and alter the dump settings.

   Note: This option is available only for the flexible service processor (FSP) based systems.

Notes:

1. You can search for a dump by typing the file name of the dump as a keyword in the search bar that is available at the beginning of the **Dumps** table.
2. You can customize the columns in the Dumps table by clicking the **Customize columns** icon.
3. You can export dumps data by clicking the **Export** icon. The following file formats are supported for the **Export** option:
   - PNG
   - PDF
   - CSV

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 **Serviceability**, and then select **Transmit service information**.
2. In the **Transmit Service Information** window, click the **Schedule and Send Data** tab to transmit the service information to your service provider immediately or to schedule the transmission.
   a. 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**: Verify and update the Access Key information.
      - **Disk Health**: Send the disk health information such as idle time, power on hours, reassigned sectors, and soft errors.
      - **Fix Level Reporting Tool (FLRT)**: Send the Fix Level Reporting Tool information.
   b. Select the interval (in days) and the time to schedule repeating transmissions. To transmit the information immediately, click **Send Now**.
   c. Click **Save** to save the schedule information.

3. You can also click the following tabs to select the data that you want to send and to configure FTP connections:
   - **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.

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

Remote support connection

Manage the service connection that securely accesses the remote system.

To manage the connection that service uses to securely access the system remotely, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Remote support connection**.
2. In the **Remote support connection** window,
   a. Click Open to keep the connection open. When you select the Open option, you must specify the Connection timeout (minutes) period.
   b. Click `Close` to close the remote support connection.
3. 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.

Prerequisites for managing a Remote support connection

Learn about the prerequisites for enabling remote access for your Hardware Management Console (HMC).

About this task

Notes:

- IBM can remotely connect to your system to perform maintenance actions by using remote access. Remote access can be enabled as needed for a specified time limit up to 2 days.
- It is recommended that you install and configure the **`Remote Support Proxy`** service to simplify firewall configurations. One **`Remote Support Proxy`** can be used by multiple systems and by other management consoles.

Step 1. Configuring a firewall rule

Before you begin

With a Remote Support Proxy server

Use the following information to configure a firewall rule after you install and configure the Remote Support Proxy server:

Source	IP address of the Remote Proxy Server
Target	129.33.206.139 and 204.146.30.139
Port	443
Protocol	https
Direction	Outbound only

Note: You also need to configure the IP address of the Remote Support Proxy server into the system.

Without a Remote Support Proxy server

If the Remote Support Proxy server is not installed and configured, use the following information to configure a firewall rule:

Source	The service IP address of every management console that is running the remote support center service
Target	129.33.206.139 and 204.146.30.139
Port	22
Protocol	ssh
Direction	Outbound only

Step 2. Installing Remote Support Proxy

About this task

The Remote Support Proxy utility must be installed in the following situations:

- Your system does not have internet access.
- You want to route multiple systems to the support center through a single system. This way, firewall restrictions need to be disabled only for a single system.
- All nodes in your system have service IP addresses configured in IPv6 format. In this case, the Remote Support Proxy needs to listen on an IPv6 interface, which needs to be defined on your system as a support center.

To download and install the Remote Support Proxy utility, complete these steps:

Procedure

1. On the Linux computer where you plan to run the proxy utility, download the Remote Support Proxy utility installation package and Release Notes from the Fix Central website.
2. Assign the downloaded file execution permissions by running the following command:

   ```
   chmod +x file_name.bin
   ```

   where **file_name.bin** is the name of the installation package.
3. Install the Remote Support Proxy utility by using the following command:

   ```
   ./file_name.bin
   ```

   where **file_name.bin** is the name of the installation package for the system.
4. A software license is displayed.
5. Follow the instructions and accept the license. The installation program installs an RPM package that is named supportcenter_proxy and then exits.

   Note: Occasionally, the license is not displayed and the application ends unexpectedly. The license cannot be displayed when the **bzip2** package is missing on the system. Use the Linux package manager to reinstall the **bzip2** package to the system and try again.

   The following files are installed on the local system:

/usr/bin/supportcenter_proxy	The binary executable file.
/etc/supportcenter/proxy.conf	The configuration file. You must update this file before you start the Remote Support Proxy service.

/etc/init.d/supportcenter_proxy	The system service for starting and stopping the Remote Support Proxy. The service is configured to start when the server boots. It does not start automatically after installation.
/usr/share/supportcenter/syslog-logger	The logger program that can be modified to integrate with the existing logging and monitoring systems.
/usr/share/doc/proxy-version/license	The directory that contains the accepted software license for the Remote Support Proxy in multiple languages. In the directory path, version is the product version.
/usr/share/supportcenter/proxy_id_rsa	A cryptographic file that is used by the configuration-retrieval function.

Step 3. Configuring Remote Support Proxy

Before you begin

After you install the Remote Support Proxy on the system, you must configure it. The Remote Support Proxy is required when remote support assistance is configured on systems that do not have direct access to the internet.

To configure the Remote Support Proxy service with the system, change the following required parameters in the **/etc/supportcenter/proxy.conf** file:

ListenInterface	Specifies the IPv4 address, IPv6 address, or interface name on which the proxy service must listen for incoming connections from the system (for example, 192.0.2.1, 2001:DB8:0:0:0:0:0:0, or eth0). • If you specify an IPv4 or IPv6 address, the proxy service listens on only the specified IP address. • If you specify an interface name, the proxy service listens on all allowed addresses. You can configure which addresses are allowed by setting the **UseIPv4**, **UseIPv6,** and **UseIPv6LinkLocalAddress** parameters. By default, the proxy service listens on both IPv4 and IPv6 addresses. • If you specify the interface name, the name must be the same as the output from the **ifconfig** command. **Important:** The storage system must have access to the system that runs the Remote Support Proxy as defined by this interface name or IP address.
ListenPort	The TCP port on which the Remote Support Proxy must listen for incoming connections from the system. For example: 8988. **Important:** The storage system must have access to the system running the Remote Support Proxy as defined by this port.

ServerAddress	The TCP port on which the Remote Support Proxy must listen for incoming connections from the system. Add the following strings to the configuration file:
	`ServerAddress1 129.33.206.139`
	`ServerPort1 443`
	`ServerAddress2 204.146.30.139`
	`ServerPort2 443`

Step 4. Starting Remote Support Proxy

Procedure

After you update the Remote Support Proxy configuration file, start the Remote Support Proxy service. To start the Remote Support Proxy service, run the following command:

```
service supportcenter_proxy start
```

Note: If the proxy service does not start correctly, examine the log file for errors. The default log file is **`/var/log/supportcenter_proxy.log`**.

Remote operations

Connect to and use the Hardware Management Console (HMC) remotely.

Remote operations use the GUI used by a local HMC operator or the command line interface (CLI) on the HMC. You can perform operations remotely in the following ways:

- Use a remote HMC.
- Use a web browser to connect to a local HMC.
- Use an HMC remote command line.

The remote HMC is an HMC that is on a different subnet from the service processor, therefore the service processor cannot be auto discovered with IP multicast.

To determine whether to use a remote HMC or web browser that is connected to a local HMC, consider the scope of control that you need. A remote HMC defines a specific set of managed objects that are directly controlled by the remote HMC, while a web browser to a local HMC has control over the same set of managed objects as the local HMC. The communications connectivity and communications speed is an extra consideration. LAN connectivity provides acceptable communications for either a remote HMC or web browser control.

Using a remote HMC

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

As a complete HMC, a remote HMC has the same setup and maintenance requirements as a local Hardware Management Console. A remote HMC needs LAN TCP/IP connectivity to each managed object (service processor) that is to be managed; therefore, any customer firewall that might exist between the remote HMC and its managed objects must allow the HMC to service processor communications to occur. A remote HMC might also need communication with another HMC for service and support. Table 11 on page 152 shows the ports that a remote HMC uses for communications.

Table 11. Ports used by a Remote HMC for Communications	
Port	**Use**
udp 9900	HMC to HMC discovery
tcp 9920	HMC to HMC commands

A remote HMC needs connectivity to IBM (or another HMC that has connectivity to IBM) for service and support. The connectivity to IBM might be in the form of access to the internet (through a company firewall).

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

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

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

Using a web browser

If you need occasional monitoring and control of managed objects that are connected to a single local Hardware Management Console (HMC), use a web browser. An example of using the web browser might be an off-hours monitor from home by an operator or system programmer.

Each HMC contains a web server that can be configured to allow remote access for a specified set of users. If a customer firewall exists between the web browser and the local HMC, the ports must be accessible and the firewall setup to allow incoming requests on these ports. Table 12 on page 152 shows the ports that a web browser needs for communicating with an HMC.

Table 12. Ports that are used by a web browser for communications to the HMC	
Port	**Use**
TCP 443	Secure (HTTPS) remote interface communication
TCP 8443	Secure browser access to web server communication
TCP 9960	Browser applet communication
[1]This port is opened in the HMC firewall when remote access is enabled in HMC Version 7.8.0 and later. This port must also be opened in any firewall that is between the remote client and the HMC.	

After an HMC is configured to allow web browser access, a web browser gives an enabled user access to all the configured functions of a local HMC, except those functions that require physical access to the HMC, such as those that use the local diskette or DVD media. The user interface that is presented to the remote web browser user is the same as that of the local HMC and is subject to the same constraints as the local HMC.

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

Performance and the availability of the status information and access to the control functions of the managed objects depends on the reliability, availability, and responsiveness of the network that interconnects the web browser with the local HMC. Because there is no direct connection between the web browser and the individual managed objects, the web browser does not monitor the connection to

each service processor, does not perform any recovery, and does not report any lost connections. These functions are handled by the local HMC

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

If the URL of the HMC is specified by using the format https://*xxx.xxx.xxx.xxx* (where *xxx.xxx.xxx.xxx* is the IP address) and Microsoft Internet Explorer is used as the browser, a host name mismatch message is displayed. To avoid this message, a Firefox browser is used or a host name is configured for the HMC, by using the **Change Network Settings** task (see "Network Settings (for HMC versions between 10.2.1030.0 and 10.3.1060.0)" on page 91), and this host name is specified in the URL instead of an IP address. For example, you can use the format https://*host name.domain_name* or https://*host name* (for example, by using https://hmc1.ibm.com or https://hmc1).

Preparing to use the web browser

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

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

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

Web browser requirements

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

HMC web browser support requires HTML 2.0, JavaScript 1.0, Java™ Virtual Machine (JVM), Java Runtime Environment (JRE) Version 7, and cookie support in browsers that connect to the HMC. Contact your support personnel to assist you in determining whether your browser is configured with a Java Virtual Machine. The web browser must use HTTP 1.1. If you are using a proxy server, HTTP 1.1 must be enabled for the proxy connections. Additionally, pop-up windows must be enabled for all HMCs addressed in the browser if the browser is running with pop-up windows disabled. The following browsers have been tested:

Google Chrome
HMC Version 8.1 supports Google Chrome Version 33.

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

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

- If your browser is configured to use an Internet proxy, then local IP addresses are included in the exception list. For more information, see your network administrator. If you still need to use the proxy to get to the Hardware Management Console, enable Use **HTTP 1.1 through proxy connections** under the **Advanced** tab in your Internet Options window.

Mozilla Firefox
HMC Version 8.1 supports Mozilla Firefox Version 17 and Mozilla Firefox Version 24 Extended Support Release (ESR). Ensure that the JavaScript options to raise or lower windows and to move or resize existing windows are enabled. To enable these options, click the **Content** tab in the browser's Options dialog, click **Advanced** next to the Enable JavaScript option, and then select the Raise or lower windows option and the Move or resize existing windows options. Use these options to easily switch between HMC tasks. For more information about the latest Mozilla Firefox ESR levels, see Security Advisories for Firefox ESR.

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

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

Other web browser considerations

Session cookies need to be enabled in order for ASMI to work when connected to HMC remotely. The ASM proxy code saves session information and uses it.

Internet Explorer

1. Click **Tools** > **Internet Options**.
2. Click the **Privacy** tab and select **Advanced**.
3. Determine whether **Always allow session cookies** is checked.
4. If not checked, select **Override automatic cookie handling** and **Always allow session cookies**.
5. For the First-party Cookies and Third-party Cookies, choose block, prompt, or accept. Prompt is preferred, in which case you are prompted every time that a site tries to write cookies. Some sites need to be allowed to write cookies.

Firefox

1. Click **Tools** > **Options**.
2. Click the **Cookies** Tab.
3. Select **Allow sites to set cookies**.
4. If you want to allow only specific sites, select **Exceptions**, and add this HMC to allow access.

Using the HMC remote command line

An alternative to performing tasks on the HMC graphical user interface is using the command line interface (CLI).

You can use the command line interface in the following situations:

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

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

Setting up secure script execution between SSH clients and the HMC

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

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

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

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

1. Enable remote command execution. For more information, see “Enable Remote Command Execution” on page 143.
2. On the client's operating system, run the SSH protocol key generator. To run the SSH protocol key generator, complete the following steps:
   a. To store the keys, create a directory that is named `$HOME/.ssh` (either RSA or DSA keys can be used).

b. To generate public and private keys, run the following command:

```
ssh-keygen -t rsa
```

The following files are created in the $HOME/.ssh directory:

```
private key: id_rsa
public key: id_rsa.pub
```

The write bits for both group and other are turned off. Ensure that the private key has a permission of 600.“

3. On the client's operating system, use ssh and run the `mkauthkeys` command to update the HMC user's authorized_keys2 file on the HMC by using the following command:

```
ssh hmcuser@hmchostname mkauthkeys --add <the contents of $HOME/.ssh/
id_rsa.pub>
```

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

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

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

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

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

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

Enabling and disabling HMC remote commands

You can enable or disable the remote command line interface access to the Hardware Management Console (HMC).

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

1. In the navigation area, click **Users and Security**, and then select **Users and Roles**.
2. In the content pane, click **Enable Remote Command Execution**.
3. From the **Enable Remote Command Execution** window, select from the following options:
   - To enable remote commands, select **Enable remote command execution using the ssh facility**.
   - To disable remote commands, make sure **Enable remote command execution using the ssh facility** is not selected.
4. Click **OK**.

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

Log in to the Hardware Management Console (HMC) remotely from a LAN-connected web browser.

Use the following steps to log in to the HMC from a LAN-connected web browser:

1. Ensure that your web browser has LAN connectivity to the wanted HMC.

2. From your web browser, enter the URL of the wanted HMC in the format `https://hostname.domain_name` (for example: `https://hmc1.ibm.com`) or `https://xxx.xxx.xxx.xxx`.

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

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

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

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

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

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

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

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

About this task

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

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

Add Managed Systems

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

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

1. From the HMC dashboard, click **Connect System**.
2. From the **Add Managed Systems** window, you can add a BMC system by completing the following fields:

   - **IP Address/Host name**
   - **Username (BMC system)**
   - **Password**

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

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

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

Systems Management for Servers

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

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

Operations

Operations contains the tasks for operating managed systems.

Power Off

Shut down the managed system.

Choose from the following options:

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

Power On

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

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

Normal: Select this option to specify that the HMC uses the current setting for the partition start policy to determine how to power on the managed system. The default setting is set to the following value:

- **Auto-Start Always**: This option specifies that the HMC power on logical partitions automatically after the managed system powers on. If powering on the managed system is the result of a user action, the HMC starts all partitions that are configured for automatic startup. If powering on the managed system is the result of an automatic recovery process, the HMC starts only those logical partitions that were running at the time the system is powered off. This option is always available for selection.

Schedule Operations

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

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

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

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

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

From the **Scheduled Operations** window, you can perform the following tasks:

- Schedule an operation to run later.
- Define operations to repeat at regular intervals.
- Delete a previously scheduled operation.
- View details for a currently scheduled operation.

- View scheduled operations within a specified time range.
- Sort scheduled operations by date, operation, or managed system.

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

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

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

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

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

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select one or more managed systems. Click **Connections and operations** > **Schedule operations**.
3. From the **Scheduled Operations** window, click **Options** from the menu bar to display the next level of options:
   - To add a scheduled operation, click **Options** and then click **New**.
   - To delete a scheduled operation, select the operation that you want to delete, point to **Options** and then click **Delete**.
   - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
   - To view a scheduled operation, select the operation that you want to view, point to **View** and then click **Schedule Details**.
   - To change the time of a scheduled operation, select the operation that you want to view, point to **View** and then click **New Time Range**.
   - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
4. To return to the HMC workplace, point to **Operations** and then click **Exit**.

Launch BMC System Management

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

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

To connect to the BMC, complete the following steps:

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

1. In the navigation area, click **System resources**, and then select **Systems**.
2. In the content pane, select one or more managed systems. Click **Connections and operations** > **Launch BMC System Management**.
3. Click **Continue**.

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

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

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

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

   Note: You can set up multiple HMCs to receive traps. Duplicate reporting of events by multiple HMCs is possible as duplicate event verification is not performed.
3. Complete the following fields:
   - **Event Severity**
   - **Destination IP**
4. Click **Save**.
5. Verify the new alert in the table.

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

Rebuild system
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.

To rebuild a managed system, complete the following steps:

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to rebuild, and then click **Connections and operations** > **Rebuild system**. The **Rebuild managed system** window opens.
3. Confirm the system name to rebuild, and click **Rebuild**.

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

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

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

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

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

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

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

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

Attention LED

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

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

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

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

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

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

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

Connections

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

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

Service Processor Status

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

About this task

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

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.

2. In the content pane, select the system for which you want to view service processor connection status.
3. Click **Connections and operations** > **Service processor status**.

Reset or remove system connection

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

About this task

To reset or remove connections, complete the following steps:

Procedure

1. In the navigation area, click **System resources**, and then select **Systems**.
2. Select the system that you want to reset or remove.
3. Click **Connections and operations** > **Reset or remove system connection**.
4. Select **Reset Connection** or **Remove Connection**.
5. Click **OK**.

Notices

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

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

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

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

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

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

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

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

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

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Accessibility features for IBM Power 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 servers include the following major accessibility features:

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

The IBM Power servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with ICT Accessibility 508 Standards and 255 Guidelines (https://www.access-board.gov/ict/) 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 servers.

The IBM Power servers online product documentation in IBM Documentation is enabled for accessibility. For more information about IBM's commitment to accessibility, see the IBM accessibility website at IBM Accessibility (https://www.ibm.com/able/).

Keyboard navigation

This product uses standard navigation keys.

Interface information

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

The IBM Power 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 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 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 10 Release 3 Maintenance Level 1061.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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

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

Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.