System i and System p

Managing your server using the Hardware Management Console

System i and System p

Managing your server using the Hardware Management Console

Note

Before using this information and the product it supports, read the information in "Notices" on page 41 and the *IBM Systems Safety Information* manual, G229-9054.

Twelfth Edition (September 2007)

This edition applies to IBM AIX 5L Version 5.3 and to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Safety and environmental notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the U.S. English publications.

Laser safety information

IBM® System i™ models and System p™ servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM System i models and IBM System p servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:

- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http://www.ibm.com/ibm/environment/products/prp.shtml.

EU Only

Note: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan: Please recycle batteries.

For the European Union:

Note: This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California: Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

IBM Cryptographic Coprocessor Card Return Program

The following information applies only for systems originally sold prior to July 1, 2006:

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Please follow local ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Coprocessor Cards. More information can be found at http://www.ibm.com/ibm/environment/products/prp.shtml.

About this topic

The Hardware Management Console (HMC) uses its network connections to one or more servers or frames (referred to as managed systems) to perform various management functions. This topic provides information about how to perform tasks with the HMC to manage the connected systems.

For information about the accessibility features of this product, for users who have a physical disability, see "Accessibility features," on page 39.

Managing your server, adapters, and devices

Learn about managing servers, adapters, and devices using a console.

Managing your server using the Hardware Management Console

Learn how to manage your server using the Hardware Management Console.

The Hardware Management Console (HMC) uses its network connections to one or more servers or frames (referred to as *managed systems*) to perform various management functions. This topic provides information about how to perform tasks with the HMC to manage the connected systems.

For information about how to perform basic HMC administration tasks, including setting up, installing, and maintaining an HMC, see the Managing the Hardware Management Console (HMC) topic.

For information about partitioning your server using an HMC, see the Partitioning with an HMC topic.

What's new for Managing your server using the HMC

Learn about new or significantly changed information.

The following information highlights newly released or improved content for the *Managing your server using the Hardware Management Console* (HMC) topic.

Adding managed systems to the HMC environment
This information has been improved to take you directly to the information you need to know to add a managed system to your HMC environment depending on your existing network configuration.

Change in parent topic name in the table of contents
If you use the table of contents to navigate to this topic in the Hardware Information Center, note that the name for the parent topic has changed to *Managing your server, adapters, and devices* (adapters has been added to the title).

PDF file for Managing your server using the HMC

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select Managing your server using the Hardware Management Console (about 620 KB).

You can also view or download these related topics in the PDF version:

- Managing the Hardware Management Console (2778 KB)
- Partitioning the server:
  - Partitioning for AIX® (523 KB)
  - Partitioning for i5/OS® (1913 KB)
  - Partitioning for Linux® with an HMC (915 KB)
  - Using the Virtual I/O server (1074 KB)
- Working with Capacity on Demand(1250 KB)
- Customer service, support, and troubleshooting (6300 KB)

Saving PDF files

To save a PDF file on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you would like to save the PDF file.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep2.html) .

HMC concepts for managing servers

Learn about the concepts that you need to know before you use the HMC to work with managed systems.

The HMC allows you to perform a variety of tasks associated with managing your servers and frames. This information familiarizes you with the HMC concepts that you should know before working with the managed systems.

Overview of HMC tasks

Learn about the tasks that you can perform using the HMC, the user role needed to perform each task, and the remote command associated with each task.

See the HMC commands topic for HMC command descriptions.

The following tables list all of the tasks that you can perform using the HMC, the user role needed to perform each task, and the remote command associated with each task. Click one of the following links to learn more about the associated task grouping:

Managed system profile tasks:

Learn about the managed-system profile tasks and the roles that can perform them.

The following table lists the managed system profile tasks, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	**service representative**	**operator**	**product engineer**	**viewer**
Activate a system profile	chsysstate	X	X	X	X	
Create a system profile on a managed system	mksyscfg	X		X		
Modify the properties of a system profile	chsyscfg	X		X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Power on a managed system using a system profile	chsysstate	X	X	X	X	
Remove a system profile	rmsyscfg	X		X		
Validate a system profile	chsysstate	X	X	X	X	
View a system profile	lssyscfg	X	X	X	X	X

For more information about system profiles, see System profile. For more information about using the commands, see Using the remote command line.

Managed system tasks:

Learn about the tasks that enable you to manage your server operations and the roles that can perform these tasks.

The following table describes the managed system tasks, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Add a managed system	mksysconn	X		X	X	
Back up profile data	bkprofdata	X	X	X	X	
Create a network connection with a system	mksysconn	X		X	X	
Enable a remote service session for a logical partition	chsysstate	X	X	X	X	
Enable or disable service processor failover on a managed system	chsyscfg	X		X	X	
Initialize profile data	rstprofdata	X		X		

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Migrate logical partition configuration data to a managed system	migrcfg	X		X	X	
Modify the keylock position of a managed system	chsysstate	X	X	X	X	
Modify the properties of a managed system	chsyscfg	X		X	X	
Modify virtual I/O attributes of a managed system	chhwres	X	X	X	X	
Power a managed system on and off	chsysstate	X	X	X	X	
Rebuild a managed system	chsysstate	X	X	X	X	
Recover partition data for a managed system	chsysstate	X	X	X	X	
Remove the network connection to a managed system	rmsysconn	X		X	X	
Request huge-page memory for a managed system	chhwres	X	X	X	X	
Reset the network connection to a managed system	rmsysconn	X		X	X	
Restart a managed system	chsysstate	X	X	X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Restore the hardware resource configuration of a managed system following a DLPAR task failure	rsthwres	X	X	X	X	
Restore profile data	rstprofdata	X		X		
Update a password for a managed system	chsyspwd	X				
Update the LIC on a managed system	updlic	X	X		X	
View connections for a managed system	lssysconn	X	X	X	X	X
View the current state of readiness for service processor failover on a managed system	lssyscfg	X	X	X	X	X
View HCA adapter resources of a managed system	lshwres	X	X	X	X	X
View hardware resources of a managed system	lshwres	X	X	X	X	X
View I/O resources of a managed system	lshwres	X	X	X	X	X
View LIC levels accepted on a managed system	lslic	X	X	X	X	X
View LIC levels activated on a managed system	lslic	X	X	X	X	X

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
View LIC levels that are available to be retrieved	lslic	X	X	X	X	X
View Licensed Internal Code (LIC) levels installed on a managed system	lslic	X	X	X	X	X
View managed systems	lssyscfg	X	X	X	X	X
View memory resources of a managed system	lshwres	X	X	X	X	X
View processing resources of a managed system	lshwres	X	X	X	X	X
View reference codes for a managed system	lsrefcode	X	X	X	X	X
View SNI adapter resources of a managed system	lshwres	X	X	X	X	X
View virtual I/O resources of a managed system	lshwres	X	X	X	X	X

For more information about working with your managed system using your HMC, see "Working with managed systems and frames" on page 19. For more information about using commands, see Using the remote command line.

Logical partition tasks:

Learn about the logical partition tasks and the roles that can perform them.

The following table describes the tasks that you can execute from the HMC to manage logical partitions. This table provides the commands and the user roles necessary to perform the tasks from the remote command line.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Activate a logical partition	chsysstate	X	X	X	X	
Change the default partition profile for a logical partition	chsyscfg	X		X	X	
Close a virtual terminal session for an AIX, Linux, or Virtual I/O Server partition	rmvterm	X	X	X	X	
Create a logical partition on a managed system	mksyscfg	X		X	X	
Create a logical partition profile on a managed system	mksyscfg	X		X	X	
Create a Virtual I/O Server	mksyscfg	X		X	X	
Issue a command to a Virtual I/O Server	viosvrcmd	X	X	X	X	
Modify memory resources of a logical partition	chhwres	X	X	X	X	
Modify processing resources of a logical partition	chhwres	X	X	X	X	
Modify the properties of a logical partition profile	chsyscfg	X		X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Modify the hardware resource configuration of a logical partition	chhwres	X	X	X	X	
Modify the I/O resources of a logical partition	chhwres	X	X	X	X	
Modify the keylock position on a logical partition	chsysstate	X	X	X	X	
Modify the properties of a logical partition	chsyscfg	X		X	X	
Modify virtual I/O resources of a logical partition	chhwres	X	X	X	X	
Open a virtual terminal session for an AIX, Linux, or Virtual I/O Server partition	mkvterm	X	X	X	X	
Perform a Dynamic Logical Partitioning task	chhwres	X	X	X	X	
Perform a network boot of a logical partition	lpar_netboot	X	X	X	X	
Perform an operator panel function on a logical partition	chsysstate	X	X	X	X	
Remove a logical partition from the managed system	rmsyscfg	X		X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Remove a logical partition profile	rmsyscfg	X		X	X	
Restart a logical partition	chsysstate	X	X	X	X	
Retrieve MAC address and location code for a partition	lpar_netboot	X	X	X	X	
Shut down a logical partition	chsysstate	X	X	X	X	
View HCA adapter resources of a logical partition	lshwres	X	X	X	X	X
View I/O resources of a logical partition	lshwres	X	X	X	X	X
View logical partition profiles	lssyscfg	X	X	X	X	X
View logical partitions	lssyscfg	X	X	X	X	X
View processing resources of a logical partition	lshwres	X	X	X	X	X
View memory resources of a logical partition	lshwres	X	X	X	X	X
View reference codes for a logical partition	lsrefcode	X	X	X	X	X
View SNI adapter resources of a logical partition	lshwres	X	X	X	X	X
View virtual I/O resources of a logical partition	lshwres	X	X	X	X	X

For more information about logical partitions, see Partitioning the server. For more information on using commands, see Using the remote command line.

Capacity on Demand tasks:

Learn about the Capacity on Demand tasks and the roles that can perform them.

The following table lists the Capacity on Demand tasks, the associated command for each task, and the user roles necessary to perform the task.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Activate CoD resources	chcod	X				
Deactivate CoD resources	chcod	X				
Enter a CoD code	chcod	X				
Manage On/Off CoD resources	chcod	X				
Manage Reserve CoD processors	chcod	X				
Stop Trial CoD	chcod	X				
View CoD capacity settings for a managed system	lscod	X	X	X	X	X
View CoD code generation information for a managed system	lscod	X	X	X	X	X
View On/Off CoD billing information for a managed system	lscod	X	X	X	X	X
View the CoD history log for a managed system	lscod	X	X	X	X	X
View shared processor pool utilization information for Reserve CoD	lscod	X	X	X	X	X

For more information about Capacity on Demand, see Working with Capacity on Demand. For more information about using the commands, see Using the remote command line.

Virtualization Engine Technologies tasks:

Learn about Virtualization Engine™ Technologies tasks and the roles that can perform them.

The following table lists the Virtualization Engine Technologies tasks, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
View the Virtualization Engine systems technologies activation history log	lsvet	X	X	X	X	X
Enter Virtualization Engine systems technologies activation code	chvet	X				
View information used to generate a Virtualization Engine systems technologies activation code	lsvet	X	X	X	X	X

For more information about creating a Virtualization Engine Technologies environment, see Using a virtual computing environment. For more information about using commands, see Using the remote command line.

System planning tasks:

Learn about the tasks associated with creating and deploying a system plan and the roles that can perform them.

The following table lists the tasks that you can use when working with a system plan to set up a managed system, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Export a system plan for a managed system	cpsysplan	X				
Import a system plan for a managed system	cpsysplan	X				
List system plans	lssysplan	X				

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Remove a system plan for a managed system	rmsysplan	X				
Deploy a system plan to a managed system	deploysysplan	X				
Create a system plan	mksysplan	X				

For information about how to view a system plan before you deploy it, see Deploying a system plan. For more information about using the commands from the HMC command line, see Using the remote command line.

Utilization data management tasks:

Learn about the management tasks concerned with the collection of system utilization data and the roles that can perform them.

The following table lists the tasks associated with viewing and managing system utilization data, the associated commands, and the user roles necessary to perform them.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Change the settings for utilization-data collection for a managed system	chlparutil	X	X	X	X	
Remove the utilization data collected for a managed system	rmlparutil	X	X	X	X	
View utilization data for a managed system	lslparutil	X	X	X	X	X

For more information about using the commands, see Using the remote command line.

Frame tasks:

Learn about tasks that you can perform to manage your frames and the roles required to perform them.

The following table describes frame tasks, associated commands, and the roles that can perform each task:

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Add a managed frame	mksysconn	X		X	X	
Create a network connection with a frame	mksysconn	X		X	X	
Force an HMC to release its lock on a managed frame	rmlock	X			X	
Modify the properties of a managed frame	chsyscfg	X		X	X	
Power off all unowned I/O units in a managed frame	chsysstate	X	X	X	X	
Rebuild a managed frame	chsysstate	X	X	X	X	
Reset the network connection to a managed frame	rmsysconn	X		X	X	
Remove the network connection to a managed frame	rmsysconn	X		X	X	
Update a password for a managed frame	chsyspwd	X				
View which HMC owns the lock on a managed frame	lslock	X	X	X	X	X
View managed frames	lssyscfg	X	X	X	X	X
View environmental information for a managed frame	lshwinfo	X	X	X	X	X

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
View connections for a managed frame	lssysconn	X	X	X	X	X

For more information about using commands, see Using the remote command line.

Service tasks:

Learn about problem determination tasks and the roles that can perform them.

The following table describes the service tasks that you can perform in the HMC. The associated command and required user role for performing the task are also provided.

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Activate dedicated service tools (DST) on a logical partition	chsysstate	X	X	X	X	
Clear all partition configuration data on a managed system	lpcfgop	X		X		
Copy a managed system or frame dump from the HMC to DVD or a remote FTP server	cpdump	X	X	X	X	
Disable a remote service session for a logical partition	chsysstate	X	X	X	X	
Dump all logical partition configuration data on a managed system	lpcfgop	X		X		
Dump IOP control storage	chsysstate	X	X	X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Enable a remote service session for a logical partition	chsysstate	X	X	X	X	
Enable or disable service processor failover on a managed system	chsyscfg	X		X	X	
Initiate a service processor failover	chsysstate	X	X	X	X	
Launch the Advanced System Management (ASMI) menu	asmmenu	X	X		X	
Modify the state of an LED on a managed system	chled	X		X	X	
Modify the state of a logical partition LED	chled	X		X	X	
Modify Service Agent customer email notification settings	chsacfg	X	X	X	X	
Modify Service Agent FTP firewall settings	chsacfg	X	X	X	X	
Modify Service Agent FTP offload server settings	chsacfg	X	X	X	X	
Perform an operator panel service function on a logical partition	chsysstate	X	X	X	X	
Reset or reload a disk unit IOP	chsysstate	X	X	X	X	

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
Retrieve a dump from a managed system or frame	getdump	X	X	X	X	
Save and display an image of an HMC window	hmcwin	X	X	X	X	X
Start a dump on a managed system or frame	startdump	X	X	X	X	
Transfer a file from the HMC to a remote system using File Transfer Protocol	sendfile	X	X	X	X	X
Update a serviceable event on the HMC	chsvcevent	X	X	X	X	
View available dumps on a managed system or frame	lsdump	X	X	X	X	X
View LED resources of a logical partition	lsled	X	X	X	X	X
View LED resources of a managed system	lsled	X	X	X	X	X
View serviceable events for a managed system	lssvcevents	X	X	X	X	X
View reference codes for a logical partition	lsrefcode	X	X	X	X	X
View reference codes for a managed system	lsrefcode	X	X	X	X	X

Task	Associated command	Roles				
		super administrator	service representative	operator	product engineer	viewer
View Service Agent customer email notification settings	lssacfg	X	X	X	X	X
View Service Agent FTP firewall settings	lssacfg	X	X	X	X	X
View Service Agent FTP offload server settings	lssacfg	X	X	X	X	X
View managed system or managed frame dumps residing on the HMC	lsdump	X	X	X	X	X
View the current state of readiness for service processor failover on a managed system	lssyscfg	X	X	X	X	X

For more information about service and support, see Overview of service and support. For more information about using commands, see Using the remote command line.

Managed system power-on and power-off modes

Learn about the power-on options and the power-off options for a managed system.

This topic describes the power-on options and the power-off options that are available for starting and shutting down a managed system using a console.

The following table describes the power-on options. Power-off options are also available and described in a second table below.

Power-on mode	Description
Partition standby	Use this mode to create and activate logical partitions. When the partition standby power-on is completed, the operator panel on the managed system displays `Partition Standby`, indicating the managed system is ready for you to use the HMC to partition its resources. **Note:** Autostart partitions will not start if you power on using this mode. For more information about logical partitions, see Partitioning the server.
System profile	This option powers on the system according to a predefined set of profiles. **Note:** The profiles are activated in the order in which they are shown in the system profile. For more information about system profiles, see System profile.

Power-on mode	Description
Partition autostart	This option activates logical partitions that have been previously designated as autostart. For more information about logical partitions, see Partitioning the server.

For more information about powering on the managed system, see “Powering on a managed system” on page 20.

Use the following power-off options for shutting down a managed system.

Power-off mode	Description
Normal power off	The Normal power off mode shuts down the system’s operations in a controlled manner. During the shutdown, programs running active jobs are allowed to perform cleanup (end-of-job processing).
Fast power off	The Fast power off mode shuts down the system by stopping all active jobs immediately. The programs running those jobs are not allowed to perform any cleanup. Use this option when you need to shut down the system because of an urgent or critical situation.

Managed system states

Learn about the operational states that are displayed for managed systems in the HMC.

You can monitor the current state of a system (server or frame) that is connected to the HMC. The state for each system that you are managing is displayed in the Contents area of the HMC window, in the column labeled State.

The following table describes the various states for managed systems. To view the states for frames, see “Frame states” on page 19.

State	Description
Power off	The managed system is powered off.
Operating	The managed system is powered on and functioning correctly.
Initializing	The managed system is powering on.
Error	The managed system’s operating system or hardware is experiencing errors. See Correcting the managed system operating state.
Error - Dump in Progress	The managed system has started a system dump. When the dump is complete, see Managing dumps in the Troubleshooting topic.
Error - Terminated	The power-on operation failed.
Incomplete	The HMC failed to get all of the necessary information from the managed system. The managed system is not responding to requests for information. See Correcting the managed system operating state.
Pending Authentication - Password Updates Required	The managed system passwords have not been set. You must set the required passwords for the managed system, to enable secure authentication and access control from the HMC. See “Overview of passwords” on page 21 for information about setting the required passwords.
Failed Authentication	The HMC access password for the managed system is not valid. Enter a valid password for the managed system. See “Overview of passwords” on page 21 for more information about the HMC access password.
Recovery	The partition data and profile data stored in the managed system is damaged. See Correcting the managed system operating state.

State	Description
No Connection	The HMC cannot contact the managed system. See Correcting the managed system operating state.
Standby	The managed system was powered on using the partition standby power-on option.
On Demand Recovery	The anchor card has been replaced; activation codes for Capacity On Demand must be entered again.

Frame states

Learn about the various operational states that are displayed for frames in the HMC.

The following table describes the states for frames that the HMC displays in the Contents area under the State label.

State	Description
Starting/Unknown	One of the bulk power assemblies (BPAs) contained in the frame is in the process of starting. The state of the other BPA cannot be determined.
Standby/Standby	Both of the bulk power assemblies (BPAs) contained in the frame are in the standby state. A BPA in the standby state is operating normally.
Standby/Starting	One of the bulk power assemblies (BPAs) contained in the frame is operating normally (in standby state). The other BPA is in the process of starting.
Standby/Not Available	One of the bulk power assemblies (BPAs) contained in the frame is operating normally (in the standby state), but the other BPA is not operating normally.
Pending frame number	A change to the frame number is in progress. No operations can be performed when the frame is in this state.
Failed Authentication	The HMC access password for the frame is not valid. Enter a valid password for the frame. See “Overview of passwords” on page 21 for more information about the HMC access password.
Pending Authentication - Password Updates Required	The frame access passwords have not been set. You must set the required passwords for the frame, to enable secure authentication and access control from the HMC. See “Overview of passwords” on page 21 for information about setting the required passwords.
No Connection	The HMC cannot connect to the frame.
Incomplete	The HMC failed to get all of the necessary information from the managed frame. The frame is not responding to requests for information. See Correcting the managed system operating state.

Note: For information about the operational states of the managed systems contained in the frame, see “Managed system states” on page 18.

Working with managed systems and frames

Learn how to perform actions on the HMC that pertain to the managed system.

You can use the HMC to communicate with the managed systems and frames in your environment. For example, you can use power-on options to start and shut down your managed systems, and to monitor system states.

Use the information in this topic to learn more about the tasks that you can perform using the HMC to work with the managed system and frames.

Powering on and off a managed system

Read about how to use the HMC to power on and off a managed system. Also find information about scheduling managed-system power operations.

You can use the HMC to control the power on a managed system. The following tasks describe these activities:

Note: For information about the power-on states that display for managed systems in the HMC, see "Managed system states" on page 18.

Powering on a managed system:

Understand how to power on a managed system using the HMC.

You can use the HMC to power on a managed system and to monitor the power-on state.

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

- super administrator
- service representative
- operator
- product engineer

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

1. In the Navigation area, expand the **Server and Partition** folder.
2. Click the **Server Management** icon.
3. In the Contents area, select the managed system.
4. From the menu, click **Selected → Power On**.
5. Select the desired power-on mode and click **OK**.

For more information about each power-on mode, see "Managed system power-on and power-off modes" on page 17.

Powering off a managed system:

Understand how to use the HMC to power off a managed system.

By default, the managed system is set to power off automatically when you shut down the last running logical partition on the managed system. If you set the managed system properties on the HMC so that the managed system does not power off automatically, you must use this procedure to power off your managed system.

Attention: If possible, shut down the running logical partitions on the managed system before powering off the managed system. Powering off the managed system without shutting down the logical partitions first causes the logical partitions to shut down abnormally and can cause data loss.

For more information about shutting down your logical partitions, see the following topics:

- Shutting down AIX
- Shutting down i5/OS
- Shutting down Linux

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

- super administrator

- service representative
- operator
- product engineer

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

1. In the Navigation area, expand the **Server and Partition** folder.
2. Click the **Server Management** icon.
3. In the Contents area, select the managed system.
4. From the menu, click **Selected** → **Power Off**.
5. Select the desired power-off mode and click **OK**.

For more information about the power-off modes, see "Managed system power-on and power-off modes" on page 17.

Scheduling power-on and power-off operations for a managed system:

Use the HMC to schedule power on and off operations for a managed system.

You can power your managed system on and off at regular intervals by scheduling an operation using the HMC.

To schedule a power on or off operation for the managed system using your HMC, complete the following steps:

1. In the Navigation area, expand the **HMC Management** folder.
2. In the Navigation area, click the **HMC Configuration** icon.
3. In the Contents area, click **Schedule Operations**.
4. From the list, select the managed system for which you want to schedule an operation and click **OK**.
5. Select **Options** → **New**.
6. In the Add a Scheduled Operation window, select the managed system power operation that you want to perform and click **OK**.
7. In the appropriate fields, enter the time and date that you want this managed system power operation to occur.
8. If you want this scheduled operation to repeat, click the **Repeat** tab and select the intervals at which you want the power operation to repeat.
9. When you are finished, click **Save**.

Accessing a managed system

Learn how to access a managed system from the HMC after the HMC has been connected to it.

This topic describes how to access the managed system for the first time, after you have connected the HMC to the managed system and powered on the managed system.

The following topics explain more about accessing your managed system using the HMC.

- "Overview of passwords"
- "Virtual operating system consoles" on page 26

For more information about connecting the HMC, see Setting up the Hardware Management Console.

For more information about the Advanced System Management Interface (ASMI), see Managing your server using the Advanced System Management Interface.

Overview of passwords:

Describes the passwords that you need in order to access a managed system using your HMC.

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

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

If all required passwords are not set, the state of the managed system displays *Pending Authentication – Password Updates Required* until these passwords are set.

To change the managed system's password, see "Changing the managed system's password."

If you are using an HMC to access the managed system before all required passwords have been set, enter the appropriate password for each password that is presented in the Update Password Pending Authentication window. If another HMC subsequently needs access to this managed system, upon attempting to access this HMC the user is presented with the Update Password Failed Authentication window, which will prompt for the HMC access password you entered.

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

For more information about the Advanced System Management Interface (ASMI), see Managing your server using the Advanced System Management Interface.

Changing the managed system's password:

Update a managed system's password using the HMC.

You can use the HMC interface to change a managed system's HMC access password. If you change this password, you must change the password for any other HMCs that connect to this managed system.

The super administrator user role is required to change this password.

To change the managed system's HMC access password, complete the following steps:

1. In the Navigation area, expand the **Server and Partition** folder.
2. In the Navigation area, click the **Server Management** application icon.
3. In the Contents area, right-click the managed system and then select **Update Managed System Password**.
4. Type in your current password and new password in the entry fields.
5. Click **OK**.

For information about additional passwords that must be set before you can perform any tasks, see "Overview of passwords" on page 21.

Enabling service processor failover

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

You can use your HMC to have your managed system automatically enable a secondary service processor if your managed system's primary service processor fails.

To enable service processor failover, you must be a member of one of the following roles:

- super administrator
- service representative
- operator
- product engineer

To enable service processor failover, complete the following steps:

1. In the Navigation area, expand the **Server and Partition** folder.
2. Click the **Server Management** icon.
3. In the Contents area, right-click the managed system or frame.
4. Select **Status**.
5. In the Service Processor Connection Status window, click **Service processor failover enabled**.
6. Click **OK**.

   In the error log, an informational SRC of B1xxE66C indicates that the primary service processor in the managed system has performed an administrative failover and transferred system management to the secondary service processor. The error log entry that contains this SRC is created in the primary service processor's error log and copied over to the secondary service processor's error log.

Initiating a service processor failover:

Force a failover after enabling the service processor failover mode on your managed system.

After enabling service processor failover mode on a managed system, you can use your HMC to initiate a failover. This task is useful for forcing a failover to test that the secondary processor is activated during a failover event. The service processor readiness state must be *ready* before you can initiate a failover.

To initiate a service processor failover, you must be a member of one of the following roles:

- super administrator
- service representative
- product engineer

To initiate a service processor failover, complete the following steps:

1. In the Navigation area, expand the **Service Applications** folder.
2. Click **Service Focal Point** and select **Service Utilities** from the Tasks list.
3. In the Service Utilities dialog box, select the managed system and click **Selected** from the Service Utilities menu.
4. Select **Service Processor Failover**.
5. In the Administrative Processor Failover dialog box, ensure that the service processor failover is enabled and the readiness state is *ready*.
6. Click **OK**.

   In the error log, an informational SRC of B1xxE66C indicates that the primary service processor in the managed system has performed an administrative failover and transferred system management to the secondary service processor. The error log entry that contains this SRC is created in the primary service processor's error log and copied over to the secondary service processor's error log.

Setting huge-page memory values

Specify the number of 16-GB pages to allocate to a huge-page memory pool.

On managed systems that support huge-page memory, you can use the Hardware Management Console (HMC) to set the value for the huge-page memory pool. You can also specify values for the number of huge pages to allocate to logical partitions.

Using huge pages can improve performance in specific environments that require a high degree of parallelism, such as in DB2® partitioned database environments. You can specify huge-page memory that can be used for the shared-memory buffer pools in DB2. For logically partitioned systems, you can specify the minimum, desired, and maximum number of huge pages to assign to a partition when you create the partition or partition profile. See Creating logical partitions and partition profiles.

To set the huge-page memory values, the system must be in the powered-off state. The new value will take effect when you restart the system.

Use the following information to determine the requirements and appropriate values for your specific application, and to set the huge-page values.

Calculating huge-page memory requirements:

Calculate the value for the number of pages to allocate to a huge-page memory pool.

To use huge-page memory, you must ensure that your system has adequate memory resources to dedicate to the huge-page memory pool. The huge-page memory pool is a region of system memory that is mapped as 16-GB page segments and is managed separately from the system's base memory. Before you can specify the value for huge-page memory, you must determine which applications you are running and what the huge-page requirements are for your applications.

Determining huge-page memory requirements for your application

The huge-page memory pool can be used to enhance performance for DB2 partitioned database environments in AIX operating systems. For DB2 applications, you would typically use huge pages for large DB2 multipartitioned database environments to efficiently support the degree of parallel activity required of shared memory buffer pools. To determine this value, calculate the amount of memory required for the shared buffer pool to support your DB2 applications. Refer to the DB2 recommendations for buffer pool memory for your particular application.

In logically partitioned systems, you can assign huge-page memory when you create the partitions. This value is separate from the value that you specify for the configured-partition memory region. You can specify a minimum, desired, and maximum value. To determine the number of huge pages needed for your logical partitions, see the section below that discusses calculating huge page values.

Note: The huge page memory allocation cannot be changed dynamically. Changing the number of huge pages on the server requires a server reboot, and changing the number of assigned huge pages for a partition requires a partition reboot.

Considerations for calculating the huge page values

The amount of huge-page memory that you can allocate is dependent on the following factors:

- Total amount of licensed memory for your server
- Amount of available memory after configured memory resources are accounted for
- Number of physical IO connections to the server (each IO connection requires memory for the IO tables, which can be distributed among the physical memory regions and reduces the memory available for huge pages)
- Base memory configuration for logical partitions (huge pages are not calculated as part of the configured-partition memory allocation)
- The requirements that define a huge page, that is each huge page requires 16 GB of contiguous real memory and must start on a 16-GB memory boundary
- Huge pages cannot span memory affinity nodes. Each memory affinity node requires 32 GB to ensure at least one 16 GB huge page when all of the other considerations listed above are taken into account.

Note:

1. For the 9133-52A, 9133-55A, 9116-561, 9406-550, 9406-570, and 9117-570 a physical processors card is a memory affinity node, so the 32 GB must be put on a single 2-way processor card.
2. For the 9119-590, 9119-595, and 9406-595 each 4-way processor on the 16-way processor backplane is a memory affinity node, so the 32 GB must be put into the slots on the same 4-way processor on the backplane.

Attention: The server firmware will reduce the huge-page pool size to satisfy some of these dependencies. When this occurs, error log entries are generated to indicate that the huge-page pool size was reduced. The error log reference code is B700 5300. The reference code details will indicate hexadecimal values that indicate why the huge-page pool size could not be satisfied. The following example shows the possible entries and how to interpret the additional words in these entries:

- word 3 = 0x0000000100000106 - huge page pool reduced to satisfy system hardware configuration
  - word 4 = number of user-configured huge pages
  - word 5 = number of huge pages that could be provided
- word 3 = 0x0000000100000105 - huge page pool reduced to satisfy the memory configuration of partitions
  - word 4 = number of huge pages before partitions were created
  - word 5 = firmware calculated number of huge pages after satisfying partition memory requirements
  - word 6 = number of huge pages in the pool

Calculating huge-page memory values

To calculate the server memory requirements to support huge pages, use the following steps:

1. Determine the amount of base system memory and round that figure to the next 16-GB value. To determine the base server memory requirements, which includes the POWER™ hypervisor and partition, but not huge pages, use the LPAR Validation tool (LVT) or System Planning Tool. See Planning for logical partitions for information about using these planning tools.
2. Determine the number of IO connection loops on your system and multiply the number by 16 GB. This calculation is required because the server needs a memory table for each IO connection, and a 16-GB huge page cannot be located where an IO table exists.
3. Take the larger of the values determined in step 1 and step 2. This will be your base memory value.
4. Determine the number of huge pages that will be required for your AIX applications. To determine this value, use the guidelines provided by your application documentation and the AIX Performance Management Guide. Multiply the number of anticipated huge pages by 16 GB. Add this figure to the base figure determined in step 3. The resulting figure provides an estimate of the amount of licensed memory required to satisfy partition and huge-page pool memory requirements for your system.

Viewing and setting huge page memory values:

View and set values for huge-page memory allocation.

On systems that support huge-page (16 GB) memory allocation, you can view and set the current value in the huge-page memory table. On a new system you must set this value initially to establish the huge-page memory pool. You must set the value when the managed system is in the powered-off state. If this value is already set, you might need to change the value to adjust for performance needs based on the applications that you are running and your partitioning configurations. You can also change the values set for the number of huge pages allocated to your logical partitions.

Use this task to view huge-page values and to set or adjust the number of 16-GB pages for the huge-page allocation according to your needs. Before setting a value, review the information in “Calculating huge-page memory requirements” on page 24.

To view or change huge-page-memory table values, you must be a member of one of the following roles:

- super administrator
- service representative

Note: You must power off the managed system before you can change the huge page memory value for the system. To change the values for logical partitions you must shut down the partition. The new value will take effect when you restart the system.

To view or set huge-page memory values, complete the following steps:

1. In the Navigation area, expand the **Server and Partition** folder.
2. Click the **Server Management** icon.
3. In the Contents area, select the managed system.
4. In the menu click **Selected**, and choose **Properties**.
5. In the Managed System Properties dialog box, view the **Capabilities** information to determine if huge page memory allocation is supported on the managed system. Click the **Memory** tab to view or change the huge page memory allocation displayed under Advanced Options. If the information is not displayed in the Advanced Options area, click **Show details**.

   Note:

   a. You can view and change the current settings for huge-page minimum, desired, and maximum values for logical partitions by viewing the partition properties. See Modifying partition properties for further details.
   b. When you change the huge page memory value, you need to power on the managed server to standby before the changes will be visible.
   c. When you change the huge page memory value, you can go to advanced system management and select System Memory Page Setup to check the setting before powering on the system.

Virtual operating system consoles

Learn how to use virtual operating system consoles on your HMC.

You can connect to logical partition operating systems, for example to manage i5/OS resources, by using your HMC interface to open a virtual console window. The following task explains how to verify that consoles are configured.

Verify that consoles are configured:

Explains how to verify that an i5/OS console is already configured for an operating system.

To verify that a console is configured for your i5/OS logical partition, check the logical partition's properties.

To view a partition's properties, complete the following steps:

1. In the Contents area, right-click the logical partition and then select **Properties**. The Properties window lists which console is configured for this logical partition.
2. Click the **Settings** tab. The **Tagged I/O** field lists console information.

For more information about items displayed in this field, refer to the online help on the HMC interface.

Finding and updating managed systems data on the HMC

Find and update managed-system information that is displayed on the HMC interface. Also, learn more about working with managed system profile data.

This topic describes how to find information about each of the managed systems that are attached to the HMC. Also, learn how to perform tasks to ensure the integrity of the managed system data maintained by the HMC.

Viewing information about the managed system:

View information about the managed system's configuration and capabilities.

You can view the managed system's configuration and capabilities. Any user can view managed system properties. To view information about the managed system:

1. Expand the **Server and Partition** folder in the Navigation area.
2. Click the **Server Management**.
3. The Contents area expands to show each managed system, which you can then expand to show information about the managed system, including its name, its state, and the operator panel value.
4. To expand your view of the managed system's properties, click the plus sign (+) next to the managed system's name to view its contents.

To view the detailed managed system properties, do the following:

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

The HMC displays the system's name, logical partition capability, state, serial number, model and type, and policy information. A system that is powered on using the Partition Standby option displays this information, as well as available and assigned processors, memory, I/O drawers and slots, power-on parameters, reference codes, and policy information. The HMC also displays power-on parameters and reference codes for a managed system in the power-off state.

The Processor tab displays information that is helpful when performing Dynamic Logical Partitioning processor tasks. Use the Processor tab to view processor usage data for partitions and determine whether a processor is assigned to a logical partition. The information in the Processor tab is also helpful when you need to know if processors are disabled and therefore cannot be used by any logical partition.

The Memory tab shows deconfigured resources, as well as information about available and configured memory. To view or change memory allocation on systems with huge page table support, use the Memory tab and select **Show details** in the Advanced Options area. To change the requested value for huge page memory, the system must be powered off.

The information provided in the memory tab (for example, deconfigured resources), along with the information provided on the I/O tab, is useful for planning for processors and dynamic logical partitions.

Updating managed system or frame information:

Update the system information for a managed system or frame in the HMC that is in an Incomplete state.

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

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

To update managed system or frame information, you must be a member of one of the following roles:

- super administrator
- service representative
- operator
- product engineer

To update the managed system or frame information, complete the following steps:

1. In the contents area, select the managed system or frame.
2. From the menu, click **Selected**.
3. Choose from the following options:
   - To rebuild a managed system, click **Rebuild Managed System**. The current system information displays.
   - To rebuild a managed frame, click **Rebuild Managed Frame**. The current system information displays.
4. Click **Yes**.

Disconnecting another HMC connection:

Read about how to manually unlock an HMC locked connection to the managed system.

If you have two HMCs connected to the managed system, one HMC temporarily locks the other out while it is performing operations. This action prevents the other HMC from operating on the managed system because simultaneous operations could cause conflicting results. If the interface is locked, most console operations automatically wait for the lock to release.

However, in the rare event that an HMC has a problem that prevents the lock from being properly released, you need to manually disconnect the connection to the managed system. Typically, if one HMC has locked the connection, you must unlock it from the other HMC, which then allows other HMCs to communicate with the managed system and run further commands.

To release a lock on a managed system requires the super administrator role.

To unlock an HMC connection, complete the following steps:

1. In the Contents area, select the managed system.
2. In the menu, click **Selected**.
3. Select **Disconnect another HMC**. The Disconnect Another HMC window opens.
4. From the list, select the HMC that you want to disconnect, and then click **OK**.

Recovering partition data on a managed system:

Learn how to recover the partition data on your managed system if it becomes corrupted.

Through the HMC interface, you can recover partition data on your managed system if the data becomes damaged. This partition data includes information about logical partitions, partition profiles, and system profiles. If the partition data on your managed system becomes damaged, the managed system is in *recovery* state. You can either restore the partition data from a backup file that is saved automatically on your HMC by selecting **Restore profile data from the HMC backup data**, or clear all partition configuration with **Initialize the managed system**.

This procedure recovers the partition data in the service processor of your server. To recover the partition data on your managed system, see Restoring profile data.

Note: The HMC might not show *operating* state for the managed system after completing this recovery procedure. After a partition is activated, the managed system will transition to an *operating* state and clear the A700 4091 or C700 4091 SRC.

To recover the partition data on your managed system, you must be a member of one of the following roles:

- super administrator
- operator

To recover the partition data on your managed system, do the following:

1. In the Navigation Area, open **Server and Partition**.
2. Select **Server Management**.
3. In the contents area, right-click the managed system whose partition data you want to recover and select **Recover Partition Data**.
4. Select one of the following:
   - **Restore profile data from HMC backup data**: This option restores the partition data using the backup file that is saved automatically on the HMC.
   - **Initialize the managed system**: This option clears all partition configuration data, and can only be used if all partitions are in the *Not Activated* state.
5. Click **OK**.

Managing frames using the HMC

Learn about the tasks that you can use to manage your frames in the HMC.

This topic describes how to perform various tasks related to managing your frame that is connected to the HMC.

Adding a frame:

Use this procedure to add a frame manually to the HMC.

New frames are automatically detected, or discovered, by the HMC when the HMC is configured as a DHCP server. For information about configuring your HMC as a DHCP server, see The HMC as a DHCP server. Upon detection of a new frame, the DHCP server assigns an IP address to the frame. This newly assigned IP address remains static as long as the MAC address remains unchanged. When a frame is replaced, the DHCP server assigns a new IP address and broadcasts an update to all HMCs on the network.

Note: Add a frame by configuring your HMC to automatically detect new frames. Use the instructions provided at the link referenced in the preceding paragraph.

In addition to adding a frame automatically, the HMC allows you to manually add frames to the managed frames of this HMC. You will need to provide the host name and IP address for each frame that you want to add. You can also find a frame on the network within a specified IP address range. The discovery processing time can vary depending on the range of IP addresses that you entered and your network configuration.

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

- super administrator
- operator
- product engineer

To add a frame, complete the following steps:

1. In the Navigation Area, expand the **Server and Partition** folder.
2. Select **Frame Management**.
3. Select **Add Managed Frame(s)**. Type the requested information. If you want to find a frame in the network, select **Find managed frames** and type the IP address range.
4. Click **Next**.
5. Click **Finish**.

Initializing a frame:

This topic explains how to initialize a frame after a new frame has been added.

After you add a frame in the HMC, it must be initialized before it can be detected by the managed system. Initialization of the frame consists of powering on all the I/O drawers followed by powering on all the managed systems that belong to the managed frame. The initialization time might vary depending upon your setup.

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

- super administrator
- operator
- product engineer

To initialize a frame, complete the following steps:

1. In the Navigation Area, expand the **Server and Partition** folder.
2. Select **Frame Management**.
3. From the menu, click **Frame Management**.
4. Select **Initialize Frame(s)**.
5. Click **Continue**.

Modifying information about a frame:

Change a frame's name and number.

You can view frame information and change the frame name and number.

Any user can view or modify frame properties.

To view and change the frame's properties, complete the following steps:

1. In the Navigation Area, expand the **Server and Partition** folder.
2. Select **Frame Management**.
3. In the Contents area, select the frame.
4. From the menu, click **Selected**.
5. Click **Properties**. You can also access this option by right-clicking the frame and selecting **Properties** on the menu.

   By default, you are viewing the General tab that includes the frame name, number, state, type and serial number. To view a list of all the managed systems contained in the frame, use the Managed Systems tab. The information in the I/O Units tab is helpful when you need to know all the I/O Units contained in the frame.
6. Change the frame name and number, if desired.
7. Click **OK**.

Updating frame information:

Rebuilding the managed frame information for theHMC. This procedure is helpful when clearing an *Incomplete* state.

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

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

To update frame information, you must be a member of one of the following roles:

- super administrator
- operator
- product engineer

To update the frame, complete the following steps:

1. In the Navigation Area, expand the **Server and Partition** folder.
2. Select **Frame Management**.
3. In the Contents area, select the frame.
4. From the menu, click **Selected**.
5. Click **Rebuild Managed Frame**. The current frame information displays.
6. Click **Yes**.

Resetting or removing a frame connection:

This information explains how to reset the HMC connection to a frame, or remove a locked connection to a managed system.

When you no longer want to manage a frame using the HMC, you can remove the connection. You must remove the connection before you physically disconnect the HMC from the managed frame (or from the network).

In the rare event that the frame is in the *No connection* state, you can recover by resetting the connection with the frame. Reset the connection with the managed frame after you have verified that the network settings are correct on both the HMC and the managed frame. Performing this action will break and reestablish the connection.

To reset or remove a frame connection, you must be a member of one of the following roles:

- super administrator
- service representative
- operator

To reset or remove a frame connection, complete the following steps:

1. In the Navigation Area, expand the **Server and Partition** folder.
2. Select **Frame Management**.
3. In the Contents area, select the managed system.
4. In the menu, click **Selected**.
5. Select **Reset or Remove Connection** from the menu.
6. Click **Remove Connection** or **Reset Connection**.
7. Click **OK**.

After the frame's logical connection is removed, you can remove the HMC from the network.

Managing operating systems

Understand how you can use the HMC to interact with the operating systems running on the managed systems.

You can force some operating systems to shut down or reset using the HMC interface. For more information about these tasks, review the following topics.

Resetting the operating system on a partition:

Restart the operating system when an operating system in a logical partition hangs.

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

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

- super administrator
- service representative

Note: For i5/OS logical partitions, use this task only if you cannot restart the i5/OS logical partition from the command line of the operating system. Using this window to restart an i5/OS logical partition will result in an abnormal IPL.

To reset the operating system on a logical partition, complete the following steps:

1. In the Navigation Area, expand **Server and Partition**.
2. Click **Server Management**.
3. In the Contents area, select the logical partition that is running the operating system that you want to reset.
4. In the menu, click **Selected → Restart partition**.
5. Select the type of operating system restart.
6. Click **Yes**.

Shutting down an operating system:

This information explains how to shut down an operating system in a logical partition.

You can use the HMC interface to perform shutdown operations on a logical partition. You can perform this task only if the operating system that is running on the logical partition supports this function.

Note: If your logical partition is running i5/OS, shut down the operating system manually through the operating system, if possible. Using the HMC interface to power off the logical partition operating system will cause longer restart times. For more information about shutting down an i5/OS logical partition, see Shutting down i5/OS.

To shut down an operating system on a logical partition, complete the following steps:

1. In the Contents area, select the logical partition running the operating system that you want to reset.
2. In the menu, click **Selected → Shut Down Partition**.
3. Select the type of shutdown that you want to perform.
4. Click **OK**.

Adding managed systems to the HMC environment

Understand how to add managed systems to the HMC, so that you can manage them using the HMC interface.

You can manage multiple systems from a Hardware Management Console (HMC). To add a managed system to the HMC, you must establish a network connection between the HMC and the service processor of the new system. Configuring the HMC to work with the new managed system depends on how you have set up and configured the existing network connections between the HMC and the already-installed managed systems, including connections to the logical partitions.

For more information about configuring network connections on the HMC, see HMC network connections.

Use the following topics to determine how to add a managed system to your HMC environment based on your existing network configuration. After completing the HMC connection, add the system to your HMC environment by selecting the managed system connection in the HMC GUI and selecting Add managed system from the Selected menu. Follow the instructions in the Add managed system window by specifying the name or IP address of the managed system or specifying a range of IP addresses to find and select the managed system to add. For more information about the Add managed system function, refer to the HMC GUI help.

Using an existing private network with the HMC acting as a DHCP server:

Use a dedicated private network that you already have set up with the HMC acting as a DHCP server to manage your system.

If your existing network is already set up as a ″private″ dedicated network with the HMC acting as a DHCP server, then you must physically connect to the new system. For more information about physically connecting to a new managed system, see Setting up the Hardware Management Console. If you have an Ethernet switch with available ports connected to the HMC, connect the Ethernet cable from the service processor of the new system to the Ethernet switch. When the connection is made, the HMC automatically detects the managed system and adds it to the Contents area of the HMC interface. Automatic detection does not occur if you removed the managed system prior to its availability.

Using an existing open network:

Understand the requirements for using the HMC in a configured open network.

If the HMC was connected to existing managed systems over an ″open″ (public) network, other types of devices and systems can exist on the network. More specifically, the HMC is not acting as a DHCP server. In this environment, you must take one of the following actions to use the HMC:

- Manually configure the new managed system’s service processor with a static (fixed) set of IP parameters using the Advanced System Management Interface.
- Manually configure the IP address of the new system’s service processor, if there is an existing DHCP server on the network.

When the connection is made, you can add the managed system by using the **Add managed systems** function or the mksysconn command.

Deleting a managed system

Disconnect a managed system from the HMC before you physically detach it from the HMC.

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

Note: You must delete the managed system from the Contents area before you disconnect the Ethernet or the network-attached cable from the hardware.

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

To delete the managed system from the Contents area, complete the following steps:

1. In the Contents area, select the managed system.
2. From the menu, click **Selected**.
3. Select **Reset or Remove Connection** from the menu.
4. Click **remove**, then click **OK**.

After the managed system's logical connection is removed, you can remove the managed system from the network.

Moving the managed system from an open network to a private network

Learn how to move a managed system that is attached to an HMC on an open network to an HMC that is located on a private network.

You can move a managed system from an open network to a private network. It is recommended that you configure the HMC that is located on the private network as a DHCP server before you attach the new managed system. This configuration will allow the HMC to automatically detect the newly added managed system and assign it a unique IP address.

To perform this operation, you must be a member of one of the following roles:

- super administrator
- service representative
- product engineer

To move the managed system from an open network to a private network, complete the following steps:

1. Configure the HMC that is located on the private network as a DHCP server. For more information, see Configuring the HMC as a DHCP server.
2. Remove the static IP address of the managed system that you want to move using the Advanced System Management Interface (ASMI). For more information about how to use ASMI to configure the HMC as a DHCP server, see Configuring network interfaces.
3. Disconnect the cable of the managed system that you want to move from the HMC that is located on the open network.
4. Connect the cable of the managed system to the HMC located on the private network. Because you previously configured the HMC that is located on the private network as a DHCP server, the newly attached managed system is automatically detected and assigned a new IP address.

Servicing the managed system

Understand how you can use the HMC to perform service actions.

The Customer service, support, and troubleshooting topic provides an overview of the elements of the service and support environment. It also describes the different functions and features of the environment and the HMC applications that provide those functions.

Using the IBM Network Manager

Learn how to use the IBM Network Manager to manage InfiniBand networks.

The IBM Network Manager enables you to manage your InfiniBand network from the Hardware Management Console (HMC).

Use the IBM Network Manager to manage IB switches, update switch software, view network topology information, and view and modify management properties. You must enable the Network Manager from the HMC before you can use it to manage your network.

For information about setting up the HMC in an InfiniBand network, see Setting up the HMC.

The following topics describe the tasks that you can perform with the IBM Network Manager:

Enabling and disabling the IBM Network Manager

Enable the IBM Network Manager to manage your InfiniBand switch network.

Before you can use the IBM Network Manager to manage your InfiniBand network switches and systems, you must enable it from the HMC. When you enable the IBM Network Manager, it starts discovery and begins providing data about the status of your IB switch network.

Any user can enable or disable the IBM Network Manager.

Note: If you decide to move the IBM Network Manager functions from one HMC host to another HMC host, you must first disable the IBM Network Manager on the first HMC host before enabling it on the second host.

To enable or disable the IBM Network Manager, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **Enable IBM NM Software**.
   To disable the IBM Network Manager, select **Disable IBM NM Software**.

Viewing switch topology information in an InfiniBand network

View information about the switch layout and connectivity in your InfiniBand network.

You can view information about the switches in your InfiniBand network that identifies the physical location and connection activity for all connected switch devices. From within the topology view window, you can access additional menu options for the objects that you select in the list. For example, when you select a switch and then click **Selected → Properties**, you can view system, subnet manager, and backplane details for that item. For more information about the menu options in the switch topology view, see the online help.

Any user can view the switch topology information.

Note: The IBM Network Manager must be enabled in order for you to access this task in the HMC.

To view the switch topology information, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **View Switch Topology**.
   The HMC displays a table with a list of the switches in the IB network. By default, the information presented shows the switch device name (or identifier), location code, frame information, power on and off status, GUID, port status, and neighboring port (link) information.
   To change the columns displayed in the list of information, click **View → Show Columns** and select or clear the check box for the columns that you want to designate as the default columns.

Viewing server topology information in an InfiniBand network

View information about the physical layout of your InfiniBand network.

You can view information about the servers, adapters, and ports in your InfiniBand network.

Any user can view the server topology information.

Note: The IBM Network Manager must be enabled in order for you to access this procedure.

To view the server topology information, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **View End-Point Topology**.

   The HMC displays a table with a list of the servers in the InfiniBand cluster. By default, the information presented shows the server name, location code, power on/off status, frame/cage information, adapter status, port status, and neighbor port (link) information.

   To change the columns displayed in the list of information, click **View → Show Columns** and select or clear the check box for the columns that you want to designate as the default columns.

Viewing logical topology information in an InfiniBand network

View information about the logical server layout in your InfiniBand network.

You can view information about the servers, adapters, ports, and related status for the logical partitions in your InfiniBand network.

Any user can view the logical topology information.

Note: The IBM Network Manager must be enabled in order for you to access this procedure.

To view the logical topology information, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **View Logical Topology**.

   The HMC displays a table with a list of the servers and partitions in the InfiniBand configuration. By default, the information presented shows the server name, location code, system or logical partition status, adapter status, type, the GUID, port status, and neighbor port (link) information.

   To change the columns displayed in the list of information, click **View → Show Columns** and select or clear the check box for the columns that you want to designate as the default columns.

Viewing IBM Network Manager properties

View and manage switch information and the properties of the currently enabled IBM Network Manager for your InfiniBand environment.

You can view and modify the IBM Network Manager properties and the switch-management properties for your InfiniBand network. For example, use this procedure to change the IBM Network Manager default name assigned to the managed switches. Using switch names provides a convenient way to keep track of the switches you are managing (particularly when frame numbers or cage numbers are not readily available). You can also change the switch-management priority (change the subnet manager master and succession order), synchronize the switch local time with the HMC time (NTP time is not currently supported), and view the switch topology.

Any user can view the Network Manager properties.

Note: The Network Manager must be enabled in order for you to access this task from the HMC.

To view the properties, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **View Management Properties**.
4. Click the IBM NM tab to view the IBM Network Manager properties.
   The HMC displays the HMC host name, the IP address, and version number of the currently enabled IBM Network Manager.
5. Click **Switch** to view and modify information about the switches in your InfiniBand environment.

Viewing the IBM Network Manager log

View the IBM Network Manager event log.

The IBM Network Manager maintains an event log that you can view to track the IBM Network Manager activities.

Any user can view the event log.

Note: The IBM Network Manager must be enabled in order for you to access this task in the HMC.

To view the IBM Network Manager event log, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **View IBM NM Event Log**.
   The HMC displays the contents of the log file.

Updating switch software

Use the IBM Network Manager to update the software for all the switches in your InfiniBand network.

You can update multiple switches simultaneously for a single software version, or choose a switch and the version of software to apply for the update of that switch. You can start another switch installation before a switch update procedure that is currently running has finished; however, if both installations run concurrently and contain the same switch, the subsequent installation action might fail.

An Import option allows you to add more software versions from a DVD.

Any user can update the switch software.

Note: The IBM Network Manager must be enabled in order for you to access this task from the HMC.

To update your switch software, complete the following steps:

1. In the Navigation area, expand the **Switch Management** folder.
2. Click **IBM Network Manager**.
3. In the Network Manager menu, select **Update Switch Software**.
4. Select the switches that you want to update.
5. Select the software version to install for the selected switch or switches.
6. Click **OK** to start the software update.

Note: To uninstall the last update, select **Return switch to previous software**.

Related information for Managing your server using the HMC

Product manuals, IBM Redbooks™ (in PDF format), Web sites, and information center topics contain information related to the Managing your server using the HMC topic. You can view or print any of the PDF files.

Manuals

- Managing the Hardware Management Console
- Managing your server using the Advanced System Management Interface
- Clustering systems using InfiniBand hardware
- Partitioning the server
- Working with Capacity on Demand
- Setting up your server to connect to service and support

Other information

- HMC Education module in IBM Resource Link™

Appendix. Accessibility features

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

The following list includes the major accessibility features:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are tactilely discernible and do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

IBM and accessibility

See the IBM Accessibility Center at http://www.ibm.com/able/ for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

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

Trademarks

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

AIX
DB2
i5/OS
IBM
POWER
Resource Link
System i
System p
Virtualization Engine

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

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THESE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA