

Power Systems

*Installing and configuring the
Hardware Management Console*

IBM

Power Systems

*Installing and configuring the
Hardware Management Console*

IBM

Note

Before using this information and the product it supports, read the information in “Safety notices” on page vii, “Notices” on page 175, the *IBM Systems Safety Notices* manual, G229-9054, and the *IBM Environmental Notices and User Guide*, Z125-5823.

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

© Copyright IBM Corporation 2014, 2017.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Safety notices	vii
---------------------------------	------------

Installing and configuring the Hardware Management Console	1
---	----------

What's new in Installing and configuring the HMC	1
Installation and configuration tasks	2
Installing and configuring a new HMC with a new server	2
Updating and upgrading your HMC code	2
Adding a second HMC to an existing installation	3
Setting up the HMC	3
Cabling your stand-alone HMC	4
Installing the 7310-CR4 HMC into a rack	5
Completing a parts inventory	6
Determining the location	7
Marking the location without using a rack-mounting template.	8
Installing slide rails into the rack	8
Installing the HMC on the slide rails	11
Installing the cable-management arm	13
Cabling your rack-mounted HMC	14
HMC port locations	15
Installing the 7042-CR5 and 7042-CR6 into a rack	19
Installing the 7042-CR7 and 7042-CR8 into a rack	24
Installing the 7042-CR9 HMC into a rack	33
Installing the 7063-CR1 into a rack	42
Prerequisites for installing the rack-mounted 7063-CR1 system	43
Completing inventory for your system	43
Determining and marking the location in the rack for the 7063-CR1 system	43
Attaching the rails to the rack	45
Installing the system into the rack and connecting and routing power cables	46
Cabling the rack-mounted 7063-CR1 HMC	47
Configuring the 7063-CR1 HMC	48
Installing the HMC virtual appliance	51
Installing the HMC virtual appliance on x86	51
Installing the HMC virtual appliance by using the KVM hypervisor	52
Installing the HMC virtual appliance by using the Xen hypervisor	52
Installing the HMC virtual appliance by using VMware ESXi.	53
Installing the HMC virtual appliance on POWER.	54
Installing the HMC virtual appliance on PowerVM (logical partition)	54
Using the Activation Engine for the HMC virtual appliance	57
Setting up the configuration profile for the Activation Engine	58
Installing the monitor and keyboard	64
Completing a parts inventory	66
Marking the location without using a rack-mounting template	66
Installing the monitor and keyboard into a rack	66
Installing the console switch (optional)	70
Configuring the HMC by using the HMC Classic or HMC Enhanced interface	72
Choosing network settings on the HMC	72
HMC network connections	72
Types of HMC network connections	72
Deciding which connectivity method to use for the call-home server	76
Simplified connectivity	78
Using Internet SSL to connect to remote support	78
Choosing an Internet Protocol	79
Internet SSL address lists	79
Using a virtual private network to connect to remote support	80
VPN server address list	80

Using the telephone and modems to connect to remote support	80
Using multiple call-home servers	81
Preparing for HMC configuration	81
Preinstallation configuration worksheet for the HMC	83
Configuring the HMC	89
Configuring the HMC by using the fast path through the Guided Setup wizard	90
Start the HMC and complete the steps in the Guided Setup wizard.	90
Review your configuration	91
Configuring the HMC by using the HMC menus.	91
Starting the HMC	92
Changing the date and time	93
Configuring the HMC network types.	93
Changing HMC firewall settings	98
Configuring a routing entry as the default gateway	99
Configuring domain name services	100
Configuring domain suffixes	100
Configuring the HMC so that it uses LDAP remote authentication	100
Configuring the HMC so that it uses Key Distribution Center servers for Kerberos remote authentication	101
Configuring the HMC so that it can contact service and support	101
Configuring the Events Manager for Call Home.	106
Setting passwords for the managed system	107
Testing the connection between the HMC and the managed system	108
Postconfiguration steps	108
Backing up critical HMC data	108
Backing up the entire HMC hard disk drive to a remote system	109
Updating, upgrading, and migrating your HMC machine code	110
Determining your HMC machine code version and release	110
Obtaining and applying machine code updates for the HMC with an Internet connection	111
Step 1. Ensure that you have an Internet connection	111
Step 2. View the existing HMC machine code level	111
Step 3. View the available HMC machine code levels	111
Step 4. Apply the HMC machine code update	111
Step 5. Verify that the HMC machine code update installed successfully.	112
Obtaining and applying machine code updates for the HMC using DVD or an FTP server	112
Step 1. View the existing HMC machine code level	112
Step 2. View the available HMC machine code levels	112
Step 3. Obtain the HMC machine code update	112
Step 4. Apply the HMC machine code update	113
Step 5. Verify that the HMC machine code update installed successfully.	113
Upgrading your HMC software	113
Step 1. Obtain the upgrade	113
Step 2. View the existing HMC machine code level	114
Step 3. Back up the managed system's profile data	114
Step 4. Back up HMC data	114
Step 5. Record the current HMC configuration information	115
Step 6. Record remote command status.	115
Step 7. Save upgrade data	115
Step 8. Upgrade the HMC software	116
Step 9. Verify that the HMC machine code upgrade installed successfully	116
Upgrading HMC from remote location using network upgrade images	116
Configuring the HMC by using the HMC Enhanced+ interface	117
Choosing network settings on the HMC	117
HMC network connections	117
Types of HMC network connections	117
Deciding which connectivity method to use for the call-home server	121
Using Internet SSL to connect to remote support	123
Choosing an Internet Protocol	123
Internet SSL address lists	123
Using a virtual private network to connect to remote support	124
VPN server address list	125
Using the telephone and modems to connect to remote support	125

Using multiple call-home servers	125
Preparing for HMC configuration	126
Preinstallation configuration worksheet for the HMC	127
Configuring the HMC	134
Configuring the HMC by using the fast path through the Guided Setup wizard	134
Start the HMC and complete the steps in the Guided Setup wizard	134
Review your configuration	135
Configuring the HMC by using the HMC Enhanced+ interface menus	135
Starting the HMC	136
Changing the date and time	137
Configuring the HMC network types	138
Changing HMC firewall settings	144
Configuring a routing entry as the default gateway	145
Configuring domain name services	145
Configuring domain suffixes	146
Configuring the HMC so that it uses LDAP remote authentication	146
Configuring the HMC so that it uses Key Distribution Center servers for Kerberos remote authentication	147
Configuring the local console to report errors to service and support	148
Configuring the Events Manager for Call Home	153
Setting passwords for the managed system	154
Testing the connection between the HMC and the managed system	155
Postconfiguration steps	155
Backing up management console data	155
Updating, upgrading, and migrating your HMC machine code	156
Determining your HMC machine code version and release	157
Obtaining and applying machine code updates for the HMC with an Internet connection	157
Step 1. Ensure that you have an Internet connection	157
Step 2. View the existing HMC machine code level	157
Step 3. View the available HMC machine code levels	158
Step 4. Apply the HMC machine code update	158
Step 5. Verify that the HMC machine code update installed successfully	158
Obtaining and applying machine code updates for the HMC using DVD or an FTP server	159
Step 1. View the existing HMC machine code level	159
Step 2. View the available HMC machine code levels	159
Step 3. Obtain the HMC machine code update	159
Step 4. Apply the HMC machine code update	160
Step 5. Verify that the HMC machine code update installed successfully	160
Upgrading your HMC software	160
Step 1. Obtain the upgrade	160
Step 2. View the existing HMC machine code level	161
Step 3. Back up the managed system's profile data	161
Step 4. Back up HMC data	161
Step 5. Record the current HMC configuration information	162
Step 6. Record remote command status	162
Step 7. Save upgrade data	163
Step 8. Upgrade the HMC software	163
Step 9. Verify that the HMC machine code upgrade installed successfully	164
Upgrading HMC from remote location using network upgrade images	164
Securing the HMC	165
Solving common problems while securing HMC	166
Security profiles: Global Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI-DSS)	169
HMC port locations	171
Notices	175
Accessibility features for IBM Power Systems servers	176
Privacy policy considerations	177
Trademarks	178
Electronic emission notices	178
Class A Notices	178
Class B Notices	182

Terms and conditions. 185

Safety 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, safety information documentation is included in the publications package (such as in printed documentation, on DVD, or as part of the product) shipped with the product. The documentation 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 documentation. You should also refer to the safety information documentation any time you do not clearly understand any safety information in the U.S. English publications.

Replacement or additional copies of safety information documentation can be obtained by calling the IBM Hotline at 1-800-300-8751.

German safety information

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Laser safety information

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

Laser compliance

IBM servers may be installed inside or outside of an IT equipment rack.

DANGER: When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- If IBM supplied the power cord(s), connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
 - For AC power, disconnect all power cords from their AC power source.
 - For racks with a DC power distribution panel (PDP), disconnect the customer's DC power source to the PDP.
- When connecting power to the product ensure all power cables are properly connected.

- For racks with AC power, connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- For racks with a DC power distribution panel (PDP), connect the customer's DC power source to the PDP. Ensure that the proper polarity is used when attaching the DC power and DC power return wiring.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Do not attempt to switch on power to the machine until all possible unsafe conditions are corrected.
- Assume that an electrical safety hazard is present. Perform all continuity, grounding, and power checks specified during the subsystem installation procedures to ensure that the machine meets safety requirements.
- Do not continue with the inspection if any unsafe conditions are present.
- Before you open the device covers, unless instructed otherwise in the installation and configuration procedures: Disconnect the attached AC power cords, turn off the applicable circuit breakers located in the rack power distribution panel (PDP), and disconnect any telecommunications systems, networks, and modems.

DANGER:

- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To Disconnect:

1. Turn off everything (unless instructed otherwise).
2. For AC power, remove the power cords from the outlets.
3. For racks with a DC power distribution panel (PDP), turn off the circuit breakers located in the PDP and remove the power from the Customer's DC power source.
4. Remove the signal cables from the connectors.
5. Remove all cables from the devices.

To Connect:

1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. For AC power, attach the power cords to the outlets.
5. For racks with a DC power distribution panel (PDP), restore the power from the Customer's DC power source and turn on the circuit breakers located in the PDP.
6. Turn on the devices.

Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)

(R001 part 1 of 2):

DANGER: Observe the following precautions when working on or around your IT rack system:

- Heavy equipment—personal injury or equipment damage might result if mishandled.
- Always lower the leveling pads on the rack cabinet.
- Always install stabilizer brackets on the rack cabinet.
- To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.
- Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices. In addition, do not lean on rack mounted devices and do not use them to stabilize your body position (for example, when working from a ladder).



- Each rack cabinet might have more than one power cord.
 - For AC powered racks, be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.
 - For racks with a DC power distribution panel (PDP), turn off the circuit breaker that controls the power to the system unit(s), or disconnect the customer's DC power source, when directed to disconnect power during servicing.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

(R001 part 2 of 2):

CAUTION:

- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- *(For sliding drawers.)* Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.



- *(For fixed drawers.)* This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.

CAUTION:

Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building.

- Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must observe the following precautions:
 - Remove all devices in the 32U position (compliance ID RACK-001 or 22U (compliance ID RR001) and above.
 - Ensure that the heaviest devices are installed in the bottom of the rack cabinet.
 - Ensure that there are little-to-no empty U-levels between devices installed in the rack cabinet below the 32U (compliance ID RACK-001 or 22U (compliance ID RR001) level, unless the received configuration specifically allowed it.
- If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.
- If the rack cabinet you are relocating was supplied with removable outriggers they must be reinstalled before the cabinet is relocated.
- Inspect the route that you plan to take to eliminate potential hazards.
- Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.
- Verify that all door openings are at least 760 x 230 mm (30 x 80 in.).
- Ensure that all devices, shelves, drawers, doors, and cables are secure.
- Ensure that the four leveling pads are raised to their highest position.
- Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.
- Do not use a ramp inclined at more than 10 degrees.
- When the rack cabinet is in the new location, complete the following steps:
 - Lower the four leveling pads.
 - Install stabilizer brackets on the rack cabinet.
 - If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.
- If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.

(R002)

(L001)



DANGER: Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label. (L001)

(L002)



DANGER: Rack-mounted devices are not to be used as shelves or work spaces. (L002)

(L003)



or



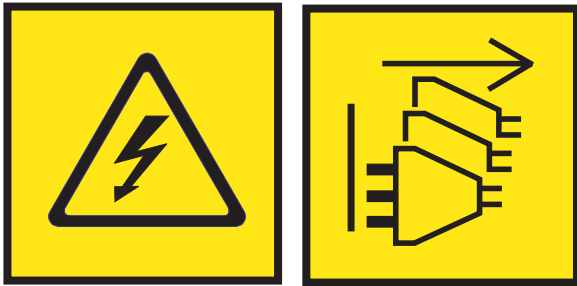
or



or



or



DANGER: Multiple power cords. The product might be equipped with multiple AC power cords or multiple DC power cables. To remove all hazardous voltages, disconnect all power cords and power cables. (L003)

(L007)



CAUTION: A hot surface nearby. (L007)

(L008)



CAUTION: Hazardous moving parts nearby. (L008)

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. Although shining light into one end and looking into the other end of a disconnected optical fiber to verify the continuity of optic fibers many not injure the eye, this procedure is potentially dangerous. Therefore, verifying the continuity of optical fibers by shining light into one end and looking at the other end is not recommended. To verify continuity of a fiber optic cable, use an optical light source and power meter. (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)

CAUTION:

The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do Not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C003)

CAUTION:

Regarding IBM provided VENDOR LIFT TOOL:

- Operation of LIFT TOOL by authorized personnel only.
- LIFT TOOL intended for use to assist, lift, install, remove units (load) up into rack elevations. It is not to be used loaded transporting over major ramps nor as a replacement for such designated tools like pallet jacks, walkies, fork trucks and such related relocation practices. When this is not practicable, specially trained persons or services must be used (for instance, riggers or movers).
- Read and completely understand the contents of LIFT TOOL operator's manual before using. Failure to read, understand, obey safety rules, and follow instructions may result in property damage and/or personal injury. If there are questions, contact the vendor's service and support. Local paper manual must remain with machine in provided storage sleeve area. Latest revision manual available on vendor's web site.
- Test verify stabilizer brake function before each use. Do not over-force moving or rolling the LIFT TOOL with stabilizer brake engaged.
- Do not move LIFT TOOL while platform is raised, except for minor positioning.
- Do not exceed rated load capacity. See LOAD CAPACITY CHART regarding maximum loads at center versus edge of extended platform.
- Only raise load if properly centered on platform. Do not place more than 200 lb (91 kg) on edge of sliding platform shelf also considering the load's center of mass/gravity (CoG).
- Do not corner load the platform tilt riser accessory option. Secure platform riser tilt option to main shelf in all four (4x) locations with provided hardware only, prior to use. Load objects are designed to slide on/off smooth platforms without appreciable force, so take care not to push or lean. Keep riser tilt option flat at all times except for final minor adjustment when needed.
- Do not stand under overhanging load.
- Do not use on uneven surface, incline or decline (major ramps).
- Do not stack loads.
- Do not operate while under the influence of drugs or alcohol.
- Do not support ladder against LIFT TOOL.
- Tipping hazard. Do not push or lean against load with raised platform.
- Do not use as a personnel lifting platform or step. No riders.
- Do not stand on any part of lift. Not a step.
- Do not climb on mast.
- Do not operate a damaged or malfunctioning LIFT TOOL machine.
- Crush and pinch point hazard below platform. Only lower load in areas clear of personnel and obstructions. Keep hands and feet clear during operation.
- No Forks. Never lift or move bare LIFT TOOL MACHINE with pallet truck, jack or fork lift.
- Mast extends higher than platform. Be aware of ceiling height, cable trays, sprinklers, lights, and other overhead objects.
- Do not leave LIFT TOOL machine unattended with an elevated load.
- Watch and keep hands, fingers, and clothing clear when equipment is in motion.
- Turn Winch with hand power only. If winch handle cannot be cranked easily with one hand, it is probably over-loaded. Do not continue to turn winch past top or bottom of platform travel. Excessive unwinding will detach handle and damage cable. Always hold handle when lowering, unwinding. Always assure self that winch is holding load before releasing winch handle.
- A winch accident could cause serious injury. Not for moving humans. Make certain clicking sound is heard as the equipment is being raised. Be sure winch is locked in position before releasing handle. Read instruction page before operating this winch. Never allow winch to unwind freely. Freewheeling will cause uneven cable wrapping around winch drum, damage cable, and may cause serious injury. (C048)

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

The following comments apply to the IBM 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 metalically 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 metalically 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.

The dc-powered system is intended to be installed in a common bonding network (CBN) as described in GR-1089-CORE.

Installing and configuring the Hardware Management Console

Describes how to install the Hardware Management Console (HMC) hardware, connect it to your managed system, and configure it for use. You can perform these tasks yourself, or contact a service provider to perform these tasks for you. You might be charged a fee by the service provider for this service.

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

What's new in Installing and configuring the HMC

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

August 2017

- The HMC Classic interface is no longer supported on Hardware Management Console (HMC) version 8.7.0, or later. The functions that were previously available with the HMC Classic interface are now available with the HMC Enhanced+ interface.
- Added the following topics:
 - “Installing the 7063-CR1 into a rack” on page 42
 - “Configure BMC connectivity” on page 142
- Added the “Installing the 7063-CR1 into a rack” on page 42 topic.

October 2016

- Updated the “HMC port locations” on page 15 topic.

May 2016

- Added the “Installing the 7042-CR9 HMC into a rack” on page 33 topic.

October 2015

- Added the “Installing the HMC virtual appliance” on page 51 topic.
- Updated the following topics:
 - “Internet SSL address lists” on page 79
 - “Preparing for HMC configuration” on page 81

June 2015

- The procedures and functions of the HMC Enhanced + Tech Preview (Pre-GA) interface, which was an option that was provided with HMC version 8.2.0, are the same as the HMC Enhanced+ interface that is provided with HMC version 8.3.0. Only the HMC Enhanced+ is referred to in the documentation, but that content also applies to the HMC Enhanced + Tech Preview (Pre-GA) interface.
- The procedures and functions of the HMC Enhanced interface, which was an option that was provided with HMC version 8.2.0, are now a part of the HMC Enhanced+ interface that is provided with HMC version 8.3.0.
- Added the “Configuring the HMC by using the HMC Enhanced+ interface” on page 117 section.
- Updated the “Configuring the Events Manager for Call Home” on page 106 topic.

October 2014

- Added the following topics:
 - “Installing the 7042-CR7 and 7042-CR8 into a rack” on page 24
 - “Configuring the Events Manager for Call Home” on page 106
- Updated the “Starting the HMC” on page 92 topic.

June 2014

- Added information for IBM Power Systems servers that contain the POWER8 processor.

Installation and configuration tasks

Learn about the tasks associated with different HMC installation and configuration tasks.

This section describes, at a high level, the tasks you must perform when you install and configure your HMC. There are different ways you can install and configure your HMC. Find the situation that best matches the task you want to perform.

Note: If you are managing POWER8[®] processor-based servers, the HMC must be at Version 8.1.0. For more information, see “Determining your HMC machine code version and release” on page 110.

Installing and configuring a new HMC with a new server

Learn more about the high-level tasks you must perform when installing and configuring a new HMC with a new server.

Table 1. Tasks you need to perform when installing and configuring a new HMC with a new server

Task	Where to find related information
1. Gather information and complete the Preinstallation Configuration Worksheet.	“Preinstallation configuration worksheet for the HMC” on page 83 “Preparing for HMC configuration” on page 81
2. Unpack the hardware.	
3. Cable the HMC hardware.	“Cabling your stand-alone HMC” on page 4 “Cabling your rack-mounted HMC” on page 14
4. Power on the HMC by pressing the power button.	
5. Log in and launch the HMC web application.	
6. Access the Guided setup wizard or use the HMC menus to configure the HMC.	“Configuring the HMC by using the fast path through the Guided Setup wizard” on page 90 “Configuring the HMC by using the HMC menus” on page 91
7. Attach the server to the HMC.	

Updating and upgrading your HMC code

Learn more about the high-level tasks you must perform when you update and upgrade your HMC code.

If you have an existing HMC and want to update or upgrade your HMC code, you must complete the following high-level tasks:

Table 2. Tasks you need to perform when updating or upgrading HMC code

Task	Where to find related information
1. Obtain the upgrade.	"Upgrading your HMC software" on page 113
2. View the existing HMC machine code level.	
3. Back up the managed system's profile data.	
4. Back up HMC data.	
5. Record the current HMC configuration information.	
6. Record remote command status.	
7. Save upgrade data.	
8. Upgrade the HMC software.	
9. Verify that the HMC machine code upgrade installed successfully	

Adding a second HMC to an existing installation

Learn more about the high-level tasks you must perform when adding a second HMC to your managed system.

If you have an existing HMC and managed system and want to add a second HMC to this configuration, do the following:

Table 3. Tasks you need to perform when adding a second HMC to an existing installation

Task	Where to find related information
1. Ensure your HMC hardware supports HMC Version 7 code.	
2. Gather information and complete the Preinstallation Configuration Worksheet.	"Preinstallation configuration worksheet for the HMC" on page 83
3. Unpack the hardware.	
4. Cable the HMC hardware.	"Cabling your stand-alone HMC" on page 4 "Cabling your rack-mounted HMC" on page 14
5. Power on the HMC by pressing the power button.	
6. Log in to the HMC.	
7. The HMC code levels must match. Change the code on one of the HMCs to match the code on the other.	"Determining your HMC machine code version and release" on page 110 "Upgrading your HMC software" on page 113
8. Access the Guided setup wizard or use the HMC menus to configure the HMC.	"Configuring the HMC by using the HMC menus" on page 91
9. Configure this HMC for service using the Call-Home Setup Wizard.	"Configuring the HMC so that it can contact service and support" on page 101
10. Attach the server to the HMC.	

Setting up the HMC

You must set up the HMC hardware before you configure the HMC software. Learn more about setting up a desk-side HMC or a rack-mounted HMC.

Cabling your stand-alone HMC

Position the HMC and cable each of the hardware components.

You can cable your stand-alone HMC to a managed system.

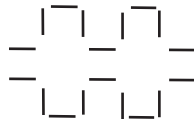
1. Ensure that you position the HMC in the correct location.
2. Attach the monitor cable to the monitor connector, and tighten the screws.
3. Attach the power cord to the monitor.
4. Ensure that the voltage selection switch on the HMC is set to the voltage used in your world region. The voltage selection switch is red and is located near the power connector. Move the switch so that the voltage used at your location is displayed.
5. Plug the power cord into the HMC.
6. Connect the keyboard and mouse to the HMC.
7. Connect the optional modem:

Note: During the installation and configuration of the HMC, the modem might automatically dial out as the HMC follows routine call-out procedures. This is usual behavior.

If you are connecting an optional external modem, do the following:

Note: You can use other connectivity methods to send error information to IBM.

- a. If you have not already done so, connect the modem data cable to the external HMC modem.
- b. Connect the modem data cable to the system port on the HMC that is labeled with the following symbol:



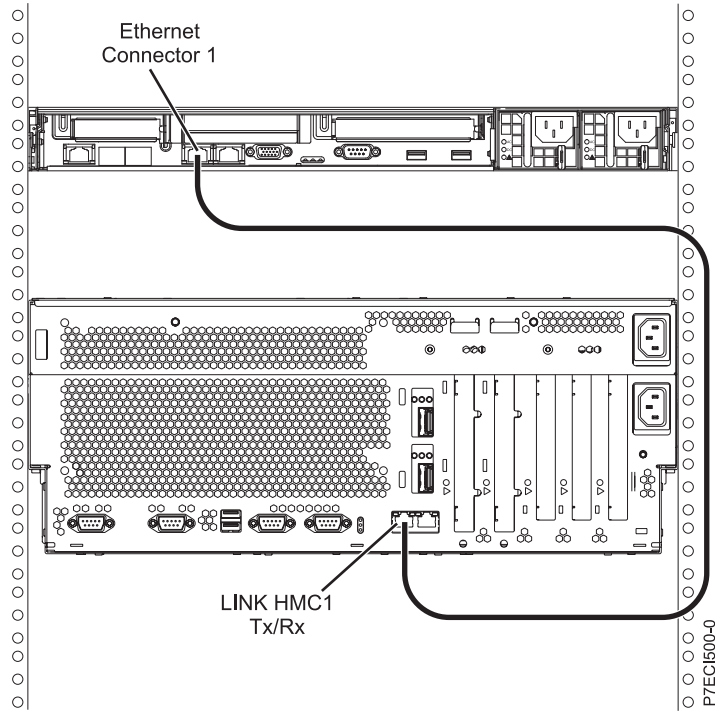
IPHAI522-0

- c. Use the telephone cable to connect the line port of the external modem to the analog telephone jack on your wall.

If you are connecting to an optional integrated modem, use the data cable to connect the integrated HMC modem to the appropriate data source. For example, use the telephone cable to connect the HMC modem line port to the analog jack on your wall.

Note: You can use other connectivity methods to send error information to IBM.

8. If your managed system is already installed, you can verify that the Ethernet cable connection is active by observing the green status lights at both the HMC and managed system Ethernet ports as your installation progresses.
9. Connect **Ethernet Connector 1** on the HMC to the **LINK HMC1** port on the managed system.



10. If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **LINK HMC2** on the managed server.
11. If you use an external modem, plug the modem power supply cord into the HMC modem.
12. Plug the power cords for the monitor, HMC, and HMC external modem into electrical outlets. If you are connecting this HMC to a new managed system, do not connect the managed system to a power source at this time.

Next, you will need to configure your HMC software. Continue with “Configuring the HMC” on page 89.

Related concepts:

- “Deciding which connectivity method to use for the call-home server” on page 76
- Learn more about the connectivity options you have when you use the call-home server.
- “HMC network connections” on page 72

Installing the 7310-CR4 HMC into a rack

This section describes how to install the 7310-CR4 HMC into a rack. This is a customer task.

If an HMC is used to manage any POWER7[®] processor-based system, the HMC must be a CR3, or later, model rack-mounted HMC.

The following is a rear-view of the 7310-CR4:

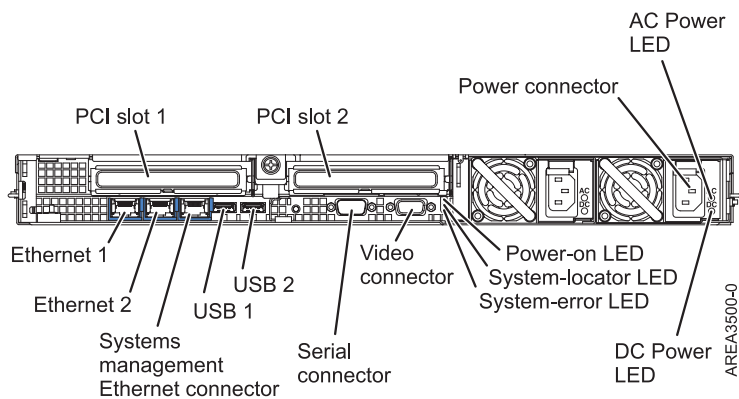


Figure 1. Rear-view of the 7310-CR4

To install the 7310-CR4 HMC into a rack, complete the following steps:

1. Complete a parts inventory. See Completing a parts inventory.
2. Locate the rack-mounting hardware kit and the system rail assemblies that were included with your system unit.

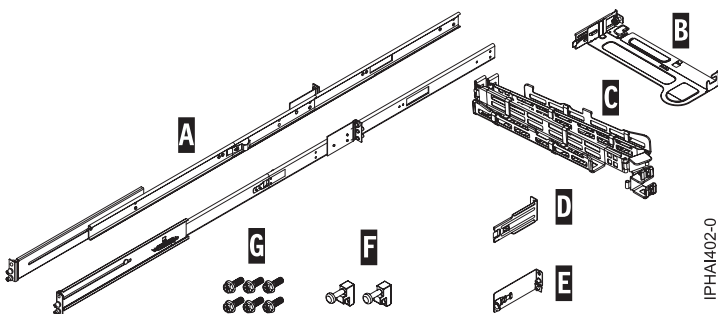


Figure 2. Rail Kit

Table 4. Rail kit parts

Sliding-rail kit parts

- A Slide rails
- B Cable-management arm mounting plate
- C Cable-management arm
- D Cable-management bracket
- E Cable-management support bracket and security tab
- F Latch strikes (2)
- G Screws (6)

Important: This system unit is 1 EIA unit high; you will need this information to complete the installation.

Completing a parts inventory

You might need to complete a parts inventory. Use the procedure in this section to perform this task.

If you have not done so, complete a parts inventory before proceeding with the installation:

1. Locate the kitting report in an accessory box.
2. Ensure that you received all the parts that were ordered.

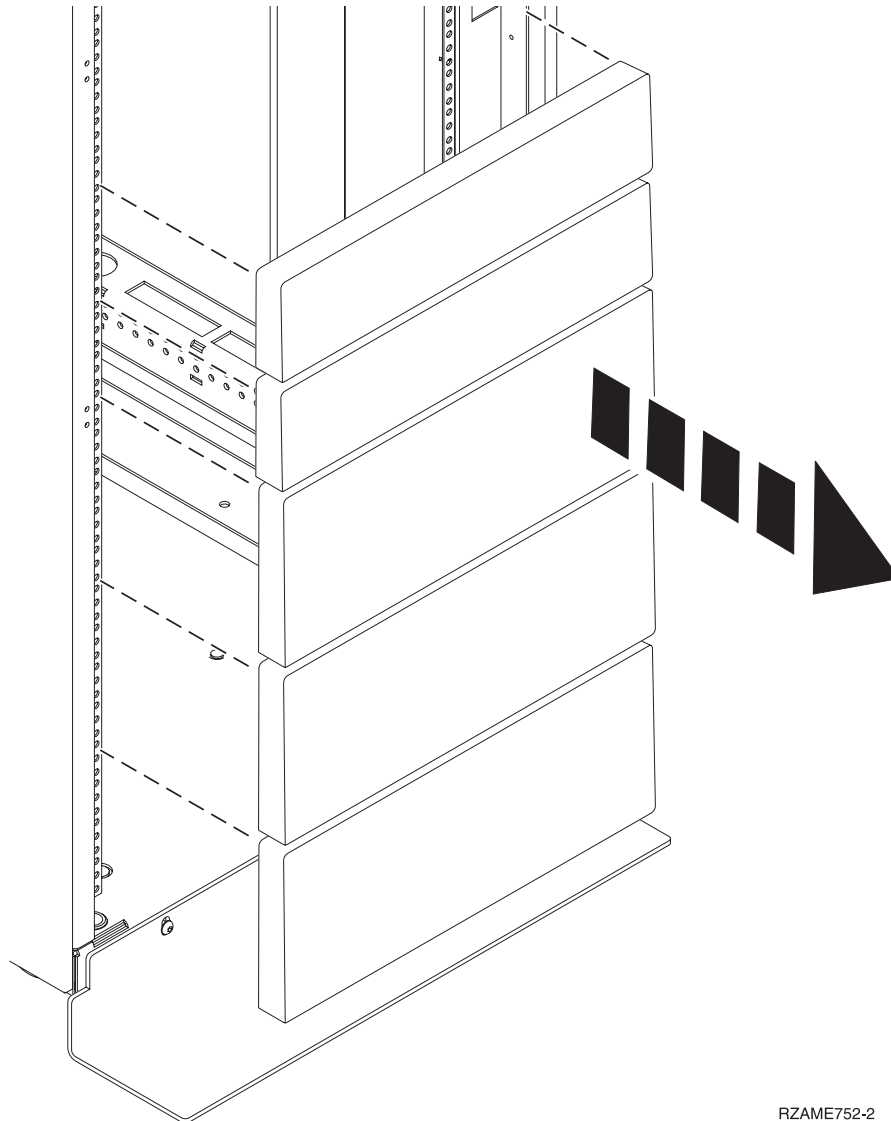
If there are incorrect, missing, or damaged parts, contact your IBM reseller or IBM sales and support.

Determining the location

You might need to determine where to install the system in the rack. This section includes procedures so that you can perform these tasks.

Before installing the HMC into a rack, complete the following steps:

1. Plan where you will place the units. Place the larger and heavier units in the lower part of the rack.
2. If the rack contains filler panels, remove the filler panels to allow access to the inside of the rack enclosure where you plan to place the unit.



RZAME752-2

Figure 3. Removing the filler panels.

3. Remove the front and rear rack doors if necessary.
4. Follow the instructions for marking the location without a template, see [Marking the location without a rack-mounting template](#).

Marking the location without using a rack-mounting template:

You can mark the location without using a template.

A rack-mounting template is not included with this system. These systems are 1 EIA unit high.

To determine the mounting location, complete the following steps:

1. Determine to place the system in the rack. Record the EIA location.

Note: An EIA unit on your rack consists of a grouping of three holes.

2. Facing the front of the rack and working from the right side, place a supplied self-adhesive dot next to the top hole of the EIA unit.

Note: The self-adhesive dots are used to aid in identifying locations on the rack. If you no longer have any of the dots, use some other form of marking tool to aid you in identifying hole locations (for example, tape, a marker, or pencil). If you are installing slide rails, place a mark or self-adhesive dot on the lower and the middle hole of each EIA unit.

3. Place another self-adhesive dot next to the bottom hole of the above EIA unit.

Note: If you are counting the holes, begin with the hole identified by the first dot and count up two holes. Place the second dot next to the third hole.

4. Repeat step 1 for the corresponding holes located on the left side of the rack.
5. Go to the rear of the rack.
6. On the right side, find the EIA unit that corresponds to the bottom EIA unit marked on the front of the rack.
7. Place a self-adhesive dot at the bottom EIA unit.
8. Place a self-adhesive dot at the top hole of the EIA unit.
9. Mark the corresponding holes on the left side of the rack.

Installing slide rails into the rack

Learn how to install slide rails into the rack.

To install the slide rails into the rack, complete the following steps:

1. Insert the right slide rail **(A)**, which is marked right, into the rack mounting flange **(B)** locations, on the rear right side of the rack. The two rail pins will protrude through the bottom and middle holes **(B)** on the EIA unit.

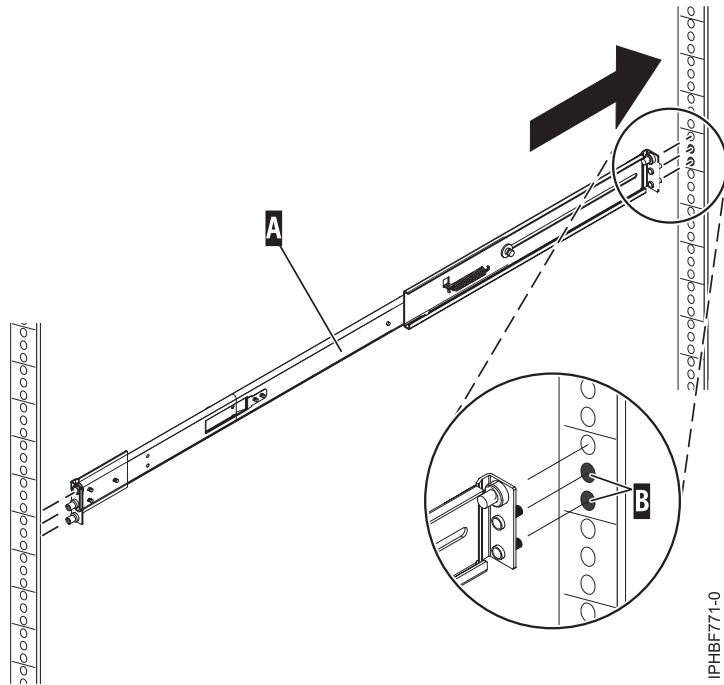


Figure 4. Installing the right slide rail into the rear of the rack

2. Push on the end of the rail (**A**) to compress the rail's spring-loaded mechanism, and insert the rail into the mounting flange (**B**) locations, on the right side of the rack. The rail will decompress and the two rail pins will protrude through the bottom and middle holes (**B**) on the EIA unit.

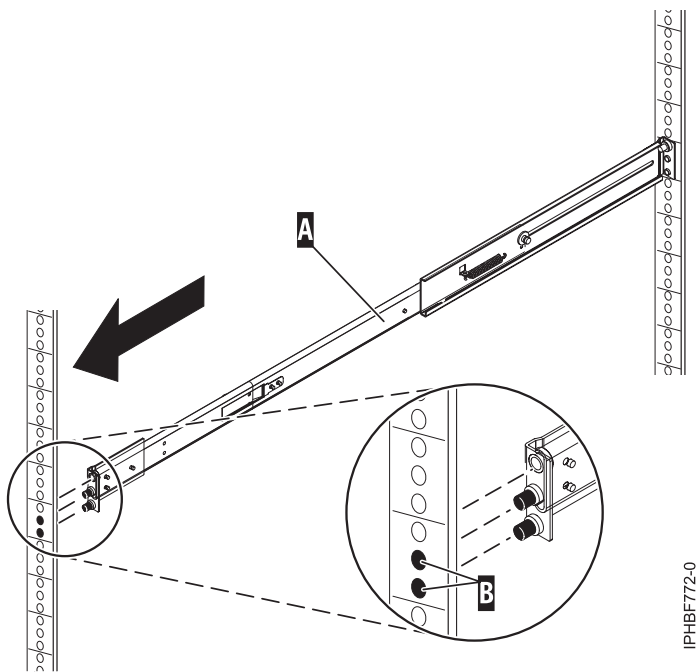


Figure 5. Installing the right slide rail into the front of the rack

3. Repeat steps 1 on page 8-2 to install the left slide rail, which is marked *left*, into the rack.

4. From the front of the rack, place the latch strike (C) over the pins. Finger-tighten the captive screw (D) into the top pin in the front of the right slide rail (A).

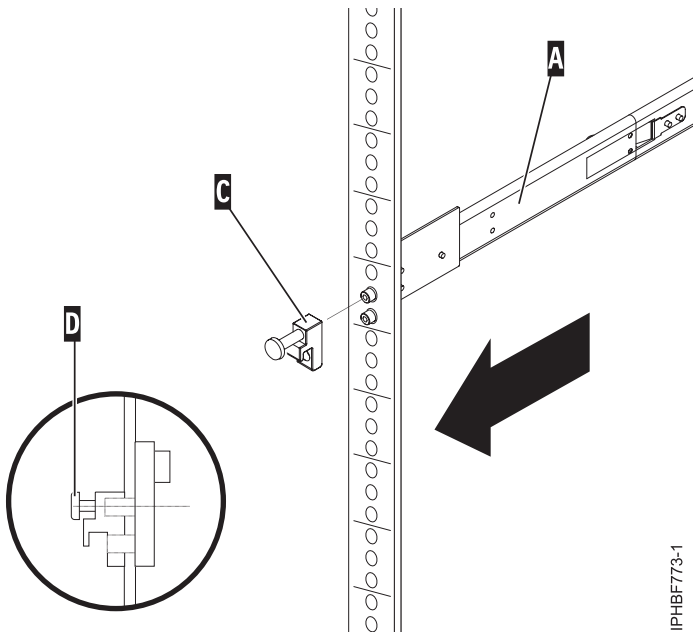


Figure 6. Installing the latch strike to the front of the rails

5. Repeat the previous step to install the latch strike on the front of the left slide rail.
6. Move to the rear of the rack. Finger-tighten screw (F) to attach the cable-management arm mounting bracket (E) to the rear of the left rail (G).

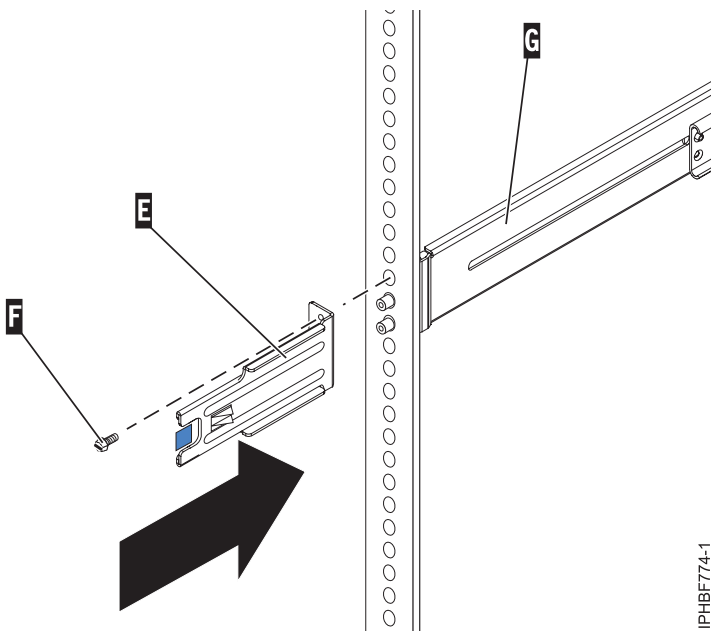


Figure 7. Attaching the cable-management bracket to the rear-left rail

7. If you do not plan to transport this system, continue with “Installing the HMC on the slide rails.” If you plan to transport this system, insert screw (I) to attach the cable-management arm support bracket (H) to the rear right side of the rail (A). Finger-tighten the screw.

The support bracket of the cable-management arm can be used to secure the cable-management arm during transportation. If the mechanism is engaged after the cable-management arm is installed, you will not be able to slide the system from the rack.

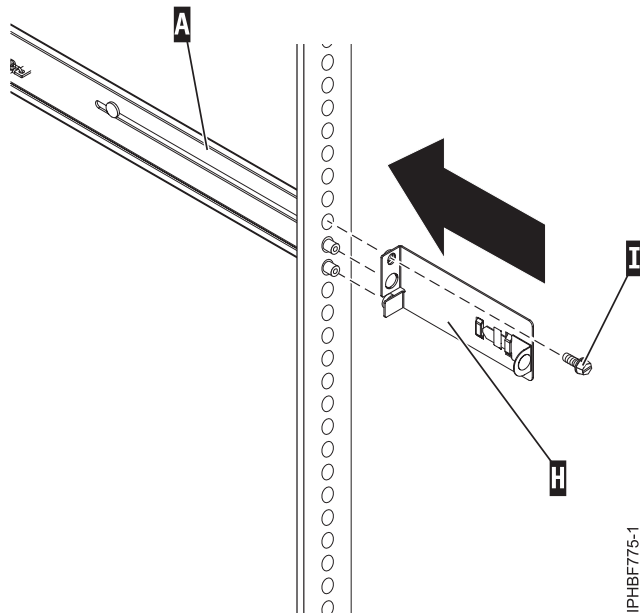


Figure 8. Attaching the support bracket of the cable-management to the rear-right rail.

Installing the HMC on the slide rails

You might need to install the HMC on the slide rails. Use the procedure in this section to perform this task.

Before installing the HMC on the slide rails, ensure that the stabilizers are extended and the rack stabilizer bracket is attached to the bottom front of the rack to prevent the rack from falling forward when the rails are pulled out of the rack.

To install the HMC on the slide-rail assembly, complete the following steps:

1. Remove the shipping bracket that covers the power supplies from the right rear of the HMC. To remove the shipping bracket, push to the bracket to the right and swivel the shipping bracket off the HMC.
2. From the front of the rack, fully extend the slide rails until the rails lock into place in the extended position (A).

Attention: The latch strikes on the front of the rail and the cable-management arm brackets must be installed *before* installing an HMC onto the rails. If these parts are not installed, the installation may cause the rails to compress and the HMC may fall out of the rack.

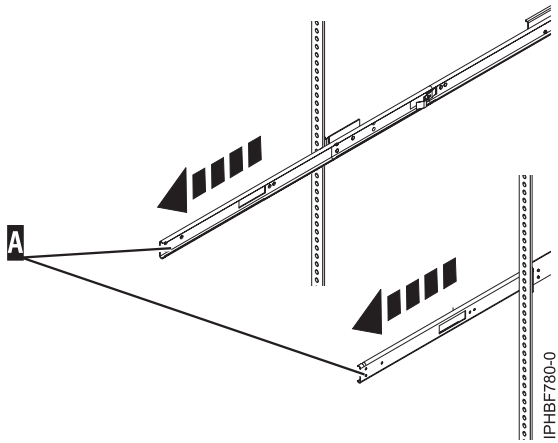


Figure 9. Extending the slide rails

Important: This unit weighs approximately 17 kg (37 pounds). Be sure that you can safely support this weight when placing the HMC into the rack.

3. Lift the HMC to the height of the rails, and position the set of wheels (B), at the rear of the HMC, between the rail guides.

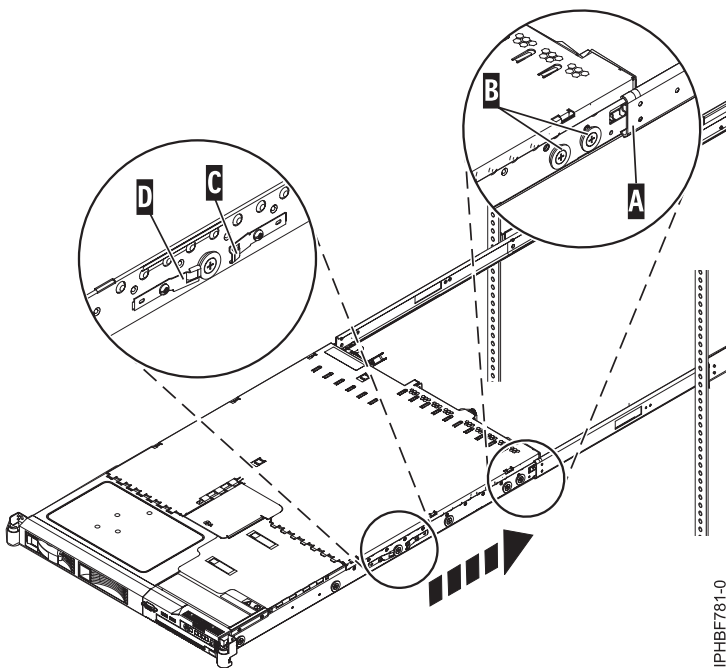


Figure 10. Installing the HMC on the slide rails.

4. Push the HMC into the slide rails until the slide release catches (C) lock into place. This locks the system in the service position on the slides. You will hear an audible click.
5. Press the front-slide rail release latches (D) on both sides of the slide rails.
6. Slide the HMC into and out of the rack to verify that the HMC moves freely without binding.

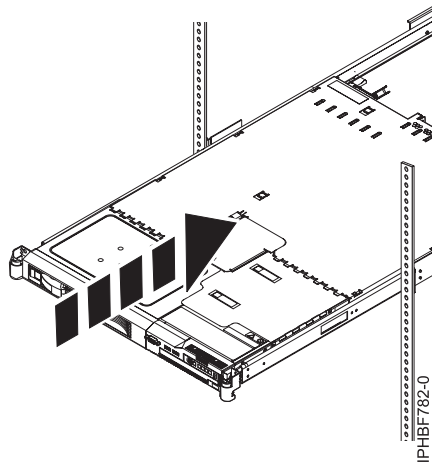


Figure 11. Slide the HMC into the rack

Important: Do not, under any circumstances, force the HMC into the slide rails. If the HMC does not slide freely into the rack, completely remove the HMC from the rails. After the HMC is clear of the rails, reposition the HMC, then reinsert the HMC into the rails. Repeat this process until the HMC slides freely into the rack.

7. Push the HMC into place until the rack latches (F) lock into place.

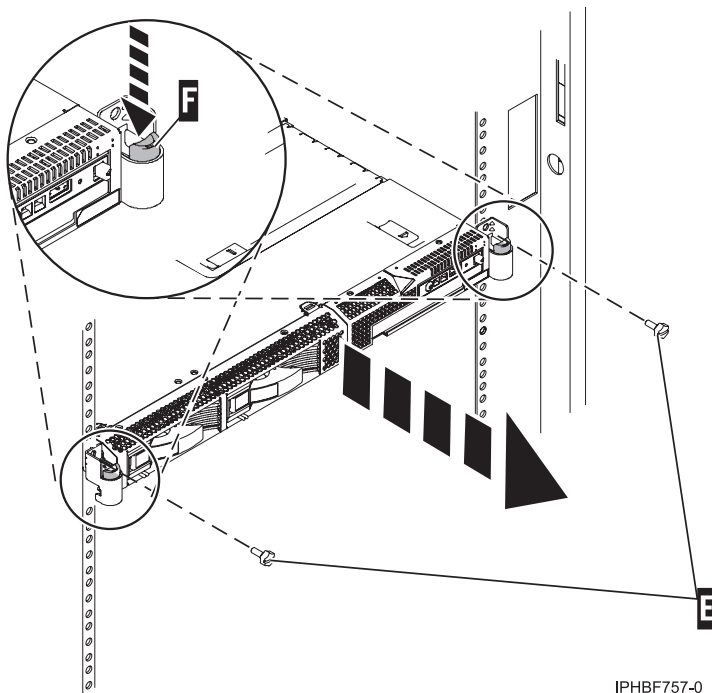


Figure 12. Rack latches and screws

8. Completely tighten each of the four screws that were installed in the front and back of both rails.
9. If the rack will be transported, insert and tighten the two rack security screws (E).

Installing the cable-management arm

You might need to install the cable-management arm. Use the procedure in this section to perform this task.

To install the cable-management arm, complete the following steps:

1. From the rear of the rack, locate the cable-management arm flange (A) located on the fixed rear portion of the left system rail assembly (viewing from the rear of the rack).
2. Attach the cable-management arm clasp (B) to the rail by pushing the clasp onto the rail until it locks into place.

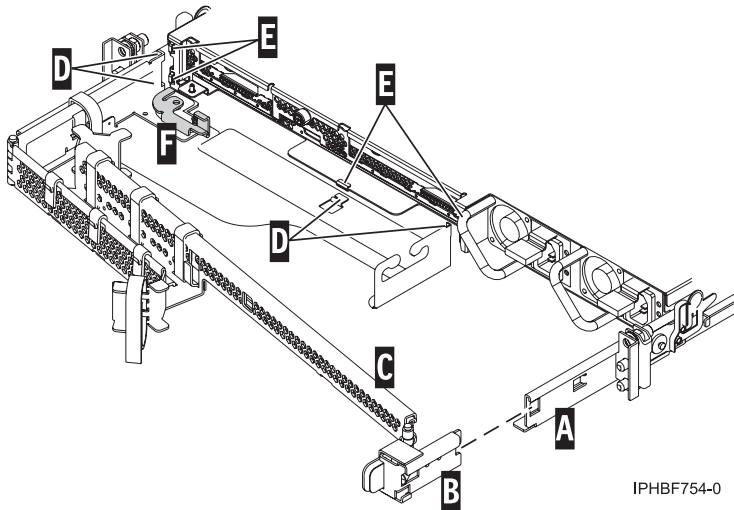


Figure 13. Cable-management arm and system unit.

3. Attach the other end of the cable-management arm (C) to the rear of the HMC. Align the tabs (D) on the cable-management arm with the slots (E) on the rear of the HMC.
4. Slide the cable-management arm to the left, securing it into place. Make sure all the tabs fit into the slots.
5. Push the locking lever (F) into the locked position. Ensure that the cable-management arm (C) is level so that it moves freely.

Cabling your rack-mounted HMC

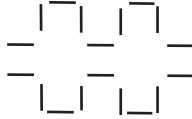
Learn how to physically install your rack-mounted HMC.

1. Ensure that you position the HMC in the correct location.
2. Install the HMC into a rack. For more information, see “Installing the 7310-CR4 HMC into a rack” on page 5. When you are finished installing the HMC into a rack, continue with the next step.
3. Plug the power cord into the HMC.
4. Connect the keyboard, monitor, and mouse.
5. Connect an optional modem:

If you are connecting an external modem, do the following:

Note: You can use other connectivity methods to send error information to IBM. For more information, see “Deciding which connectivity method to use for the call-home server” on page 76.

- a. If you want to install the external modem into a rack, do it now.
- b. If you have not already done so, connect the modem data cable to the external HMC modem.
- c. Connect the modem data cable to the system port on the HMC labeled with the following symbol:



IPHAI522-0

- d. Use the telephone cable to connect the line port of the external modem to the analog telephone jack on your wall.
- e. Plug the modem power supply cord into the HMC modem.

If you are connecting to an integrated modem, use the data cable to connect the integrated HMC modem to the appropriate data source. For example, use the telephone cable to connect the HMC modem line port to the analog jack on your wall.

Note: You can use other connectivity methods to send error information to IBM. For more information, see “Deciding which connectivity method to use for the call-home server” on page 76.

- 6. Connect the Ethernet (or crossover) cable from the HMC to the managed server:

Note: To learn more about the HMC network connections, see “HMC network connections” on page 72.

- 7. If your managed system is already installed, you can verify that the Ethernet cable connection is active by observing the green status lights at both the HMC and managed system Ethernet ports as your installation progresses.
- 8. Connect the Ethernet port on the HMC to the Ethernet port that is labeled **HMC1** on the managed server.
- 9. If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **HMC2** on the managed server.
- 10. Plug the power cords for the monitor, HMC, and HMC external modem into electrical outlets.

Note: If you are connecting this HMC to a new managed system, do not connect the managed system to a power source at this time.

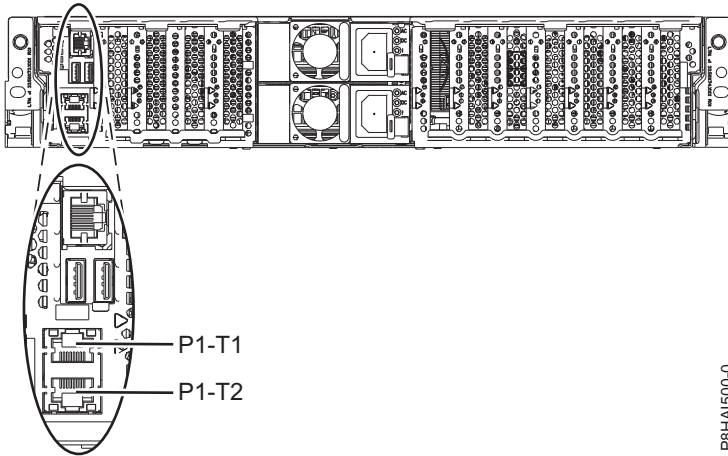
Next, you will need to configure your HMC software. Continue with “Configuring the HMC” on page 89.

HMC port locations

You can find part locations by using location codes. Use the HMC port location illustrations to map a location code to the HMC port position on the server.

Model 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

Use this diagram and table to map the HMC ports on the 8247-21L, 8247-22L, 8284-21A, or 8284-22A.



P8HA1500-0

Figure 14. 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

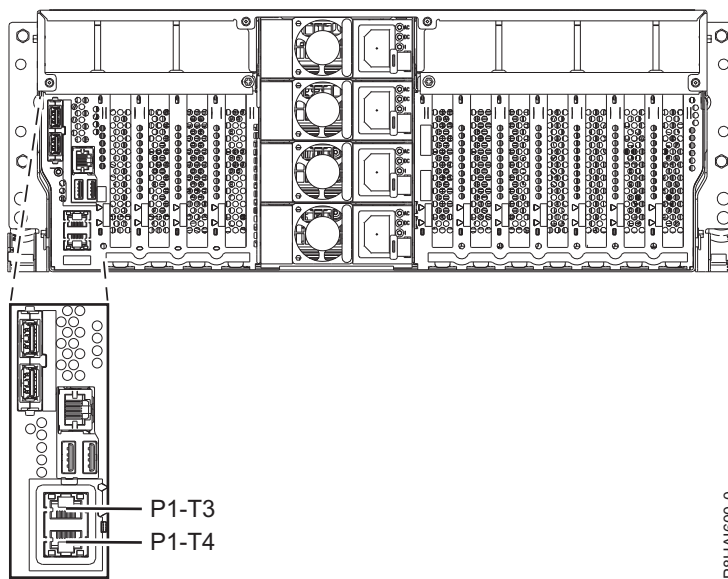
Table 5. 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-T1	No
HMC port 2	Un-P1-T2	No

For more information on HMC port locations about the 8247-21L, 8247-22L, 8284-21A, or 8284-22A, see Part location and location codes for 8247-21L, 8247-22L, or 8284-22A.

Model 8247-42L, 8286-41A, or 8286-42A HMC port locations

Use this diagram and table to map the HMC ports on the 8247-42L, 8286-41A, or 8286-42A.



P8HA1600-0

Figure 15. Rack view - 8247-42L, 8286-41A, or 8286-42A HMC port locations

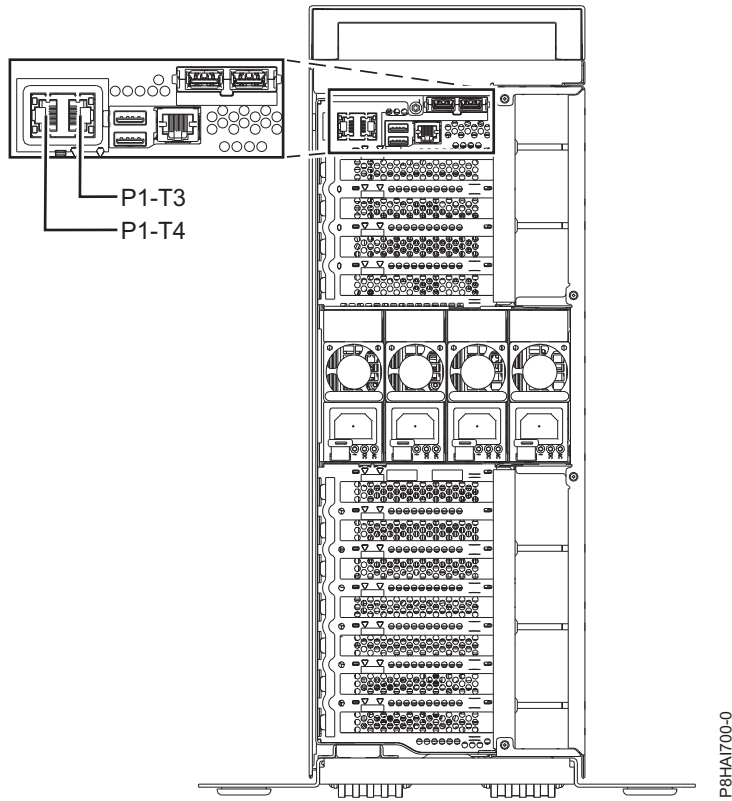


Figure 16. Tower view - 8286-41A HMC port locations

Table 6. 8247-42L, 8286-41A, or 8286-42A HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-T3	No
HMC port 2	Un-P1-T4	No
For more information about HMC port locations on the 8247-42L, 8286-41A, or 8286-42A, see Part location and location codes for 8247-42L, 8286-41A, or 8286-42A.		

Model 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Use this diagram and table to map the HMC ports on the 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME.

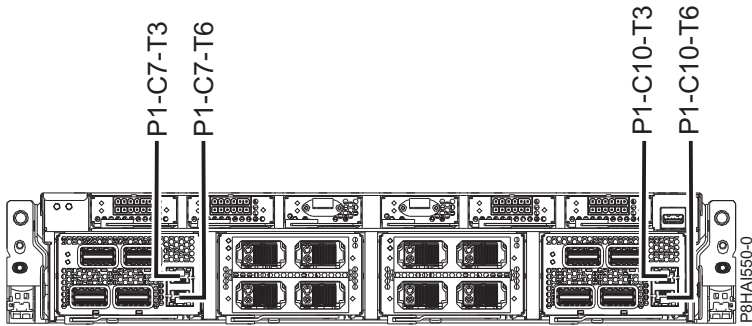


Figure 17. 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Table 7. 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Port	Physical location code	Identify LED
Service processor card 1 - HMC port 1	Un-P1-C7-T3	No
Service processor card 1 - HMC port 2	Un-P1-C7-T6	No
Service processor card 2 - HMC port 1	Un-P1-C10-T3	No
Service processor card 2 - HMC port 2	Un-P1-C10-T6	No

For more information about HMC port locations on the 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME, see Part location and location codes for 9080-MHE, 9080-MME, 9119-MHE, or 9119-MME locations.

Model 8408-44E and 8408-E8E HMC port locations

Use this diagram and table to map the HMC ports on the 8408-44E and 8408-E8E.

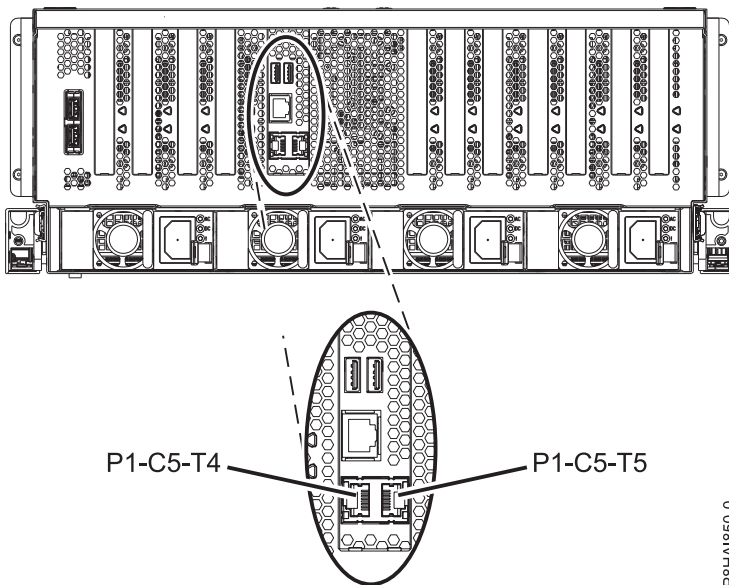


Figure 18. 8408-44E and 8408-E8E HMC port locations

Table 8. 8408-44E and 8408-E8E HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-C5-T4	No
HMC port 2	Un-P1-C5-T5	No

For more information about HMC port locations on the 8408-44E and 8408-E8E, see Part location and location codes for 8404-44E and 8408-E8E locations.

Installing the 7042-CR5 and 7042-CR6 into a rack

This section describes how to install the 7042-CR5 and 7042-CR6 HMC into a rack.

Complete a parts inventory. The following illustration shows the items that you need to install the server in the rack cabinet. If any items are missing or damaged, contact your place of purchase.

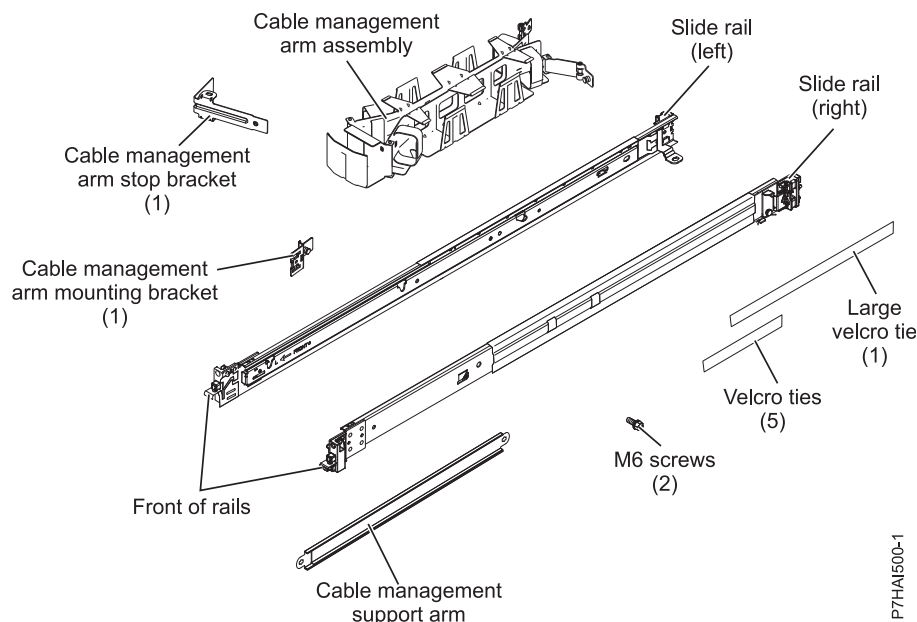
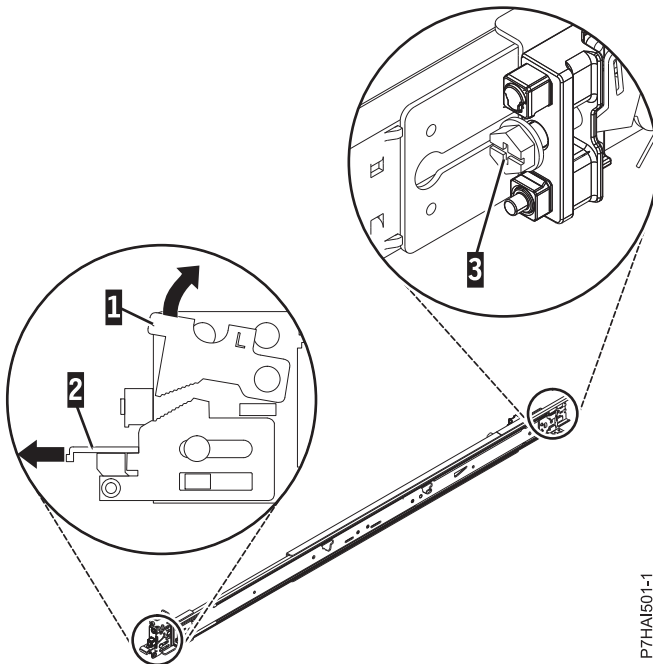


Figure 19. Parts inventory

Note: Screws can be used for shipping, or for additional stabilization in high-vibration areas.

To install a 7042-CR5 or 7042-CR6 HMC into a rack, complete the following steps:

1. Each slide rail is marked with either an R (right) or an L (left). Select one of the slide rails and push up on the front movable tab (1); then, pull out the front latch (2) to slide out the front side rail. If a thumbscrew is installed in the slide rail (3), remove it.

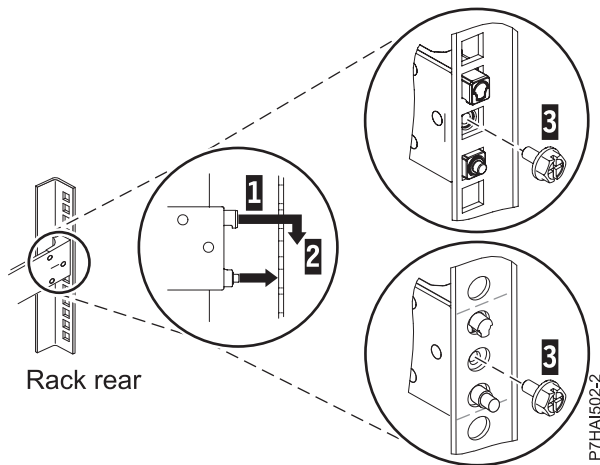


PTHAE01-1

Figure 20. Slide rail and movable tab

Note: Make sure that the movable tab remains extended and does not click back into place.

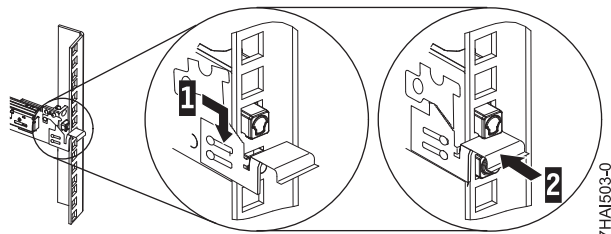
- Align the three pins on the rear of the slide rail with the three holes in the selected U on the rear of the rack. Push the rails so that the pins go into the holes (1), and drop the slide rail down (2) until it latches into place.



PTHAE02-2

Figure 21. Align the pins with the holes in the rear of the rack

- Pull the slide rail forward and insert the two pins (1) on the front of the rail into the two lower holes in the U on the front of the rack. Drop the rail into place until it clicks into place. Push the front latch (2) in all the way. Repeat steps 1 through 3 to install the other rail into the rack. Make sure that each front latch is fully seated.



Rack Front
Figure 22. Rack front rail and pins

4. Pull the slide rails forward (1) until they click, twice, into place. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads (2) on the server line up with the rear slots (3) on the slide rails. Slide the server down until the rear nail heads slip into the two rear slots, and then slowly lower the front of the server (4) until the other nail heads slip into the other slots on the slide rails. Make sure that the front latch (5) slides over the nail heads.

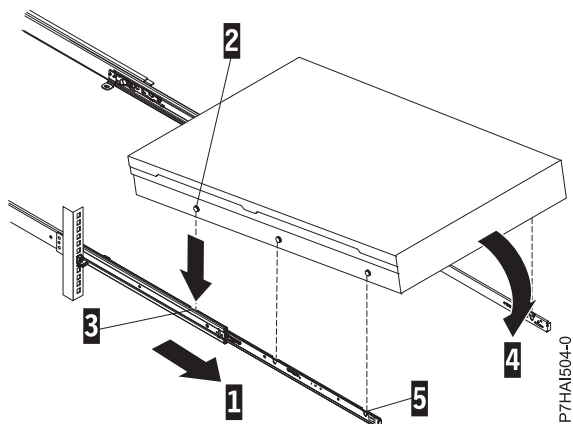


Figure 23. Slide rails extended, server nail heads aligned with slots in rail

5. Lift the blue release latches (1) on the slide rails and push the server (2) all the way into the rack until it clicks into place.

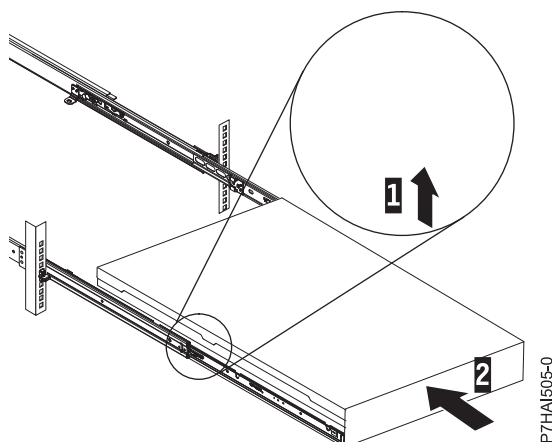


Figure 24. Release latches and server

6. The cable-management arm can be installed on either side of the server. The following figure shows it being installed on the left side. To install the cable-management arm on the right side, follow the instructions and install the hardware on the opposite side. Connect one end of the support arm (1) to the same slide rail to which you plan to attach the cable-management arm so that you can swing the other end of the support arm (2) toward the rack.

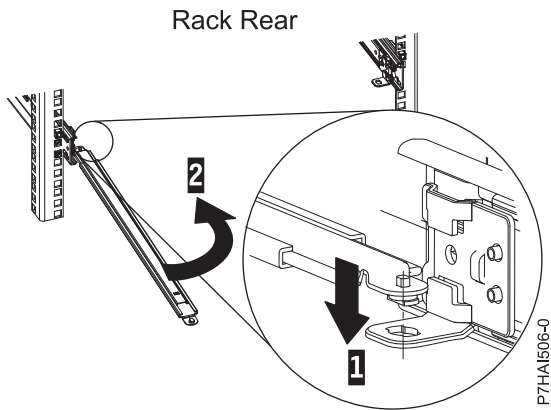


Figure 25. Support arm connection

7. Install the L-shaped cable-management stop bracket (1) on the unattached end of the support arm. Turn the bracket (2) to secure it to the support arm.

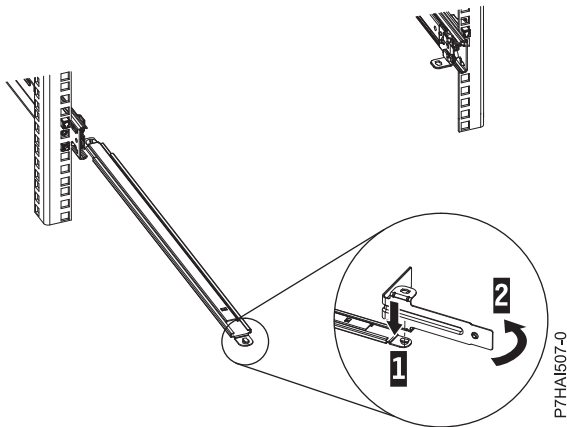


Figure 26. Cable-management stop bracket secured to the support arm

8. To attach the other side of the support arm to the backside of the slide rail, pull the pin out (1), and then slide the bracket (2) into the slide rail.

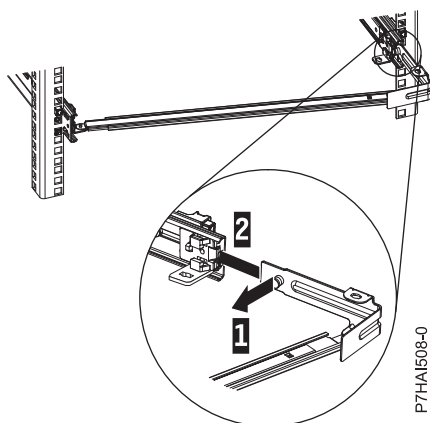


Figure 27. Pin extended, bracket installed into slide rail

9. Pull out the mounting bracket pin (1) and slide the mounting bracket (2) into the slide rail onto which you are installing the cable-management arm. Push the bracket into the slide rail until the spring-loaded pin snaps into place.

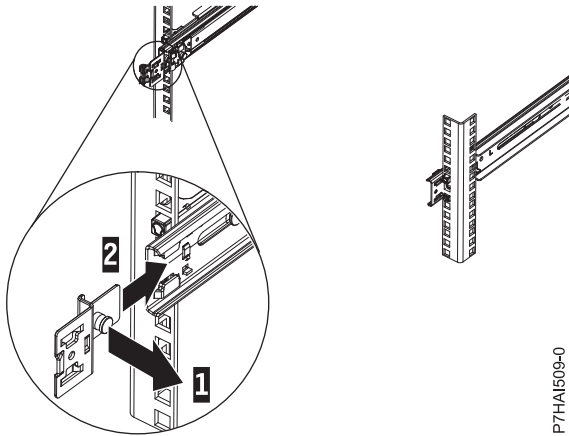


Figure 28. Mounting bracket pin extended and mounting bracket installed into slide rail

- Place the cable-management arm on the support arm. Pull out the cable-management arm pin (1), and then slide the cable-management arm tab (2) into the slot on the inside of the slide rail. Push the tab until it snaps into place. Pull out the other cable-management arm pin (3), and then slide that cable management arm tab into the slot (4) on the outside of the slide rail. Push the tab until it snaps into place.

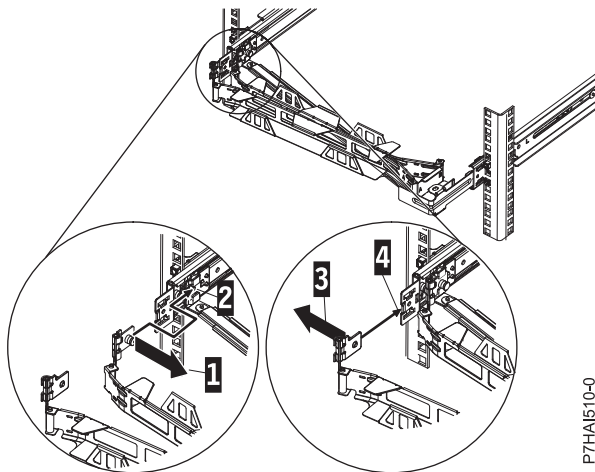


Figure 29. Cable-management arm connection

- Attach the power cords and other cables to the rear of the server (including keyboard, monitor, and mouse cables, if required). Route the cables and power cords on the cable-management arm (1) and secure them with cable ties or hook-and-loop fasteners.

Note: Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.

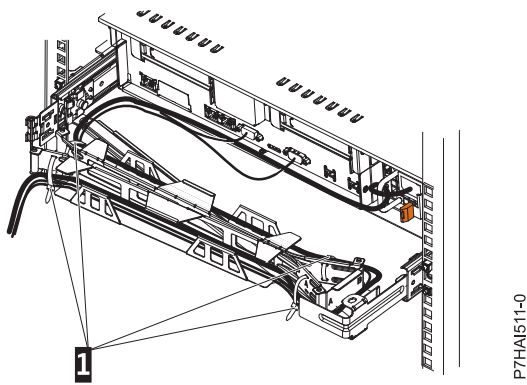


Figure 30. Power cord attachment and routing

12. Slide the server into the rack until it snaps into place.

Installing the 7042-CR7 and 7042-CR8 into a rack

Learn how to install the 7042-CR7 and 7042-CR8 Hardware Management Console (HMC) into a rack.

Complete a parts inventory. The following illustrations show the items that you need to install the server in the rack cabinet. If any items are missing or damaged, contact your place of purchase.

Cable Management Arm box contents

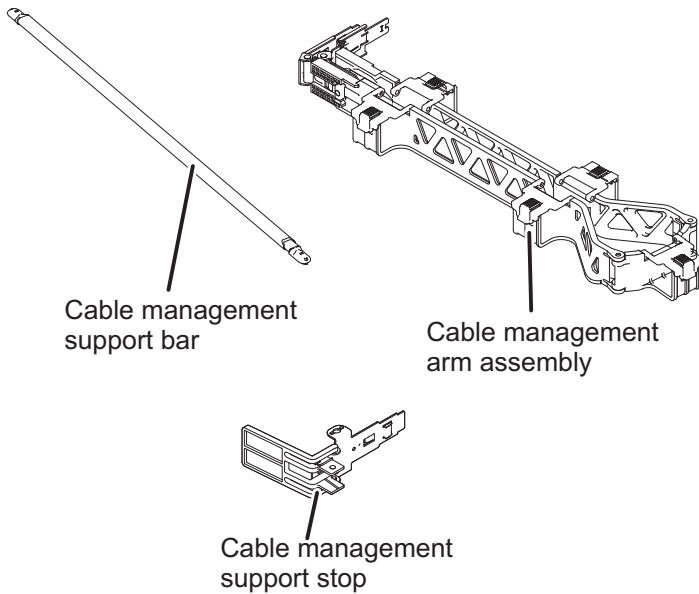
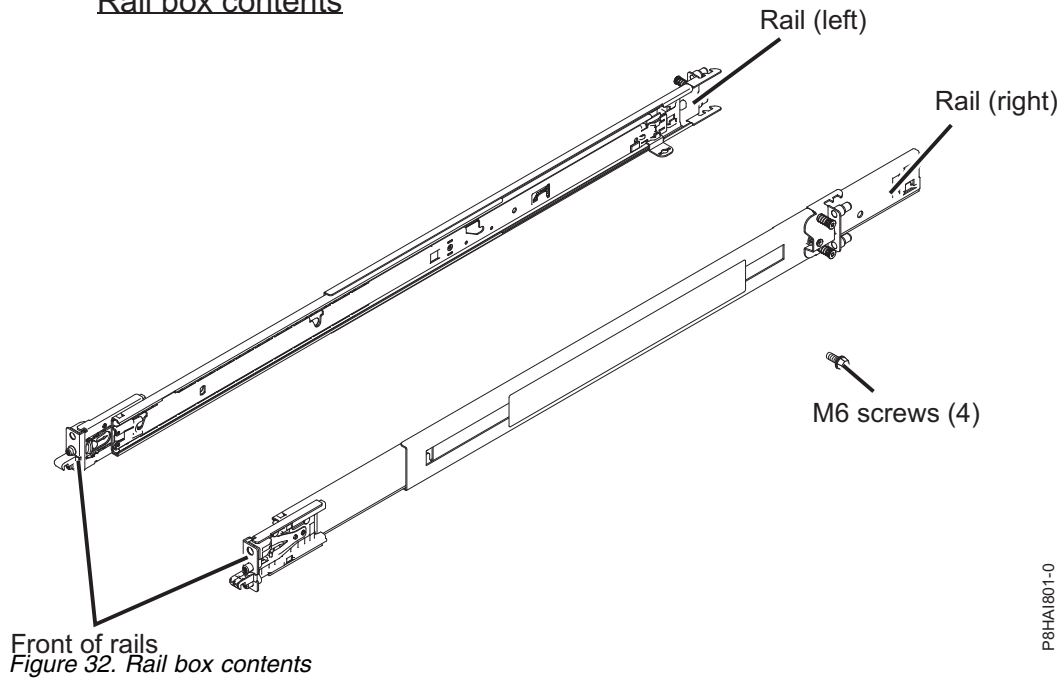


Figure 31. Cable management arm box contents

Rail box contents



Note: You will need both the slide rail box and the cable management arm box for this installation.

To install a 7042-CR7 or 7042-CR8 HMC into a rack, complete the following steps:

1. Select an available 1 unit or 2 unit space (depending on the server you are installing) in your rack to install your server.

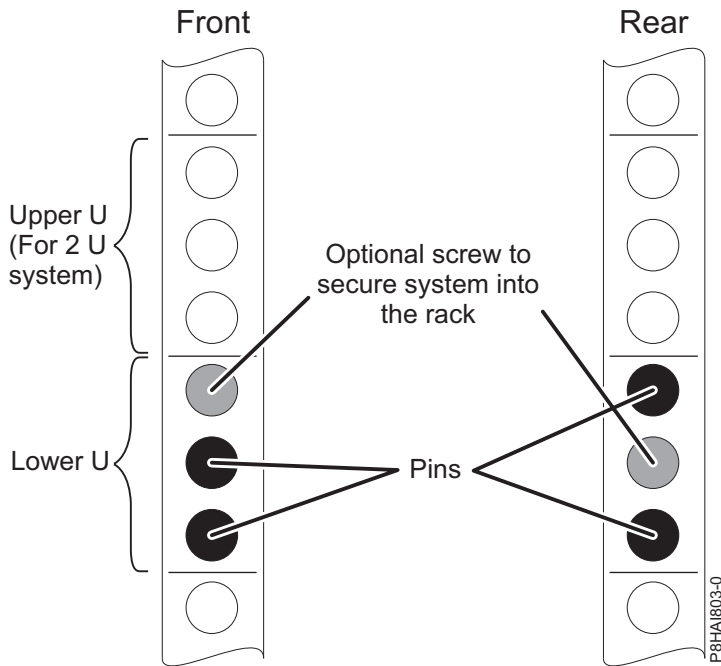


Figure 33. Identifying a rack space

Note: When you install a 2 unit server, be sure to install the slide rails in the lower U of the 2 U area in the rack.

- Each slide rail is marked as **Left Front/Rear** or **Right Front/Rear** on its end. Select one of the slide rails and pull the rear bracket all the way back until it clicks into place.

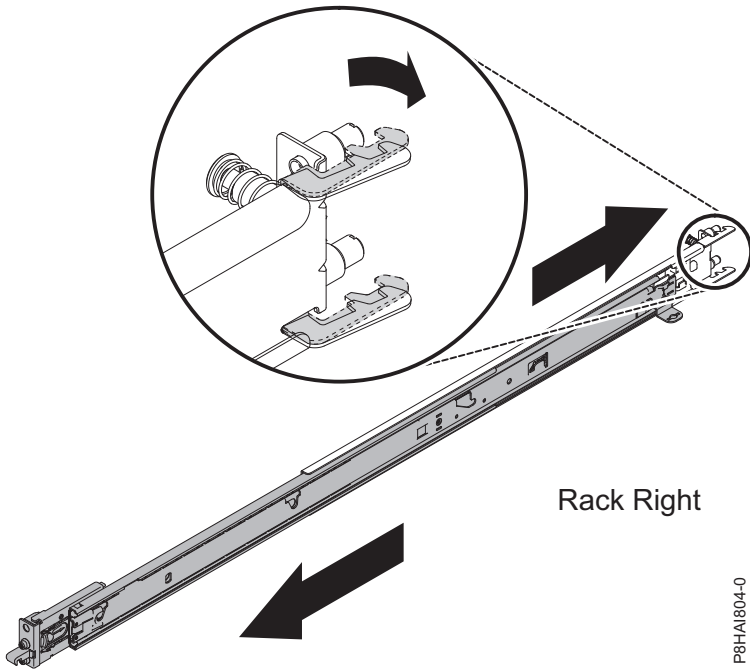


Figure 34. Slide rail and the movable tab

Note: Ensure that the movable tab remains extended and does not click back into place.

- From the front of the rack, line up the two pins on the rear of the slide rail in the selected U on the rear of the rack. Push the rails so that the pins go into the holes and slide the rails into the rack to lock the rear of the slide rails into the rack.

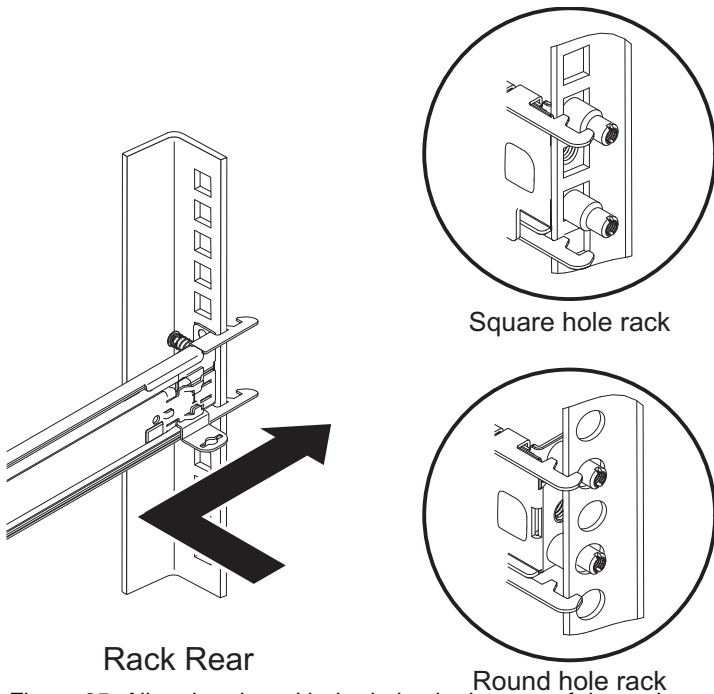


Figure 35. Align the pins with the holes in the rear of the rack

Note: If you are installing the slide rails into a 1 U space with devices already installed directly above and below this 1 U space, you must extend the rails to slide the rear of the slide rails into the rear of the rack.

4. Open the front slide rail latch. If they are closed when you receive them, open the latches by pushing the blue button in and by pushing the latch back.

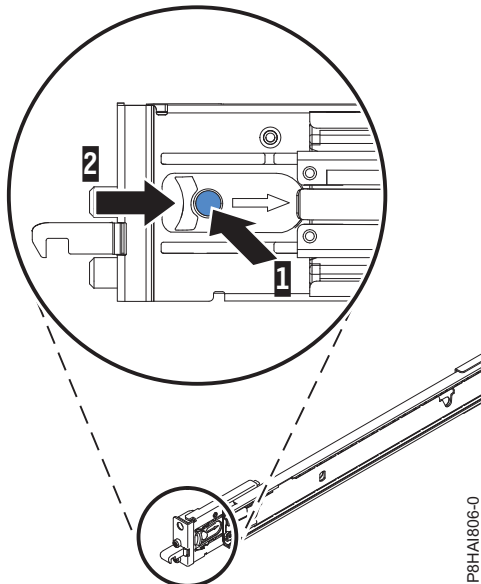


Figure 36. Front slide rail latch

5. Pull the slide rails forward and locate the front latches in the appropriate U spaces in front of the rack EIA rails. Adjust the length of the rails. Ensure that the front end is being rotated into position with the front latch in front of the EIA rail of the rack.

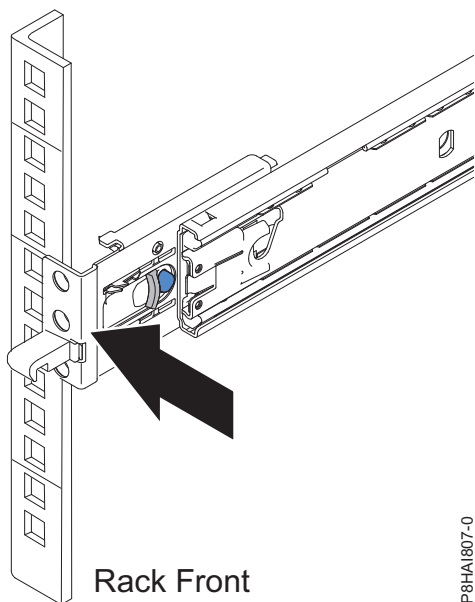
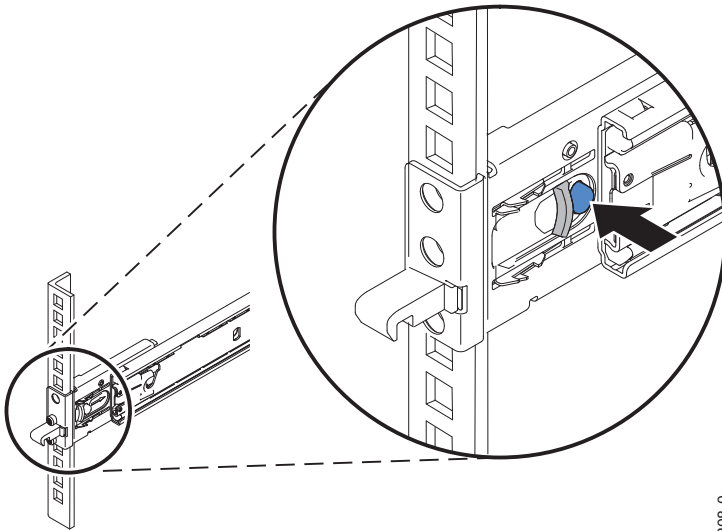


Figure 37. Rack front rail and pins

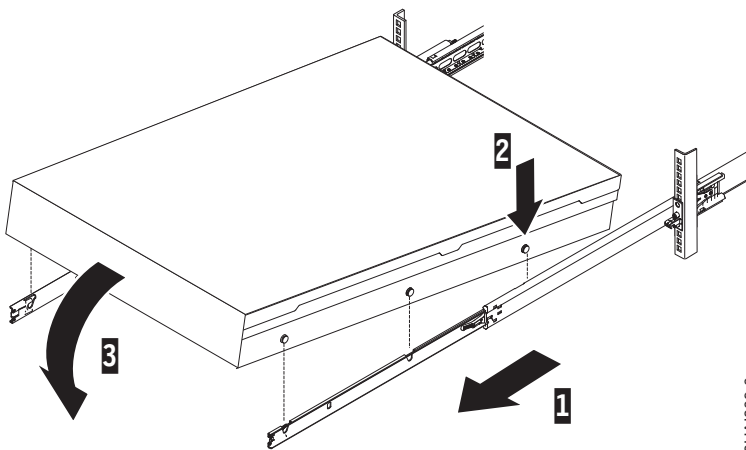
6. Press the blue button to close the bracket with the pins. Moving the slide rail up and down to ensure that the rail is fully engaged. Repeat steps 1 - 5 to install the other rail into the rack. Ensure that each front latch is fully engaged.



P8HAI808-0

Rack Front
 Figure 38. Rack front rail and pins

7. Pull the slide rails forward (1) until they click, twice, into place. Carefully lift the server and tilt it into position over the slide rails such that the rear nail heads (2) on the server line up with the rear slots on the slide rails. Lower the server down until the rear nail heads slip into the two rear slots, and then slowly lower the front of the server (3) until the other nail heads go into the other slots on the slide rails (by hearing the clicks twice). Ensure that the front latch covers the front nail head such that the system is secured to the slide rails.



P8HAI809-0

Figure 39. Slide rails extended, server nail heads aligned with slots in rail

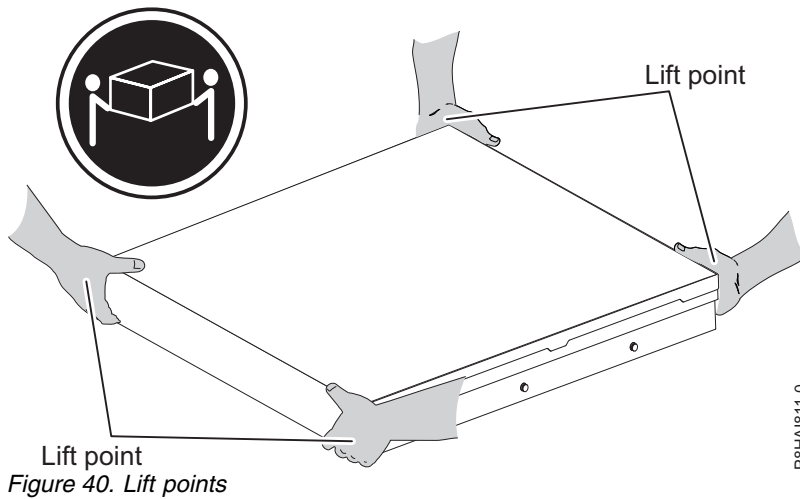


Figure 40. Lift points

Note: Use safe practices while lifting. If you are installing a 2 U server, ensure that you have two people when lifting the server. Their hands must be positioned as illustrated in Figure 40.

8. Lift the locking levers (1) on the slide rails and push the server (2) all the way into the rack until it clicks into place.

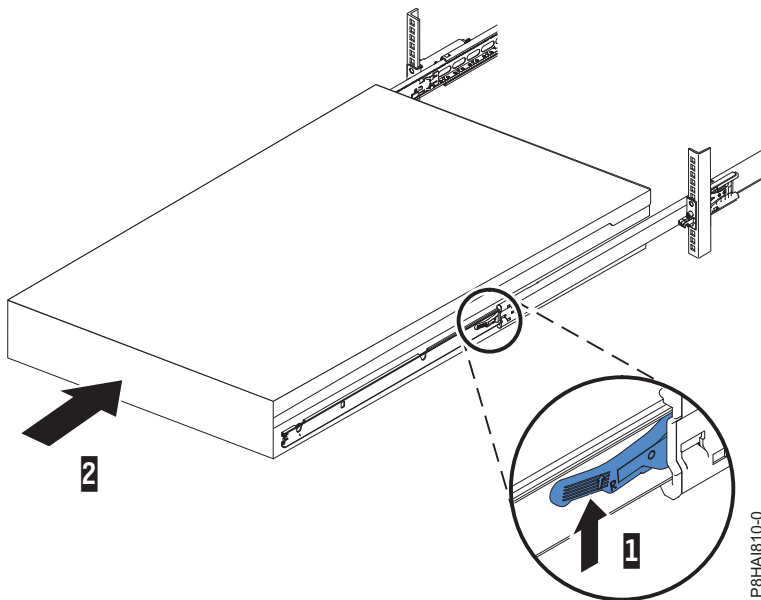
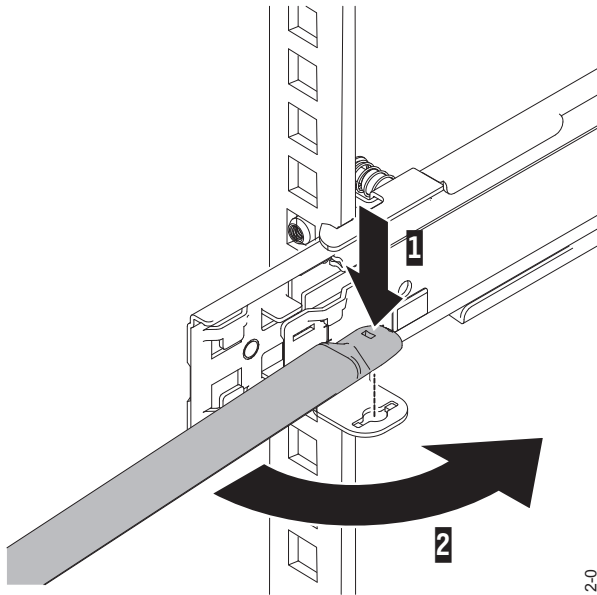


Figure 41. Release latches and server

9. The cable-management arm can be installed on either side of the server. The following figure shows it being installed on the left side. To install the cable-management arm on the right side, follow the instructions and install the hardware on the opposite side. Connect one end of the support arm (1) to the same slide rail to which you plan to attach the cable-management arm so that you can swing the other end of the support arm (2) toward the rack.



Rack Rear

Figure 42. Support arm connection

P8HA1812-0

10. Connect the other end of the support arm to the cable-management stop bracket (1). Turn the bracket (2) to secure it to the support arm.

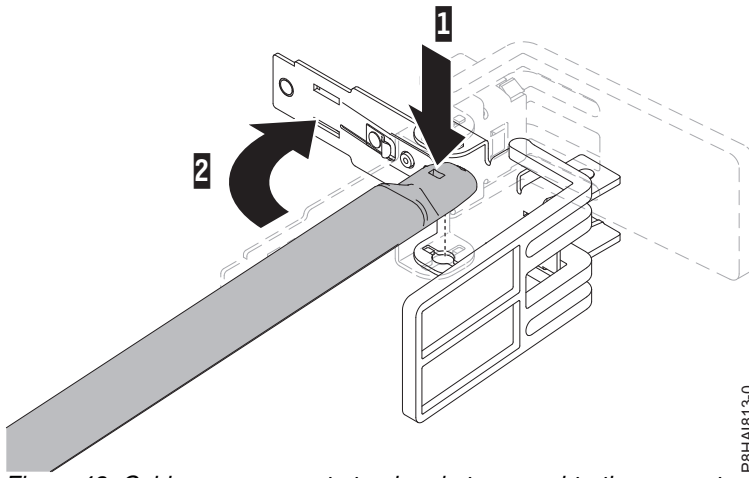


Figure 43. Cable-management stop bracket secured to the support arm

P8HA1813-0

11. The capital letters **I** and **O** are printed on cable management arm pins to identify the inside and outside pins. Install the cable management stop bracket (with capital letter **O**) on the unattached end of the support arm. Ensure that the support arm is securely installed.

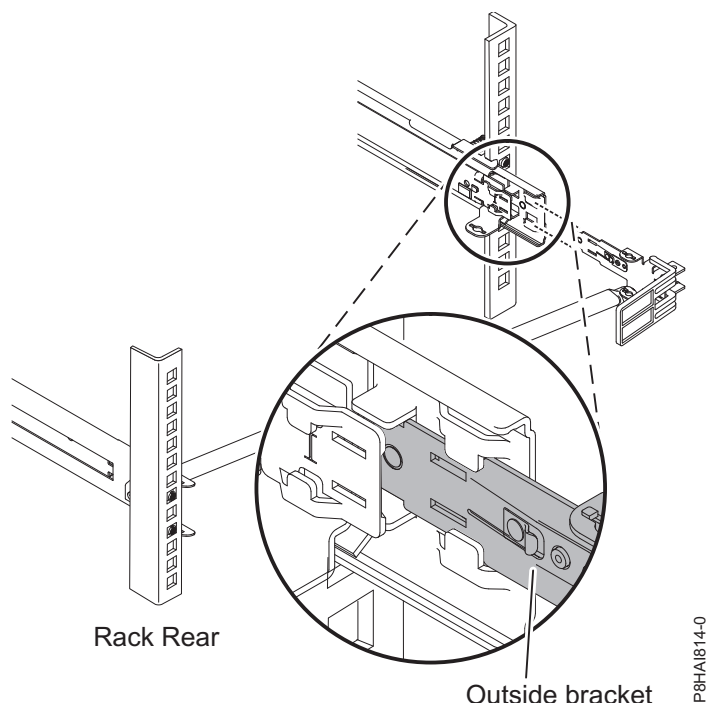


Figure 44. Connecting the stop bracket to the slide rail

12. Place the cable-management arm on the support arm. Pull out both the inside and the outside pins of the cable management arm and then slide the cable management arm tabs into both the inside and the outside slots of the slide rail. Push the tabs until they snap into places.

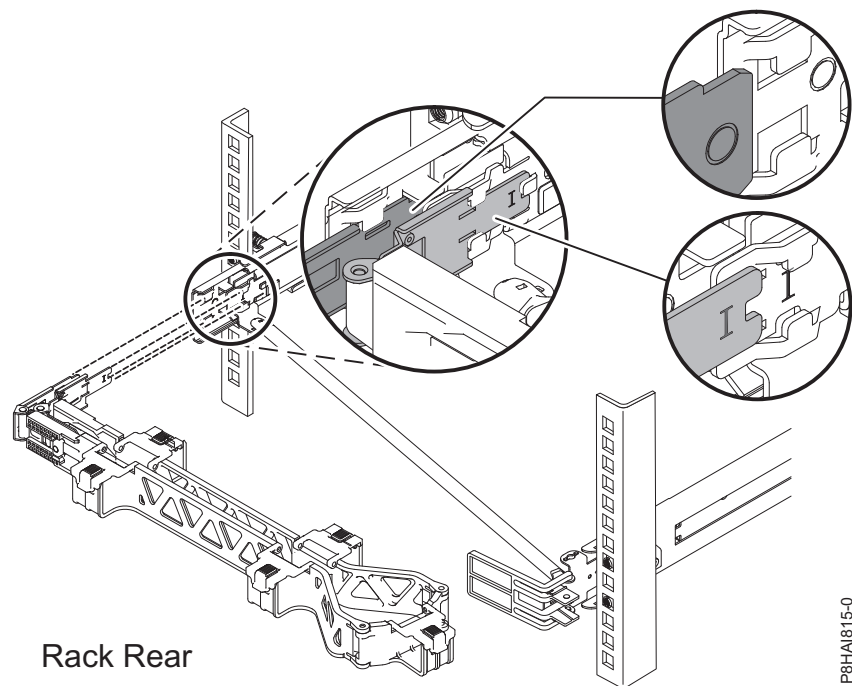
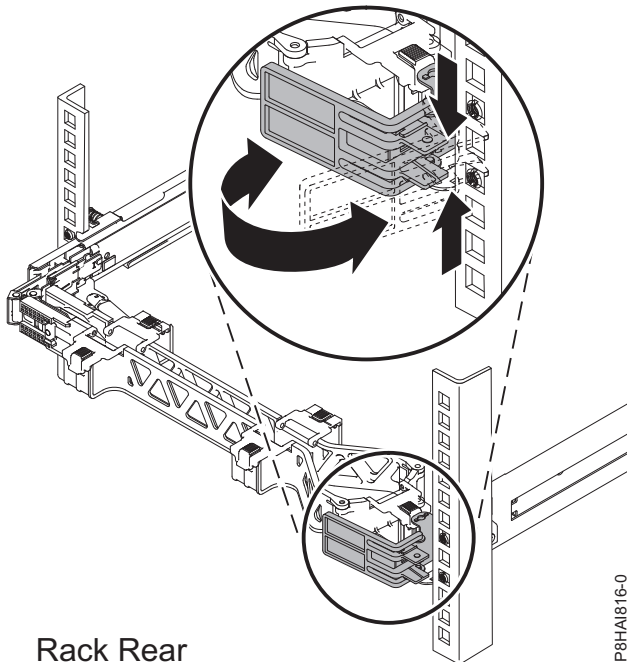


Figure 45. Cable-management arm connection

13. To make it easier to rotate the cable management arm on and off the cable management support arm, you can open the stop bracket by pushing the tabs above and below the stop bracket for closing it.

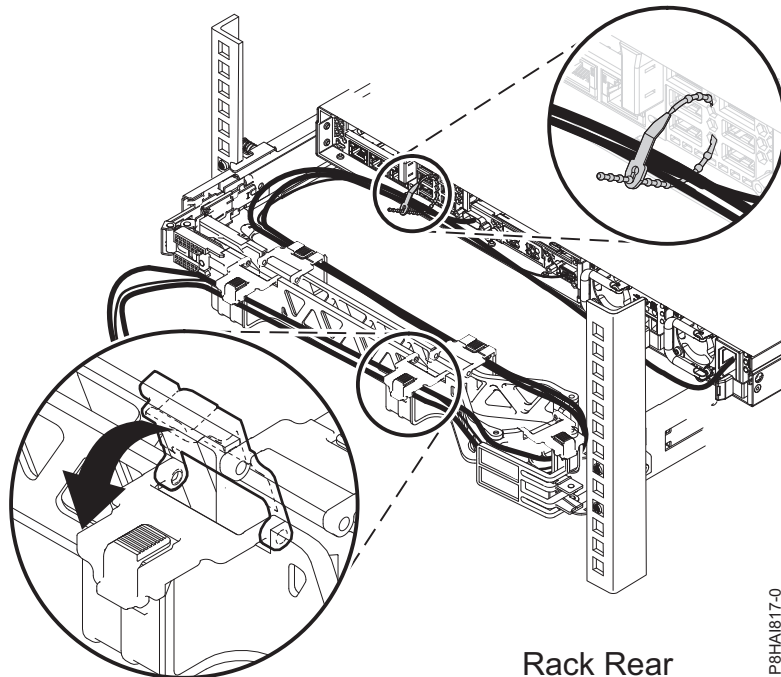


Rack Rear

Figure 46. Cable management support stop bracket

14. Attach the power cords and other cables to the rear of the server (including keyboard, monitor, and mouse cables, if required). Route the cables and power cords on the cable-management arm and secure them with cable ties or hook-and-loop fasteners.

Note: The location of the cable straps might be slightly different in different systems. Use the cable straps that are provided on the rear of the system to retain the cables and prevent them from sagging.



Rack Rear

Figure 47. Power cord attachment and cable routing

15. Cables must be bundled with a hook-and-loop fastener for proper movement of the cable management arm.

Note: Ensure that the cables do not sag below the U space so they do not get caught on the lower systems. Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.

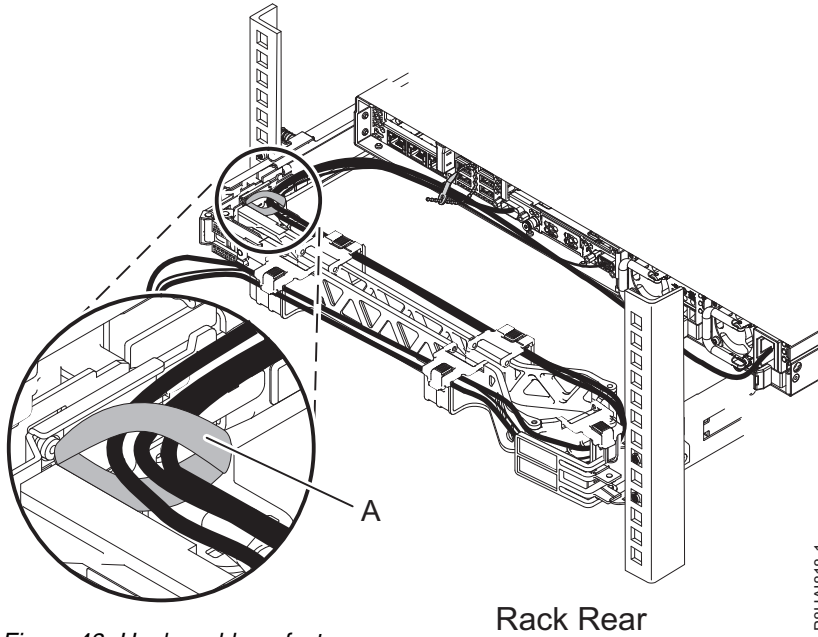
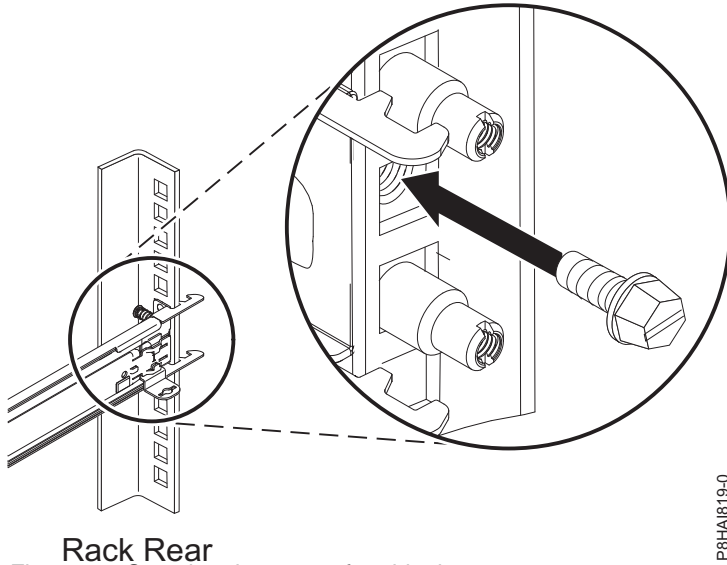


Figure 48. Hook-and-loop fastener

16. If you are shipping the rack with the system installed or if you are in a vibration-prone area, insert the M6 screws to the rear of the slides. Use a cable tie to secure the free end of the cable management arm to the rack if needed.



Rack Rear
Figure 49. Securing the server for shipping

Installing the 7042-CR9 HMC into a rack

Learn how to install the 7042-CR9 Hardware Management Console (HMC) into a rack.

Complete a parts inventory. The following illustrations show the items that you need to install the server in the rack cabinet. If any items are missing or damaged, contact your place of purchase.

Cable Management Arm box contents

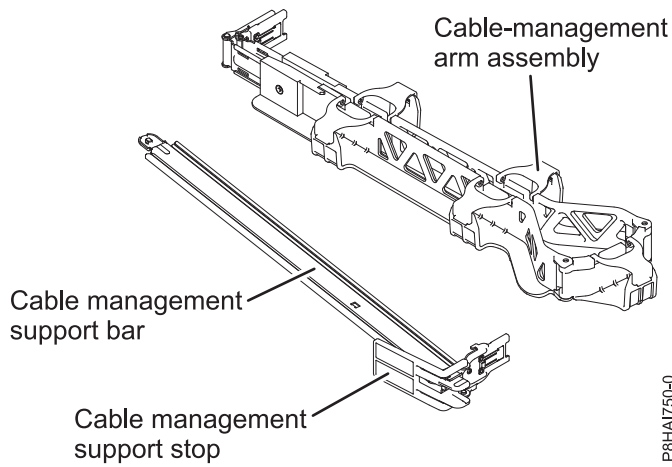


Figure 50. Cable management arm box contents

Rail box contents

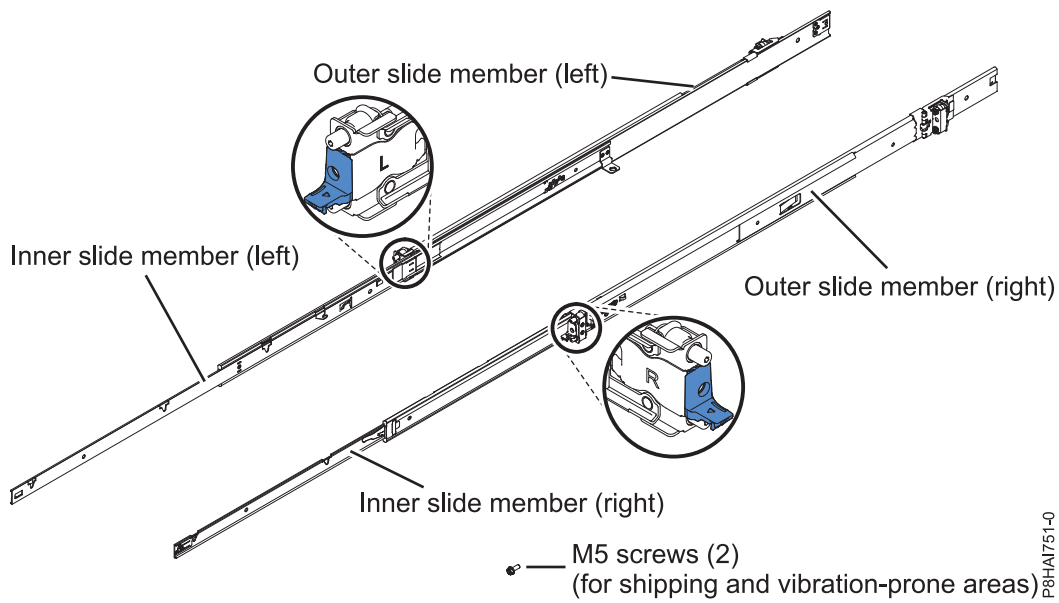


Figure 51. Rail box contents

Note: You need both the slide rail box and the cable management arm box for this installation.

To install a 7042-CR9 HMC into a rack, complete the following steps:

1. Select an available space (depending on the server you are installing) in your rack to install your server.

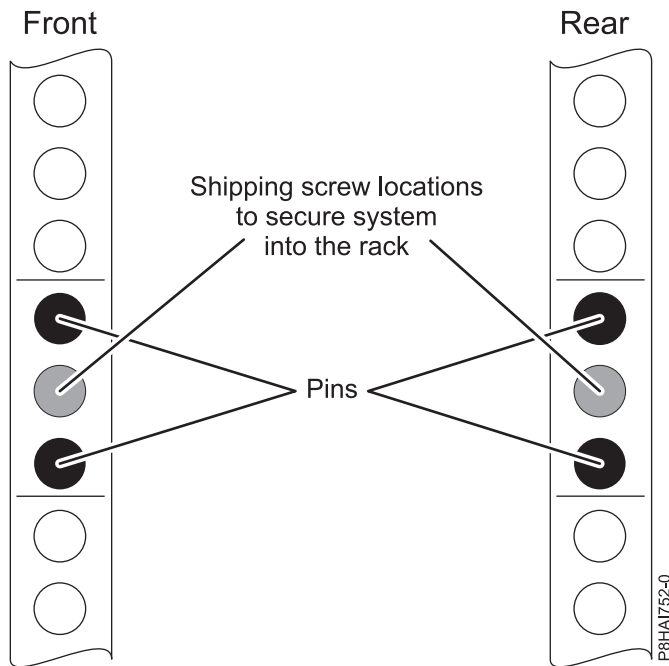


Figure 52. Identifying a rack space

Note: You need 1 unit (1 U) of space and the slide rails are installed in the bottom unit (U) of the 1 unit of space.

2. Extend the outer slide member all the way back until you hear an audible click. The rear rack mount bracket is now rotated into the unlocked position.

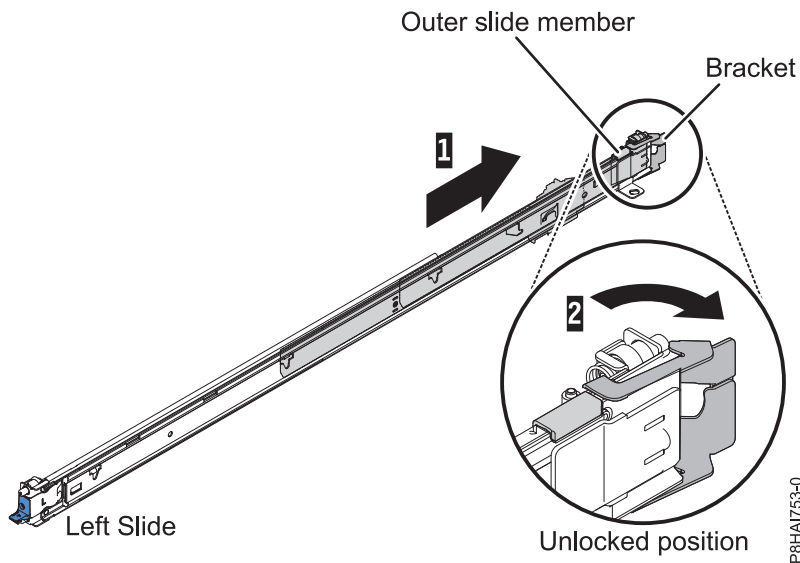


Figure 53. Slide rail and the outer slide member

Note: Each slide rail is marked as **R (right)** or **L (left)** on its end.

3. Align the rear end of the outer slide member against the holes on the rear of the rack. Line up the pins and push the slide in so that the pins go into the holes. The two slide pins protrude through the top and bottom holes on the EIA flange. Push the slide towards the rear of the rack until the rear rack mount bracket locks into place.

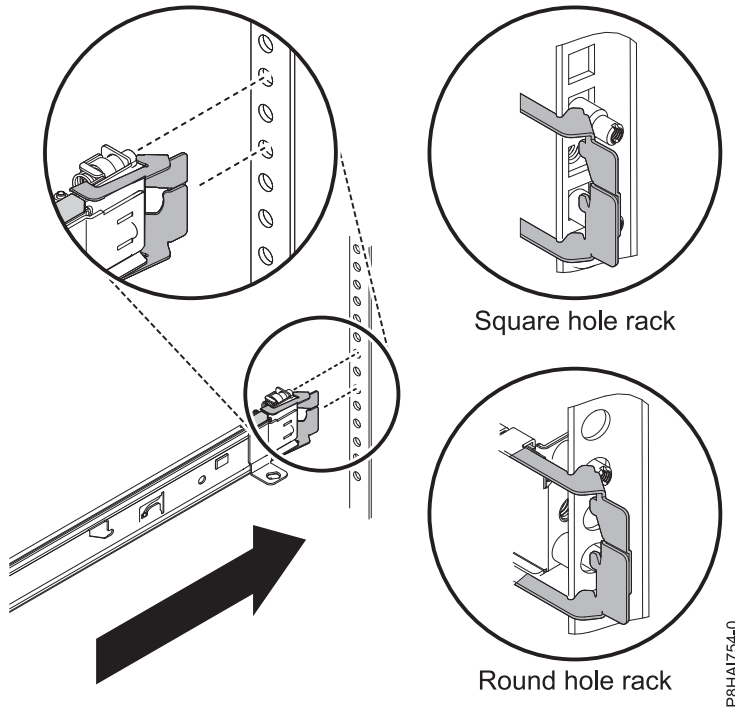


Figure 54. Align the pins with the holes in the rear of the rack

P8HAI754-0

4. Rotate the front latch to the open position and align the front end of the outer slide member against the holes on the front of the rack. Line up the pins with holes in the EIA flanges and pull the slide forward so that the pins protrude through the holes. Lock the front of the slide by allowing the front latch to rotate to the closed position. Repeat steps 2- 4 for the other outer slide member.

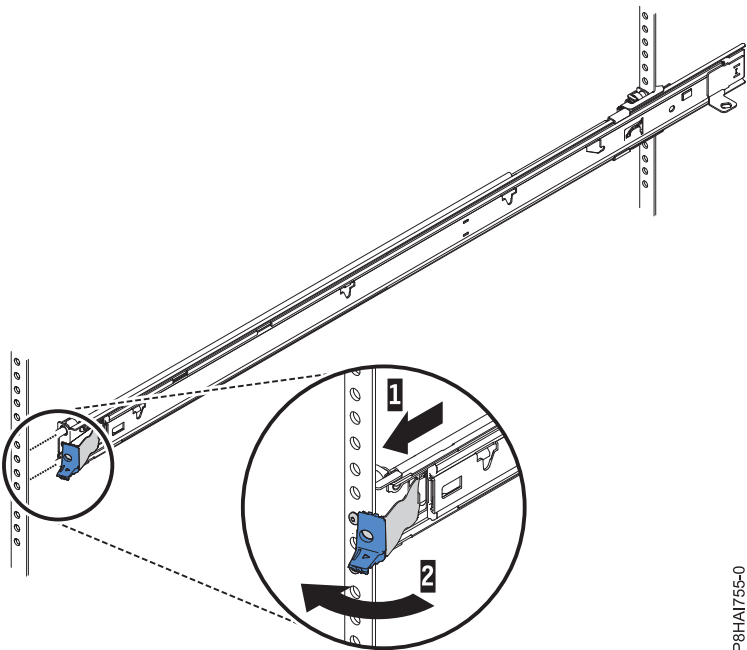


Figure 55. Front slide rail latch

P8HAI755-0

5. Press on the release latches (1). When you move the rack cabinet, or if you install the rack cabinet in a vibration-prone area, tighten the captive M5 screws (2) in the front of the server.

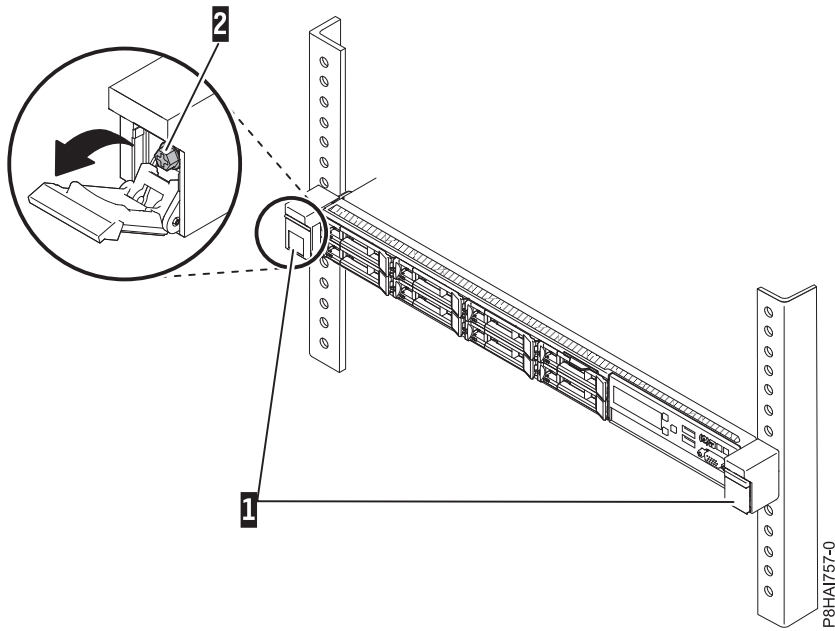


Figure 56. Rack front rail and pins

6. Pull the slide rails forward (1) until they click, twice, into place. Carefully lift the server and tilt it into position over the slide rails so that the rear rail heads (2) on the server line up with the slots in the slide rails. Lower the server down until the rear rail heads slide into the two rear slots, and then slowly lower the front of the server (3) until the other rail heads go into the other slots on the slide rails. Ensure that the front latch covers the front rail head so that the system is secured to the slide rails.

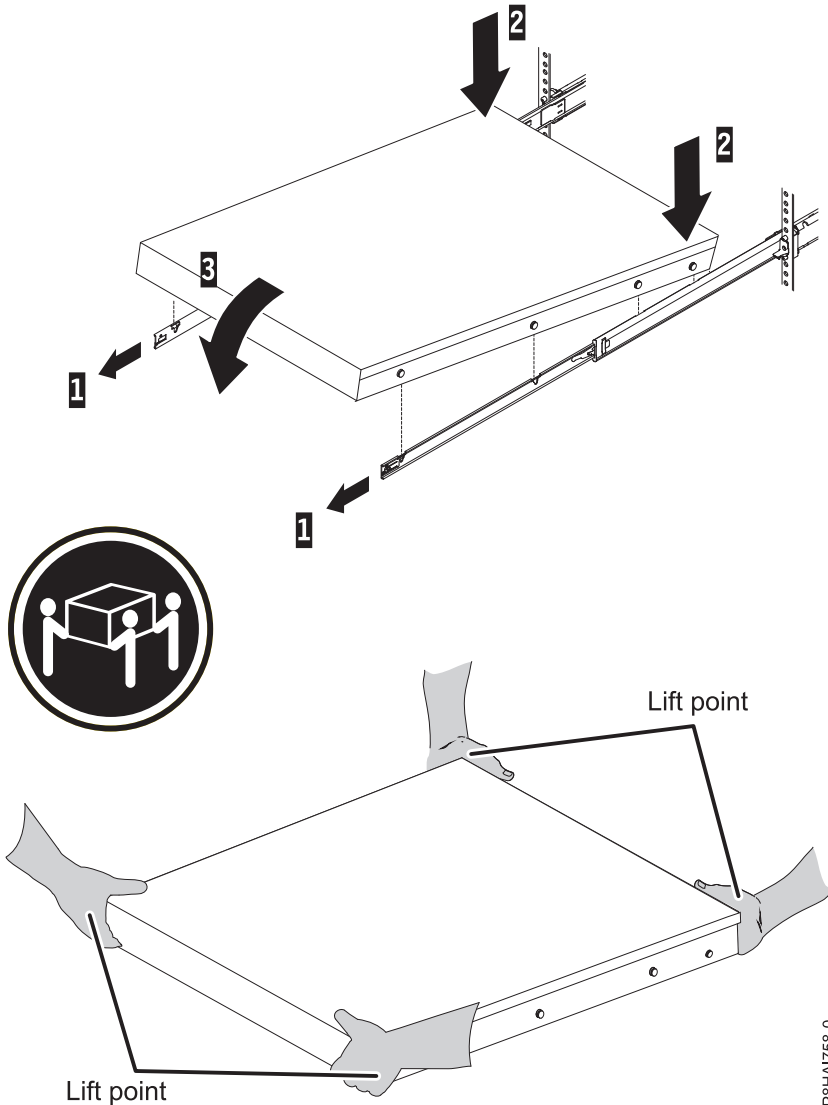


Figure 57. Slide rails extended, server nail heads aligned with slots in rail, and lift points

Note: Use safe practices while lifting. If you are installing a 1 U server, ensure that you have two people when you lift the server. Their hands must be positioned as illustrated in Figure 57.

7. Lift the locking levers (1) on the slide rails and push the server (2) all the way into the rack until it clicks into place.

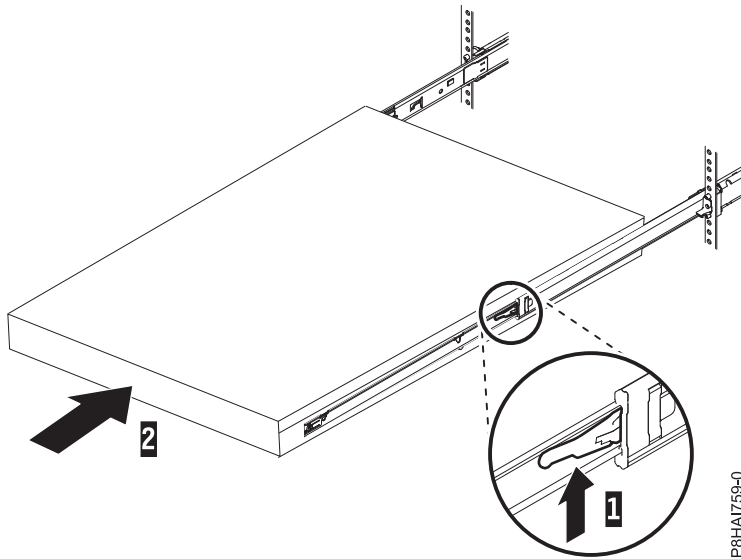


Figure 58. Release latches and server

8. The cable-management arm can be installed on either side of the server. Figure 59 shows it being installed on the left side. It is best to install the cable-management arm so that it hinges on the side opposite to the power supplies to provide access to the power supplies. To install the cable-management arm on the right side, follow the instructions and install the hardware on the opposite side. Place the pin down (1) into the horizontal slot on the rear of the slide rails. Then rotate the other end of the bar toward the rack (2) toward the rack.

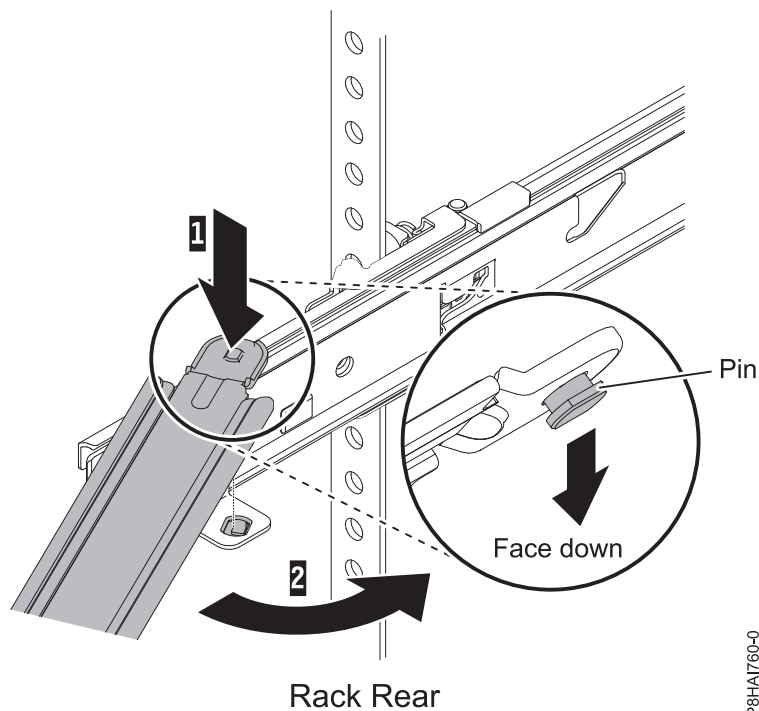


Figure 59. Support arm connection

Note: The cable management support bar must be on top of the slide tab to work correctly.

9. Install the cable management stop bracket (with capital letter O) on the unattached end of the support arm. Ensure that the support arm is securely installed.

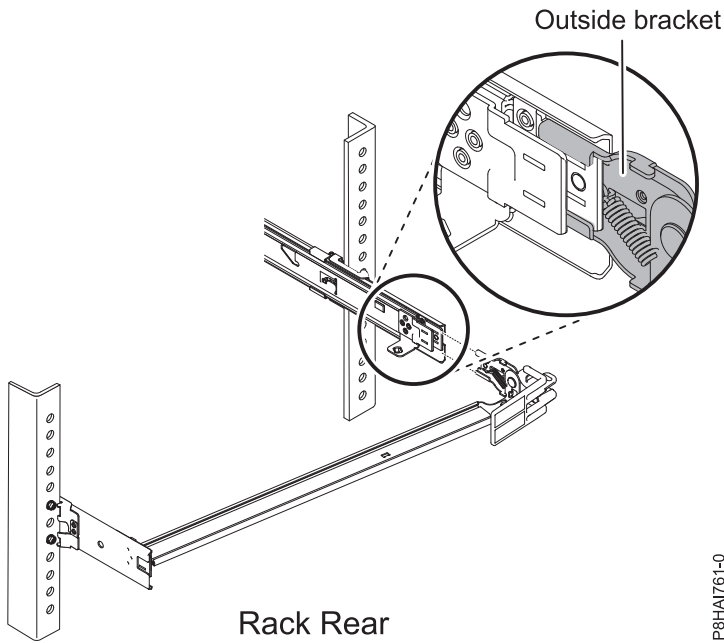


Figure 60. Connecting the stop bracket to the slide rail

P8HA1761-0

Note: The capital letter **O** is marked on cable management arm pins to identify the outside pins.

10. Place the cable-management arm on the support arm. Slide the cable management arm tabs into both the inside and the outside slots of the slide rail. Push the tabs until they snap into place.

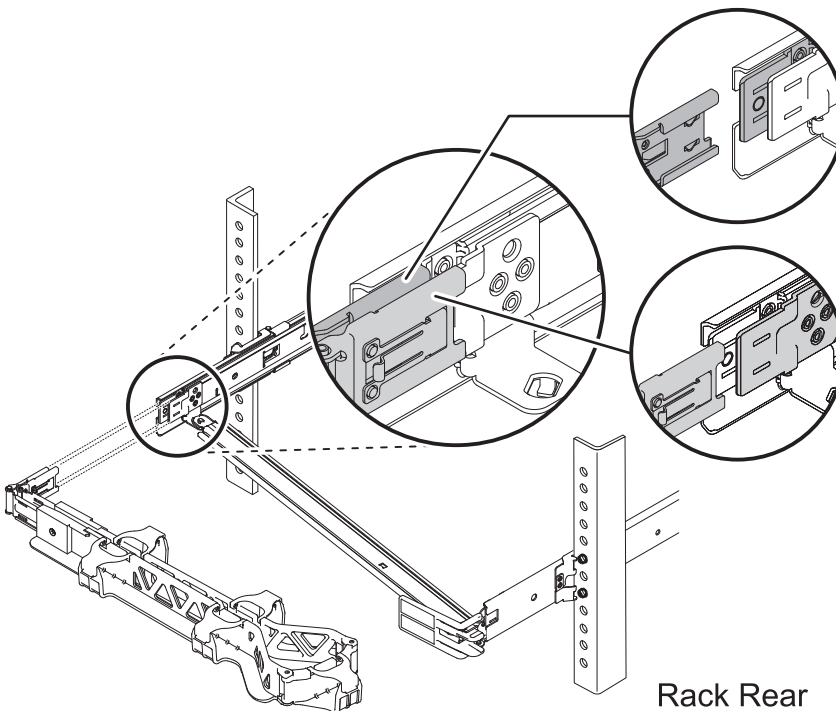
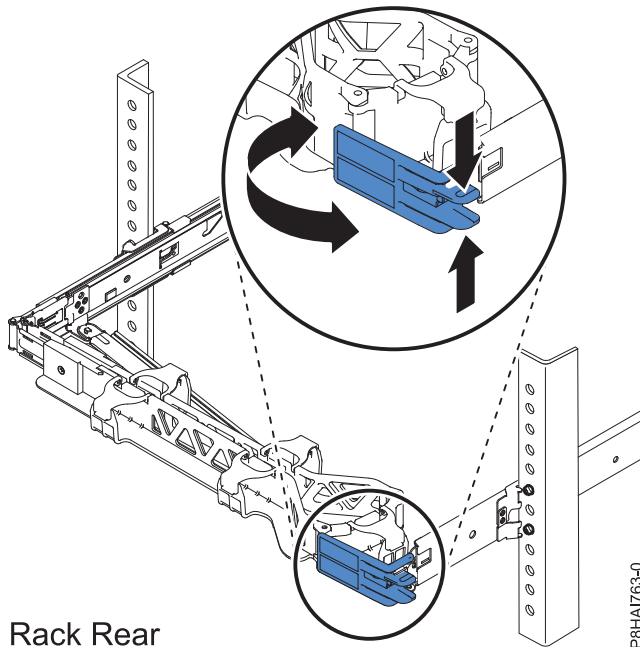


Figure 61. Cable-management arm connection

P8HA1762-0

11. To make it easier to rotate the cable management arm on and off the cable management support arm, you can open the stop bracket by pushing the tabs above and below the cable management support.

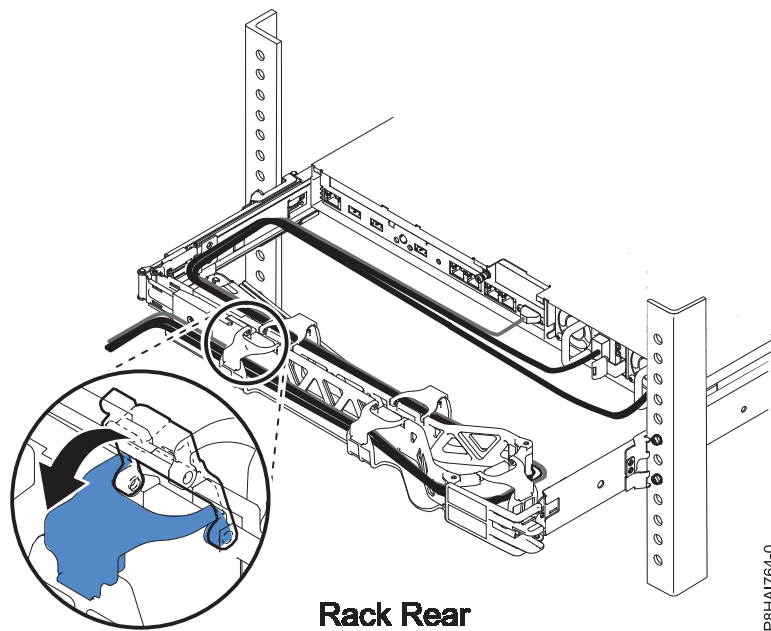


Rack Rear

Figure 62. Cable management support stop bracket

12. Attach the power cords and other cables to the rear of the server (including keyboard, monitor, and mouse cables, if required). Route the cables and power cords on the cable-management arm and secure them with cable ties or hook-and-loop fasteners.

Note: The location of the cable straps might be slightly different in different systems. Use the cable straps that are provided on the rear of the system to retain the cables and prevent them from sagging.



Rack Rear

Figure 63. Attaching the Power cord and routing the cable

13. Cables must be bundled with the cable strap for proper movement of the cable management arm.

Note: Ensure that the cables do not sag below the U space so they do not get caught on the lower systems. Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.

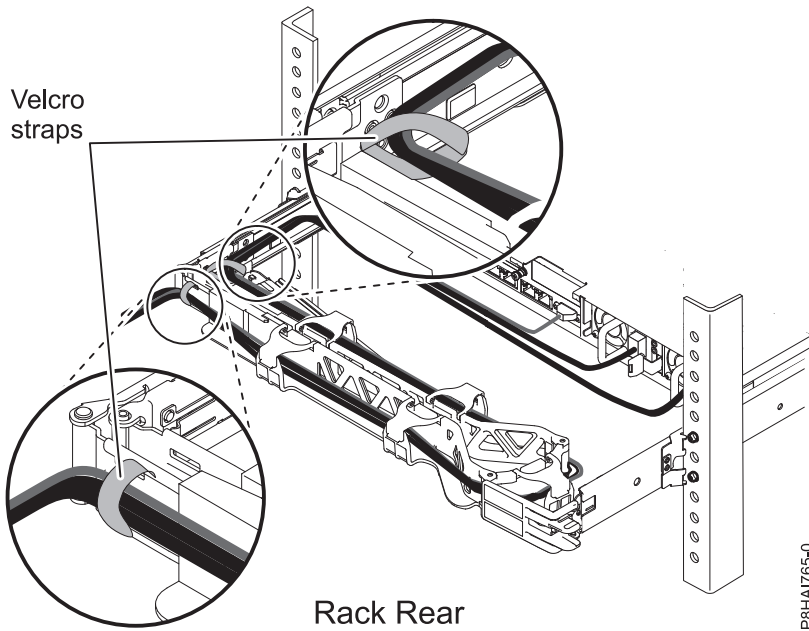


Figure 64. Hook-and-loop fastener

14. If you are shipping the rack with the system installed or if you are in a vibration-prone area, insert the M5 screws into the rear of the slides. Use a cable tie to secure the free end of the cable management arm to the rack if needed.

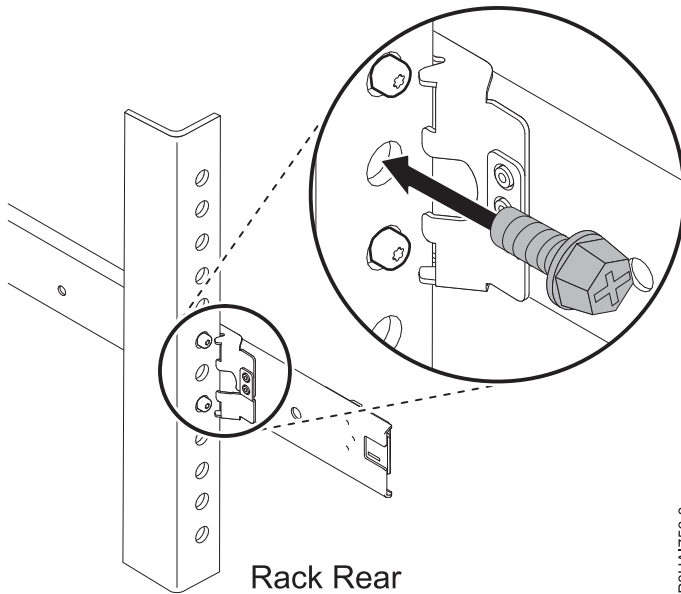


Figure 65. Securing the server for shipping

Installing the 7063-CR1 into a rack

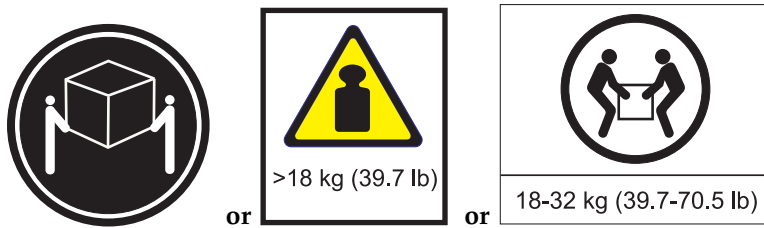
Learn how to install the 7063-CR1 Hardware Management Console (HMC) into a rack.

You can view the online installation documentation, or you can print the PDF version of the same information. To view or print the PDF version, see [Installing and configuring the Hardware Management Console](#).

Prerequisites for installing the rack-mounted 7063-CR1 system

Use the information to understand the prerequisites that are required for installing the system.

CAUTION:



The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

You might need to read the following documents before you install the server:

- The latest version of this document is maintained online, see *Installing the 7063-CR1 into a rack* (http://www.ibm.com/support/knowledgecenter/POWER8/p8hai/p8hai_install7063_kickoff.htm).
- To plan your server installation, see *Planning for the system* (http://www.ibm.com/support/knowledgecenter/POWER8/p8had/p8had_8xx_kickoff.htm).

Ensure that you have the following items before starting your installation:

- Size 2 Phillips screwdriver
- Flat-head screwdriver
- Box cutter
- Electrostatic discharge (ESD) wrist strap
- Rack with one Electronic Industries Association (EIA) unit (1U) of space.

Note: If you do not have a rack that is installed, install the rack. For instructions, see *Racks and rack features* (http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/p8hbf_8xx_kickoff.htm).

Completing inventory for your system

Use this information to complete inventory for your system.

1. Verify that you received all the boxes you ordered.
2. Unpack the server components as needed.
3. Complete a parts inventory and verify that you have received all the parts that you ordered before you install each server component.

Note:

Your order information is included with your product. You can also obtain order information from your marketing representative or the IBM Business Partner.

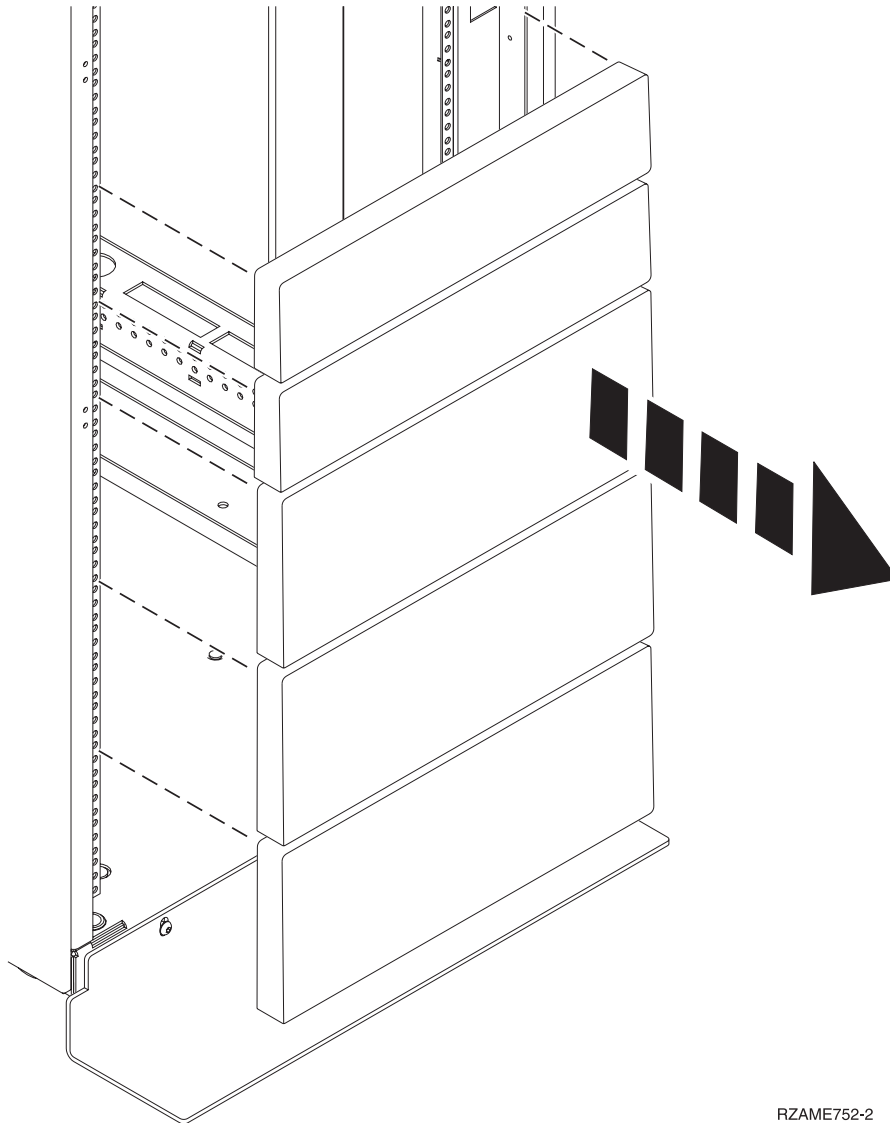
If you have incorrect, missing, or damaged parts, consult any of the following resources:

- Your IBM reseller.
- IBM Rochester manufacturing automated information line at 1-800-300-8751 (United States only).
- The Directory of worldwide contacts website <http://www.ibm.com/planetwide>. Select your location to view the service and support contact information.

Determining and marking the location in the rack for the 7063-CR1 system

You might need to determine where to install the system unit into the rack.

1. Read the Rack safety notices (<http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/racksafety.htm>).
2. Determine where to place the system unit in the rack. As you plan for installing the system unit in a rack, consider the following information:
 - Organize larger and heavier units into the lower part of the rack.
 - Plan to install units into the lower part of the rack first.
 - Record the Electronic Industries Alliance (EIA) locations in your plan.
3. If necessary, remove the filler panels to allow access to the inside of the rack enclosure where you plan to place the unit, as shown in Figure 66.



RZAME752-2

Figure 66. Removing the filler panels

4. Determine to place the system in the rack. Record the EIA location.
5. Facing the front of the rack and working from the right side, use tape, a marker, or pencil to mark the lower hole of each EIA unit.
6. Repeat step 5 for the corresponding holes located on the left side of the rack.
7. Go to the rear of the rack.

8. On the right side, find the EIA unit that corresponds to the bottom EIA unit marked on the front of the rack.
9. Mark the bottom EIA unit.
10. Mark the corresponding holes on the left side of the rack.

Attaching the rails to the rack

You must install the rails into the rack. Use this procedure to perform this task.

Note: The system requires 1 EIA rack unit (1U) of space.

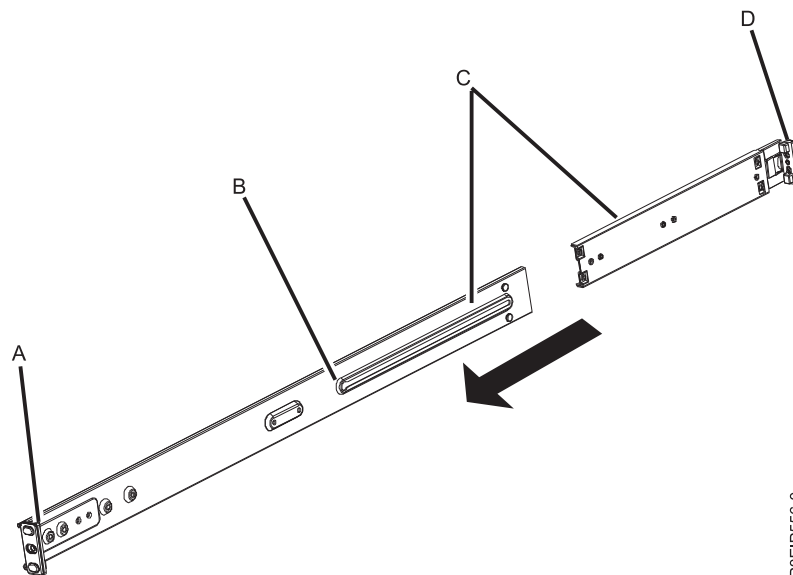
Ensure that you have the necessary parts to install the rails. The following parts are included with the rail kit:

- Slide rail rack screws and washers, used to secure the rails to the rack
- Rails
- Round Pin Adapters, 4x

1. Remove the rail pieces from the packaging and put them on a work surface.

Attention: To avoid rail failure and potential danger to yourself and to the unit, ensure that you have the correct rails and fittings for your rack. If your rack has round support flange holes, square support flange holes or screw-thread support flange holes, ensure that the rails and fittings match the support flange holes that are used on your rack. Do not install mismatched hardware by using washers or spacers. If you do not have the correct rails and fittings for your rack, contact your IBM reseller.

2. If applicable, replace the rail rack square pins (A) and (D) with the rail rack round pins.
3. Connect the two parts of each rack slide rail. To connect the two parts of the rack slide rail, perform the following tasks:
 - a. Identify the two pieces of the right rack slide rail. Align the short and long pieces (C). Ensure that the rack rail pins are pointing in the same direction (A) and (D).



P8EIP556-0

Note: The rails are identical. This graphic shows the rail that will be installed on the right side of the rack.

- b. The shorter piece of the rack slide rail has a metal pin. Insert the pin into the hole in the longer piece of the rack slide rail (B). Slide the shorter piece of the rack rail into the longer piece of the rack rail.
- c. Repeat these steps for the left slide rail.

4. Install the rack slide rails into the rack.
 - a. Move to the front of the rack.
 - b. Select the right rack slide rail, and locate the EIA unit that you previously marked. Ensure that you are holding the front end of the rack slide rail.

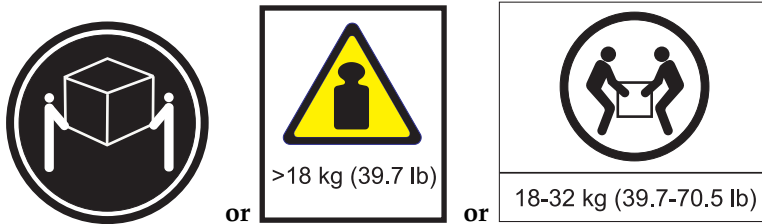
Note: The right rail pins face out, toward the right of the rack.

- c. Extend the rail from the front of the rack to the back of the rack and align the rack slide rail pins with the holes in the rack flange that you previously marked.
 - d. Push the rack rail pins into the rear rack flange until the rear rack rail latch clicks into place.
 - e. Pull the front of the rack rail toward the front of the rack rail flange. Align the slide rail pins with the holes in the rail flange and pull them until the rail latch clicks into place.
 - f. Repeat steps 4a - 4f for the left slide rail.
5. Secure the rails to the rack.
 - a. Move to the rear of the rack.
 - b. Slide each washer onto to each of the longer screws that is included with the rail kit.
 - c. Screw a screw and washer through the middle hole of each rail on each side of the rear of the rack.

Installing the system into the rack and connecting and routing power cables

Install the system onto the rails and connect and route power cables.

CAUTION:



The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

1. Remove the protective plastic film from the top of the system chassis.
2. Move to the front of the rack.
3. Using two people, one on each side of the system, lift the system and align the system chassis rails on each side of the chassis with the rack slide rails.
4. Gently push the system toward the rear of the rack.
5. Secure the system to the rack by screwing a screw through the handles on each side of the system chassis.
6. Plug the power cords into the power supplies.

Note: Do not connect the other end of the power cord to the power source now.

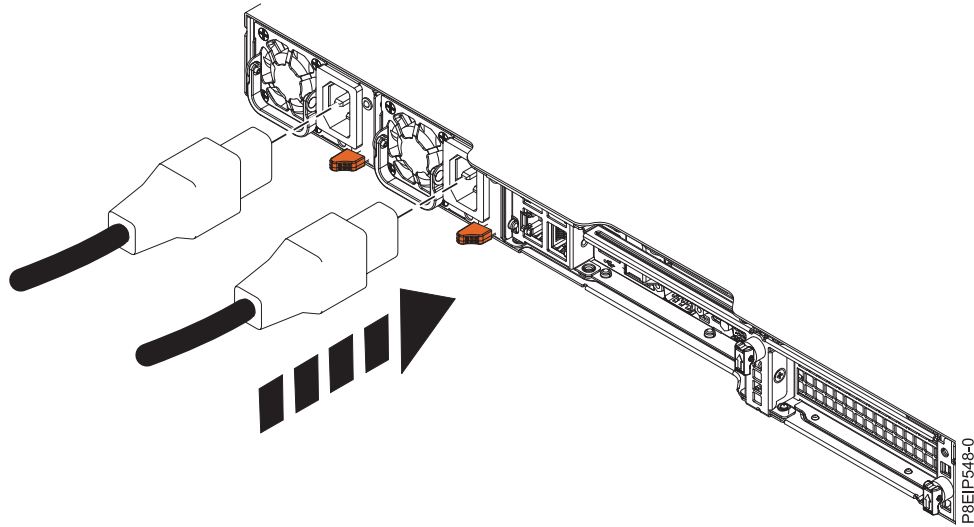


Figure 67. Plugging the power cords into the power supplies

7. Continue with “Cabling the rack-mounted 7063-CR1 HMC.”

Cabling the rack-mounted 7063-CR1 HMC

Learn how to physically install your rack-mounted Hardware Management Console (HMC).

1. Ensure that the HMC is installed into a rack and the power cords are plugged into the power supplies. For more information, see “Installing the system into the rack and connecting and routing power cables” on page 46. After you install the HMC into a rack, continue with the next step.
2. Connect the keyboard, monitor, and mouse.

Note: The system has two front USB ports that you can use. The front serial port is non-functional.

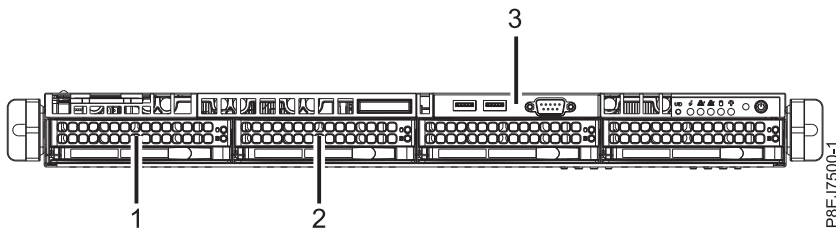


Figure 68. Front view

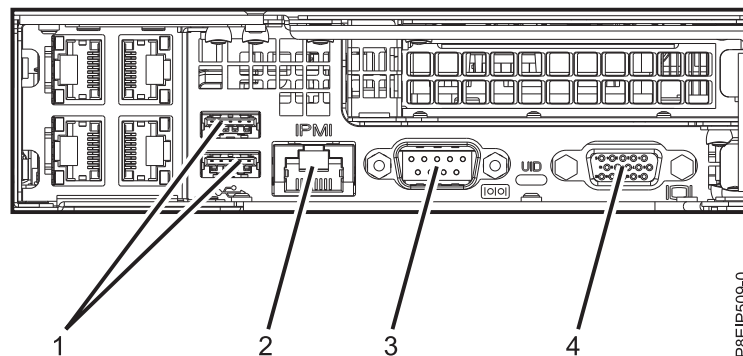


Figure 69. Rear ports

Table 9. Input and output ports

Identifier	Description
1	USB 2.0 used for keyboard and mouse
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Serial IPMI
4	Video Graphics Array (VGA) used for monitor. Only the 1024 x 768 at 60 Hz VGA setting is supported. Only up to a 3-meter cable is supported.

3. Connect the Ethernet cable that is intended for the connection to the managed system or systems.

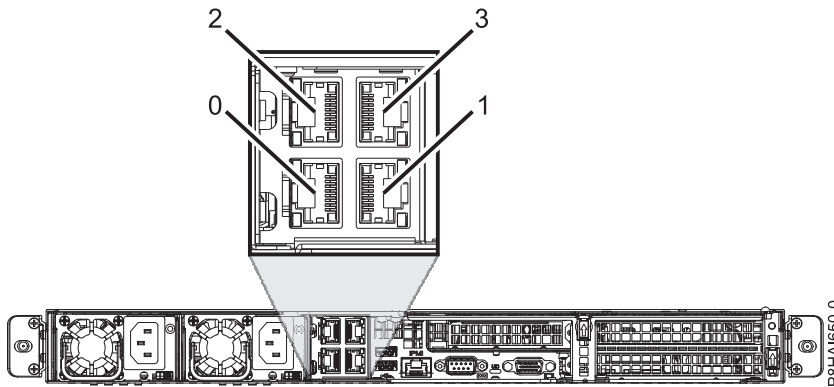


Figure 70. Ethernet ports

Note: To learn more about the HMC network connections, see “HMC network connections” on page 72.

4. If your managed system is already installed, you can verify that the Ethernet cable connection is active by observing the green status lights at both the HMC and managed system Ethernet ports as your installation progresses.
5. Connect the Ethernet Intelligent Platform Management Interface (IPMI) port to a network.

Note: This connection is required to access the baseboard management controller (BMC) on the HMC. Access to the BMC is required for service tasks and to maintain the HMC firmware. For more information, see “Types of HMC network connections” on page 72.

6. Plug the system power cords and the power cords for any other attached devices into the alternating current (AC) power source.
7. Verify the power status by using the power supply LEDs as indicators. For more information, see LEDs on the 7063-CR1 system.

Next, you need to install and configure your HMC software. Continue with “Configuring the 7063-CR1 HMC.”

Configuring the 7063-CR1 HMC

Learn how to install and configure the Hardware Management Console (HMC).

You can download the HMC version that you want from the Fix Central website. Use removable media (such as a DVD or USB) to create a bootable ISO file from the HMC package (ISO image).

Note: The following table describes the predefined (default) login information for the HMC and BMC interfaces.

Table 10.

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

Note: The following installations are shown as examples.

Installing the HMC by using USB flash drive

To install the HMC by using USB flash drive, complete the following steps for Linux systems:

1. Download the HMC version that you want from the Fix Central website.
2. Run the following command: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (where **sdx** is the name of the USB drive).

Note: The USB drive must be at least 4 GB. Certain USB drives might be too wide to fit properly into the USB port at the rear of the system. Test the fit of your USB drive before you proceed.

3. Insert the USB drive, and power on the system.
4. When the Petitboot menu is displayed, select the **Install Hardware Management Console** option that is located under **USB**.

Installing the HMC by using remote media from the console viewer

To install the HMC by using remote media from the console viewer, complete the following steps:

1. Log in to the BMC web interface (<http://<bmc-ip>>).
2. Select **Remote Control**.
3. Select **Console Redirection**.
4. Click **Launch Console**.
5. In the Java™ iKVM Viewer, select **Virtual Media > Virtual Storage**.
6. Under **Logical Drive Type**, select **ISO File**.
7. Click **Open Image** and locate the ISO file on your system.
8. Press **Plugin** to mount the ISO file.
9. Power on the system.
10. When the Petitboot menu is displayed, select the **Install Hardware Management Console** option that is located under **CD/DVD**.

Installing the HMC by using an external USB attached DVD drive

To install the HMC by using an external USB attached DVD drive, complete the following steps:

1. Download the HMC recovery version that you want from the Fix Central website.
2. Burn the HMC recovery DVD image to a DVD-R media as an image. Alternatively, you can order the recovery media on DVD.
3. Power off the HMC.
4. Connect the external USB DVD drive to the HMC and insert the HMC recovery DVD.

Note: You might need to connect the USB DVD drive to an external power source or use a USB Y cable to connect to an extra USB port to provide sufficient power to the DVD drive.

5. Power on the HMC.

Note: The display monitor might show no signal during startup. The process might take 2 or 3 minutes before the display monitor shows any status.

6. When the Petitboot bootloader starts, navigate to stop the automatic boot.

Note: A 10-second timeout is enforced. If no action is taken within 10 seconds, the system attempts to boot from the hard disk drive.

7. Wait until the **CD/DVD** device appears in the Petitboot menu.

Note: This process can take up to a minute.

8. Select the **Install Hardware Management Console** option that is located under **CD/DVD**.

Installing the HMC by using remote media that is hosted by an SMB file server

To install the HMC by using remote media that is hosted by a Server Message Block (SMB) file server, complete the following steps:

1. Copy the recovery ISO file to a share host on your SMB-compliant file server.

Note: Server Message Block version 3 (SMBv3) is not supported.

2. Log in to the BMC web interface (<http://<bmc-ip>>).
3. Select **Virtual Media**.
4. Select **CD-ROM Image**.
5. Complete the following information:

Share host

The IP of the SMB host. If you are using the host name, ensure that the domain name system (DNS) on the BMC is correctly configured.

Path to image

The SMB path to the system. For example: `/<share name>/<rest of path>/<name of iso>.iso`

User (optional)

The user name that is used to log in to the SMB host.

Password (optional)

The password for the user.

6. Click **Save**.
7. Click **Mount**.
8. Device 1 now shows the following message: **There is an iso file mounted**.

Note: If the message does not appear, recheck the information and repeat steps 6 - 8.

9. Power on the system.
10. When the Petitboot menu is displayed, select the **Install Hardware Management Console** option that is located under **CD/DVD**.

Next, you need to configure your HMC software. For instructions, see “Configuring the HMC by using the HMC Enhanced+ interface” on page 117.

Related concepts:

“Configure BMC connectivity” on page 142

You can configure or view the network settings on the BMC for the management console.

Installing the HMC virtual appliance

Learn how to install the Hardware Management Console (HMC) virtual appliance.

The HMC virtual appliance can be installed in your existing x86 or POWER® virtualized infrastructure. The HMC virtual appliance supports the following x86 virtualization hypervisors:

- Kernel-based virtual machine (KVM)
- Xen
- VMware

The HMC virtual appliance supports the following POWER virtualization hypervisors:

- PowerVM®

Minimum requirements for running the HMC virtual appliance:

- 16 GB of memory
- 4 virtual processors
- 2 network interfaces (maximum of 4 allowed)
- 1 disk drive that contains 500 GB of available disk space

Note:

PowerVM virtualization hypervisor requires 160 GB of disk space (500 GB recommended). Multipath I/O (MPIO) disks are not supported.

The minimum PowerVM processor requirement is 1.0 processing units and four shared virtual processors in capped sharing mode. 16 GB of memory recommended.

Notes:

1. The processor on the systems that host the HMC virtual appliance must be either an Intel VT-x or an AMD-V hardware virtualization-enabled processor.
2. The HMC virtual appliance DVDs that you receive are not bootable. You must mount the media first and then copy the .tgz file from the media. The method to mount the DVD can vary depending on the operating system that you use.
3. The command syntax that are used in the following examples can vary depending on the operating system that you use.

Related information:

HMC V8 network installation images and installation instructions

Installing the HMC virtual appliance on x86

Learn how to install the Hardware Management Console (HMC) virtual appliance on a x86 environment.

Installing the HMC virtual appliance by using the KVM hypervisor:

Learn how to install the Hardware Management Console (HMC) virtual appliance by using the kernel-based virtual machine (KVM) hypervisor.

To install the HMC virtual appliance on KVM, complete the following steps:

Note: The following use the command line interface and require root user authority. The command syntax might vary depending on the operating system.

1. Verify that virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) version 7.0 or later.
2. Download the <KVM vHMC installation filename>.tar.gz file to the host system.
3. Run the following command: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Run the following command: `cd /var/lib/libvirt/images/vHMC`.
5. To extract the virtual disk images, run the following command: `tar -zxvf <KVM vHMC installation filename>.tgz`

Note: In this command, specify the full path of your HMC virtual appliance .tar file.

6. A **domain.xml** file is provided in the <KVM vHMC installation filename>.tar.gz file. Complete the following steps:
 - a. Edit the **domain.xml** file and verify that the path to your disks is correct. This file contains the string **DISK_PATH**.
 - b. Make sure **virtio** is used in the bus value for your disk device.
 - c. You can choose to have a different name for your VM. The default name in the **domain.xml** file is **vHMC**.
 - d. Verify that the media access control (MAC) address is set in the **domain.xml** file. This file contains the string **MAC_ADDRESS**.

Note: Remove this line if you want a MAC address to be generated automatically for you.
 - e. Verify that your bridges match your Ethernet devices. The default **domain.xml** file specifies one Ethernet.
 - f. If you are using the Activation Engine, replace **AEDISK** with the name of Activation Engine virtual disk image. Otherwise, remove the disk element.
7. To define the VM, run the following command: `virsh define <domain>.xml`.
8. To verify that Virtual HMC was added to the list of defined VMs, run the following command: `virsh list --all`.
9. To start the VM, run the following command: `virsh start vHMC`.
10. To determine the Virtual Network Computing (VNC) display number of your console, run the following command: `virsh vncdisplay vHMC`.
11. To connect to your console with a VNC viewer, run the following command: `vncviewer HOSTNAME:ID`(Where ID is the display number, for example 0).

Note: If you require remote access, you must drop or configure your firewall to allow access to port 5900.

Installing the HMC virtual appliance by using the Xen hypervisor:

Learn how to install the Hardware Management Console (HMC) virtual appliance by using the Xen hypervisor.

The HMC virtual appliance supports Xen version 4.2 or later.

To install the HMC virtual appliance by using the Xen hypervisor, complete the following steps:

Note: The following steps use the command line interface and requires root user authority. The command syntax might vary depending on the operating system.

1. Verify that virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) version 6.4 or later.
2. Download the <XEN vHMC installation filename>.tar.gz file to the host system.
3. Run the following command: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Run the following command: `cd /var/lib/libvirt/images/vHMC`.
5. To extract the virtual disk images, run the following command: `tar -zxvf <XEN vHMC installation filename>.tgz`

Note: In this command, specify the full path of your HMC virtual appliance .tar file.

6. A **vhmc.cfg** file is provided in the <XEN vHMC installation filename>.tar.gz file. Open the **vhmc.cfg** file in a text editor and edit the following values:
 - a. Change the name of the virtual HMC (optional): Edit the **vhmc.cfg** file and verify that the path to your disks is correct. This file contains the string **DISK_PATH**.
 - b. Replace **DISK_PATH** with the path for disk1.img:

```
disk = [ 'file:DISKPATH,hda,w' ]
```
 - c. Replace **ethernet adapter** and add MAC address (optional):

```
vif = [ 'type=virtio, model=e1000, bridge=eth0' ]
```

Optional MAC Address:

```
vif = [ 'type=virtio, mac=MACADDRESS, model=e1000, bridge=eth0' ]
```

Note: When the Virtual HMC is rebooted, the Xen hypervisor automatically regenerates a MAC address. Adding the optional MAC Address solves this issue.
 - d. Replace **FLOPPYPATH** (if you are using the Activation Engine):

```
device_model_args = [ "-fda", "FLOPPYPATH" ]
```
7. To create and start the VM, run the following command: `xl create vHMC.cfg`.
8. To check that the VM was added to the list of defined virtual machines, run the following command: `xl list`.
9. To access the VM local console, run the following command: `vncviewer localhost 0`.

Installing the HMC virtual appliance by using VMware ESXi:

Learn how to install the Hardware Management Console (HMC) virtual appliance by using VMware ESXi.

You can install the HMC virtual appliance on VMware ESXi by using the graphical user interface on the vSphere client to deploy the Open Virtualization Format (OVF) template.

Note: You can install the HMC virtual appliance on VMware ESXi version 6.0 or later.

To install the HMC virtual appliance on VMware ESXi by using the vSphere client, complete the following steps:

Note: The command syntax might vary depending on the operating system.

1. Obtain the Tar archive file: <VMware vHMC installation file name>.tgz.
2. Use the `tar` command to extract the OVA file from the Tar archive file.
3. Start the vSphere client and log in to the ESXi host.
4. From the **File** menu, select **Deploy OVF template**.

5. Click **Browse** and select the OVA file.
6. Click **Next**.
7. After the deployment is completed, click **Close** and select the HMC virtual appliance icon to power the HMC virtual appliance on.

Installing the HMC virtual appliance on POWER

Learn how to install the Hardware Management Console (HMC) virtual appliance on a virtualized POWER environment.

Installing the HMC virtual appliance on PowerVM (logical partition):

Learn how to install the Hardware Management Console (HMC) virtual appliance on a PowerVM environment.

The HMC virtual appliance supports POWER8 servers on firmware level FW830 or later. For more information, see Supported Linux distributions for POWER8 Linux on Power systems (<https://www.ibm.com/support/knowledgecenter/en/linuxonibm/laam/laamdistros.htm>).

Note: You cannot manage the server that hosts the HMC virtual appliance.

Create automated HMC installation image (optional)

You can create an automated HMC installation image that automatically installs the HMC virtual appliance without prompting for the **HMC Installallation** wizard.

Note: The HMC virtual appliance on PowerVM does not provide graphics adapter support for adapters that are assigned to the partition. You can use a supported web browser to connect to the HMC for user interface support.

To create an automated HMC installation image, complete the following steps:

1. Create two directories by running the following commands: `mkdir -p oldiso` and `mkdir -p newiso`.
2. Mount the HMC installation image to the **oldiso** directory by running the following command: `sudo mount -o loop <image_path> oldiso`.
3. Copy the contents of the **oldiso** directory to the **newiso** directory by running the following command: `cp -r oldiso/* newiso`.
4. Edit the Grub file for the automated install by running the following command: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Make the Grub file read-only by running the following command: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Create a new HMC installation ISO by running the following command: `mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso (where ISO label must be HMC-<hmc version release number>, for example HMC-8.0.870.0)`.

Note: For more information about setting up the Activation Engine and the configuration file, see “Using the Activation Engine for the HMC virtual appliance” on page 57.

Logical volume setup

To set up the logical volume, complete the following steps:

1. Select a managed system.
2. From the menu pod, select **System Actions > Power VM > Virtual Storage**.
3. Select **Manage System VIOS > Action > Manage Virtual Storage**.

4. Select the **Virtual Disks** tab.
5. Click **Create virtual disk** and enter the following information:
 - **Virtual disk name:** The name of the virtual disk.
 - **Storage pool name:** The name of the storage pool.
 - **Virtual disk size:** The size of the virtual disk.
 - **Assigned partition:** The name of the logical partition.

Note: A minimum of 160 GB disk space is required (500 GB disk space is recommended).

Installation media setup - create media library

To create a media library, complete the following steps:

1. Select a managed system.
2. From the menu pod, select **System Actions > Power VM > Virtual Storage**.
3. Select **Manage System VIOS > Action > Manage Virtual Storage**.
4. Select the **Optical Devices** tab.
5. Click **Create Library** and enter the following information:
 - **Storage pool:** The name of the storage pool.
 - **Media library size:** The size of the media library.
6. Click **OK**.

Installation media setup - upload media to VIOS

To upload media to Virtual I/O Server (VIOS), complete the following steps:

1. Log in to VIOS.
2. In VIOS root mode, run the following command: `oem_setup_env`.
3. To allow NFS connection, run the following command: `nfso -o nfs_use_reserved_ports=1`.
4. To mount the NFS into the local VIOS folder, run the following command: `mount <server_ip>:/Mountpoint <local_folder>`.
5. To verify that the NFS mount includes your HMC installation ISO and Activation Engine configuration image (optional), run the following command: `ls`.

Installation media setup - link media to media library

To link media to the media library, complete the following steps:

1. Navigate back to **Manage System VIOS > Action > Manage Virtual Storage** and select the **Optical Devices** tab.
2. From the **Virtual Optical Media** section, select **Add Media** from the **Actions** menu.
3. From the **Add Virtual Media** window, select **Add existing file from VIOS filesystem** and enter the following information:
 - **Media name:** The name of the media (for example, HMCInstall or AEDrive).
 - **Optical media file name:** The file name of the installation ISO file (for example, 01234567-ppc64ie.iso).
4. Click **OK**.
5. If you created an Activation Engine configuration image, repeat steps 3 - 4 to add the Activation Engine configuration image. Otherwise, continue to step 6.
6. Verify that the optical media is uploaded to the media library by verifying that the media name is shown in available **Virtual Optical Media** list.

Logical partition setup

To set up the logical partition, complete the following steps:

1. Select a managed system.
2. From the menu pod, select **System Actions > Partitions > Partitions**.
3. Click **Create Partition** and enter the following information:
 - **Partition Name:** The name of the partition.
 - **Partition ID:** The ID of the partition.
 - **Partition Type:** Select the operating system (**AIX/Linux** or **IBM i**).
4. Click **OK**.
5. Allocate the number of processors and the amount of memory for the partition.

Note: A minimum of four virtual processors and 8 GB of memory is required.
6. From the menu pod, select **Partition Actions > Virtual I/O > Virtual Networks**.
7. Click **Manage Network Connections** and select the virtual networks for the partition.

Note: A maximum of four virtual network adapters is allowed.

8. From the menu pod, select **Partition Actions > Virtual I/O > Virtual Storage**.
9. From the **Virtual Optical Device** tab, click **Add Virtual Optical Device**.
10. Enter the **Device Name** (for example, HMCInstall or AEDrive) and select the wanted Virtual I/O Server from the table.

Note: Installing the AEDrive is optional.

11. Click **OK**.
12. Verify that the virtual optical devices that you added from step 10 is now listed in the table.
13. From the **Action** menu, click **Load**.
14. Select the media file to assign to the logical partition and click **OK**.
15. Verify that the virtual optical devices that you loaded from step 13 is now listed in the table.

Starting the HMC virtual appliance

Note: When you install the HMC virtual appliance on a partition by using the HMC ISO image file, you will not have local graphical console access to the web user interface.

To start the HMC virtual appliance on PowerVM, complete the following steps:

1. Select the managed partition.
2. Open an active connection to the logical partition by selecting **Actions > Console > Open Terminal Window**.
3. Activate the logical partition by selecting **Actions > Activate**.
4. Select **Activate (Normal)** and **Current Configuration**.
5. Click **Finish**.
6. Switch to the terminal window.
7. From the **Boot** menu, select **1 = SMS Menu**.
8. From the **Main** menu, select **5 = Select Boot Options**.
9. From the **Multiboot** menu, select **1 = Select Install/Boot Device**.
10. From the **Select Device Type** menu, select **5 = List all devices**.
11. Select the HMCInstall device based on the device location.
12. Select **2. Normal Mode Boot**.

13. Select **1. Yes** to confirm.
14. Follow the onscreen instructions from the **HMC Install** wizard.

Note: Skip this step if you used an automated HMC installation image.

15. After the installation completes and the system starts, you must select a language from the **language selection** dialog box.
16. Accept the license agreement.

Note: Ensure that the command controller is ready to accept commands before you run any commands. For example, running the **lshmc -V** command until it succeeds.

17. Log in as hscroot and use the **chhmc** command to configure the network.

The following example shows the sequence of **chhmc** commands that can be used to configure the network and enable Secure Shell (SSH) and remote web access on the HMC.

```
chhmc -c network -s modify -i ethX -a <hmc ip address> -nm <hmc network mask> --lparcomm on
chhmc -c network -s modify -h <hmc hostname> -d <hmc domain name> -g <gateway ip>
chhmc -c network -s add -ns <name server> -ds <domain search>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <ip address>
chhmc -c SecureRemoteAccess.name -s add -a <ip address>
chhmc -c remotewebui -s enable -i ethX
hmcshutdown -r -t now
```

- **ethX** is the network interface name to configure.
- **hmc ip address** is the IP address of your HMC.
- **hmc network mask** is the network mask of your HMC.
- **hmc hostname** is the host name of your HMC.
- **hmc domain name** is the domain name of your HMC.
- **gateway ip** is the IP address of the gateway on your network.
- **name server** is the name server address of your network.
- **domain search** is the names of the domains that you want the HMC to search on.
- To allow access on all IP addresses, use **-a 0.0.0.0 -nm 0** in place of **ip address**.

Note: When you use multiple virtual Ethernet adapters, run the command **cat /etc/sysconfig/network-scripts/ifcfg-ethX** on the HMC virtual appliance on each interface. Compare the media access control (MAC) address against what the HMC shows in the adapter view of the virtual network of the partition. You can click **View Virtual Ethernet Adapter Settings** for more information on the virtual Ethernet adapters. This step helps you determine the correct interface to use.

18. Restart the system.

Using the Activation Engine for the HMC virtual appliance

Learn how to use the Activation Engine for the Hardware Management Console (HMC) virtual appliance.

Activation Engine is a framework that allows various components within a virtual machine to be configured during system startup. To use the Activation Engine, you need to set up an XML configuration profile to allow the HMC virtual appliance to be in a ready-to-manage state on first start. For more information about configuring the XML configuration profile, see “Setting up the configuration profile for the Activation Engine” on page 58. The configuration file can be used to configure the following options:

- Set Default Keyboard (US)
- Default Locale (US)
- Disable Keyboard Setup
- Disable Display Setup
- License Agreement and Machine Code Agreement

- Disable Setup Wizard
- Disable Call Home Wizard
- Configure up to four Network Interface Cards
- Configure Firewall Settings for each Interface
- Configure Network interface as IPv4 DHCP Server
- Configure Private and Open Interface
- Configure Default Gateway Interface Device

Note: The number of Ethernet adapters that is defined in the **vHMC-Conf.xml** configuration file must correlate with the defined Network adapters in the **domain.xml**, **vHMC.cfg**, or **VMWare** configuration file.

The Activation Engine requires a virtual disk that holds an XML configuration. You can edit the **user_data** file with a text editor and use the XML configuration guide that is shown in the following example.

To create a virtual ISO disk image with Activation Engine configuration in a Linux environment, complete the following steps:

1. Create a directory:

```
mkdir -p config-drive/openstack/latest
```
2. Copy the edited **user_data** file into the directory:

```
cp user_data config-drive/openstack/latest
```
3. Create a virtual disk image with the Activation Engine configuration:

```
mkisofs -R -V config-2 -o AEdrive.iso config-drive
```

Setting up the configuration profile for the Activation Engine:

Learn how to set up the Activation Engine configuration file by using XML tags.

Configuration file

Use the following example of the configuration file to learn about the XML tags.

```
<vHMC-Configuration>
  <ConfigurationVersion>2.0</ConfigurationVersion>
  <LicenseAgreement></LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
  <SetupDisplay>No</SetupDisplay>
  <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
    <Hostname></Hostname>
    <Domain></Domain>
    <DNSServers></DNSServers>
    <IPV4Config>
      <NetworkType></NetworkType>
      <IPAddress></IPAddress>
      <Netmask></Netmask>
      <Gateway></Gateway>
    </IPV4Config>
    <IPV6Config>
      <NetworkType></NetworkType>
      <IPAddress></IPAddress>
      <Gateway></Gateway>
    </IPV6Config>
  </Firewall>
</vHMC-Configuration>
```

```

    <PEGASUS>Enabled</PEGASUS>
    <RPD>Enabled</RPD>
    <FCS>Enabled</FCS>
    <I5250>Enabled</I5250>
    <PING>Enabled</PING>
    <L2TP>Disabled</L2TP>
    <SLP>Enabled</SLP>
    <RSCT>Enabled</RSCT>
    <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
    <SSH>Enabled</SSH>
    <NTP>Disabled</NTP>
    <SNMPTraps>Disabled</SNMPTraps>
    <SNMPAgents>Disabled</SNMPAgents>
  </Firewall>
</Ethernet>
<NTPServers>
  <ntpparam ntpserver="" ntpversion=""/>
</NTPServers>
</vHMC-Configuration>

```

XML tags for the configuration file

XML tags are used in the Activation Engine configuration file to set specific values for various attributes. You can manually set these values in the Activation Engine configuration file. Use the following table to see a description of each tag and its allowed values:

Table 11. XML tags

Tags	Description	Acceptable values	Notes
ConfigurationVersion	Required element that defines the configuration version to use.	2.0	
LicenseAgreement	Required element that displays the HMC virtual appliance license agreement.		
AcceptLicense	Required element to accept the HMC virtual appliance license agreement.	<ul style="list-style-type: none"> Yes: Accepts the HMC license agreement. No: Prompts User to Accept HMC License Agreement 	If an invalid value is entered, the Activation Engine uses the default setting of No .
Locale	Required element to define locale settings.	en_US.UTF-8	If an invalid value is entered, the Activation Engine uses the default setting of US .
SetupWizard	Required element to enable or disable the HMC Setup wizard.	<ul style="list-style-type: none"> Yes: Displays the HMC Setup wizard. No: Disables the HMC Setup wizard display. 	If an invalid value is entered, the Activation Engine uses the default setting of Yes .
SetupCallHomeWizard	Required element to enable or disable the HMC Call Home wizard.	<ul style="list-style-type: none"> Yes: Displays the HMC Call Home wizard. No: Disables the HMC Call Home wizard display. 	If an invalid value is entered, the Activation Engine uses the default setting of Yes .

Table 11. XML tags (continued)

Tags	Description	Acceptable values	Notes
SetupKeyboard	Required element to define the keyboard configuration.	<ul style="list-style-type: none"> • Yes: Prompts the user for keyboard configuration. • No: Accepts default keyboard configuration (US). 	If an invalid value is entered, the Activation Engine uses the default setting of Yes .
SetupDisplay	Required element to enable or disable the display configuration.	<ul style="list-style-type: none"> • Yes: Prompts the user for display configuration. • No: Accepts default display configuration. 	If an invalid value is entered, the Activation Engine uses the default setting of Yes .
Ethernet	Required element that holds values for Ethernet adapter configurations. A maximum of four Ethernet adapters can be configured.	<p>Enable:</p> <ul style="list-style-type: none"> • Yes: Configure this adapter. • No: Do not configure this adapter. <p>DefaultGatewayDevice:</p> <ul style="list-style-type: none"> • Yes: Configure this adapter as the main network adapter. • No: Do not configure this adapter as the main network adapter. <p>PrivateInterface:</p> <ul style="list-style-type: none"> • Yes: Configure this adapter as a private interface. Yes is required to configure interface as an IPv4 DHCP Server. • No: Do not configure this adapter as a private interface. No is required to configure interface as IPv4 static type. 	The Activation Engine runs the default configuration if any invalid values are entered within the Ethernet adapter section or if multiple Default Gateway Devices are defined. Optional elements can be omitted from the configuration. At least one IPv4 or IPv6 configuration is required. If you do not specify an IP configuration, the Activation Engine uses the default configuration.
HostName	Optional element to define the network host name.	Any valid host name string.	If the element is not defined, the Activation Engine uses the default local host HostName value.
Domain	Optional element to define the network domain.	Any valid domain value (for example, example.us.com).	If the element is not defined, the Activation Engine uses the default empty Domain value.

Table 11. XML tags (continued)

Tags	Description	Acceptable values	Notes
DNSServers	Optional element to define the network DNS servers.	<p>It is acceptable to have one DNS Server value or up to three valid IPv4 or IPv6 addresses that are separated by a comma.</p> <ul style="list-style-type: none"> • Example 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • Example 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • Example 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844,::ffff:903:201 	If the element is not defined, the Activation Engine uses the default empty DNSServers value.
IP4Config	Optional element to define IPv4 configuration settings.	<p>IPType: Required element to define IPv4 configuration type.</p> <ul style="list-style-type: none"> • Static: Configure this adapter by using static configuration. • DHCP: Configure this adapter by using DHCP configuration. • DHCPServer: Configure this adapter to be IPv4 DHCP server (requires PrivateInterface to be set to Yes). <p>IPAddress: Optional element that is required only if Static or DHCPServer configuration is selected.</p> <ul style="list-style-type: none"> • Static Configuration: Any valid IPv4 address value. • DHCPServer Configuration: Any DHCP server IP within the IP range. <p>Netmask: Optional element that is required only if Static configuration is selected.</p> <ul style="list-style-type: none"> • Any valid IPv4 netmask value. <p>Gateway: Optional element that is required only if Static configuration is selected.</p> <ul style="list-style-type: none"> • Any valid IPv4 netmask value. 	

Table 11. XML tags (continued)

Tags	Description	Acceptable values	Notes
IP6Config	Optional element to define IPv6 configuration settings.	<p>IPType: Required element to define IPv6 configuration type.</p> <ul style="list-style-type: none"> • Static: Configure this adapter by using static configuration. • DHCP: Configure this adapter by using DHCP configuration. <p>IPAddress: It is acceptable to have long or short form IPv6 format and long or short form IPv6 prefix.</p> <ul style="list-style-type: none"> • Example 1: IPv6: 2001:4860:4860:0000:0000:0000:8888 • Example 2: IPv6: 2001:4860:4860::8888 • Example 3: IPv6: 2001:4860:4860::8888/128 <p>If no prefix is specified, the Activation Engine uses the default setting of /64 prefix.</p> <p>Gateway:</p> <ul style="list-style-type: none"> • Any valid IPv6 address value. 	

Table 11. XML tags (continued)

Tags	Description	Acceptable values	Notes
Firewall	Optional element to define firewall settings.	<p>PEGASUS:</p> <ul style="list-style-type: none"> • Enabled: Allows the PEGASUS ports to be open. • Disabled: Disables PEGASUS ports. <p>RPD:</p> <ul style="list-style-type: none"> • Enabled: Allows the RMC ports to be open. • Disabled: Disables RMC ports. <p>FCS:</p> <ul style="list-style-type: none"> • Enabled: Allows the FCS ports to be open. • Disabled: Disables FCS ports. <p>I5250:</p> <ul style="list-style-type: none"> • Enabled: Allows the 5250 ports to be open. • Disabled: Disables 5250 ports. <p>PING:</p> <ul style="list-style-type: none"> • Enabled: Allows the Ping port to be open. • Disabled: Disables Ping port. <p>L2TP:</p> <ul style="list-style-type: none"> • Enabled: Allows the L2TP ports to be open. • Disabled: Disables L2TP ports. <p>SLP:</p> <ul style="list-style-type: none"> • Enabled: Allows the SLP ports to be open. • Disabled: Disables SLP ports. <p>RSCT:</p> <ul style="list-style-type: none"> • Enabled: Allows the RSCT ports to be open. • Disabled: Disables RSCT ports. <p>SECUREREMOTEACCESS:</p> <ul style="list-style-type: none"> • Enabled: Allows the secure remote access ports to be open. • Disabled: Disables secure remote access ports. <p>SSH:</p> <ul style="list-style-type: none"> • Enabled: Allows the SSH port to be open. • Disabled: Disables SSH port. 	

Table 11. XML tags (continued)

Tags	Description	Acceptable values	Notes
Firewall	Optional element to define firewall settings.	<p>NTP:</p> <ul style="list-style-type: none"> • Enabled: Allows the NTP ports to be open. • Disabled: Disables NTP ports. <p>SNMPTraps:</p> <ul style="list-style-type: none"> • Enabled: Allows the SNMP traps ports to be open. • Disabled: Disables SNMP traps ports. <p>SNMPAgents:</p> <ul style="list-style-type: none"> • Enabled: Allows the SNMP agents ports to be open. • Disabled: Disables SNMP agents ports. 	
NTPServers	The NTPServers tag is needed if you want to configure up to five NTP servers within a HMC virtual appliance.	<p>NTPServers: Accepts <ntpparam ntpserver="server" ntpversion="version"/></p> <p>ntpparam:</p> <ul style="list-style-type: none"> • ntpserver: Accepts any valid IPv4 or IPv6 values and valid host names. • ntpversion: Accepts 1-4 numeric value <p>Example:</p> <pre><NTPServers> <ntpparam ntpserver= "test.austin.ibm.com" ntpversion="2"/> <ntpparam ntpserver="192.168.34.1" ntpversion="4"/> <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>` </NTPServers></pre>	

Installing the monitor and keyboard

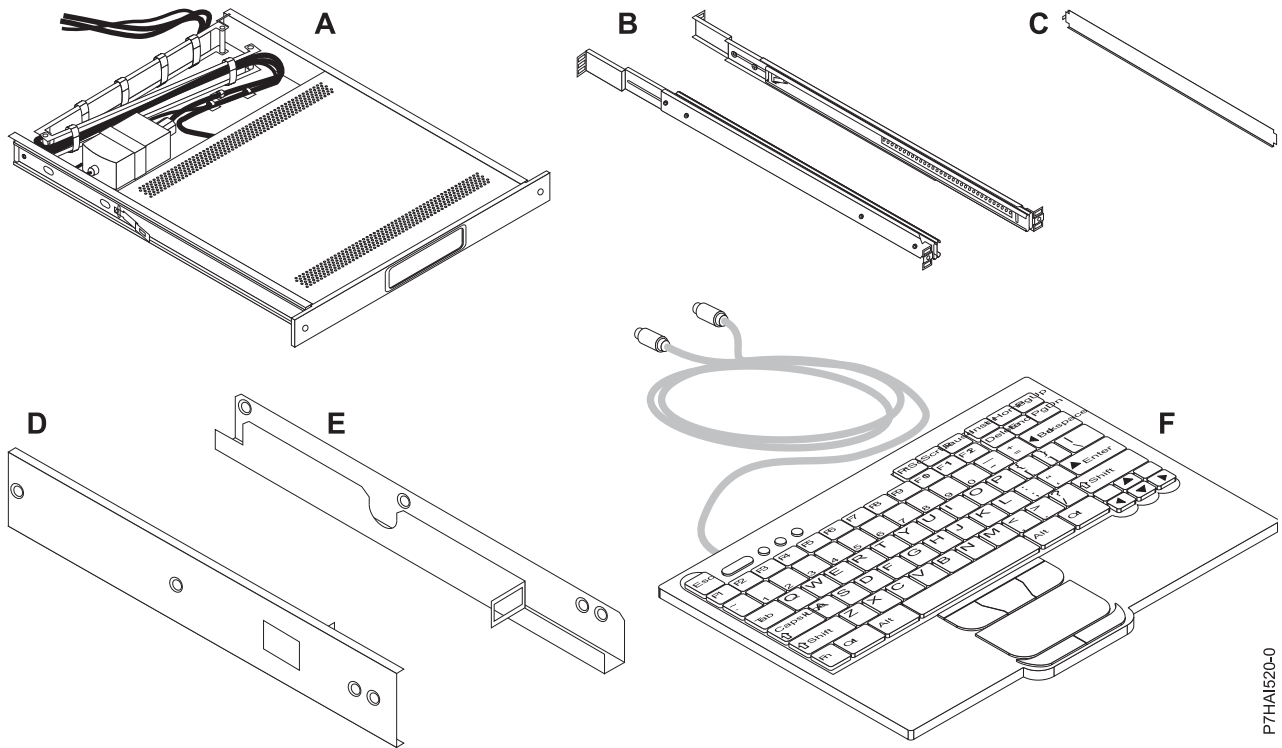
Learn how to install the monitor and keyboard, which are shipped with the 7042-CR6 HMC, into a rack. This is a customer task.

If an HMC is used to manage a POWER8 processor-based system, the HMC must be at CR3, or later, it must be a rack-mounted HMC model. The IBM eserver 7316-TF3 is a 17 inch, flat-panel, and rack-mounted monitor and keyboard tray. A special keyboard, that is available for various languages, fits inside the front of the keyboard tray. The monitor and keyboard tray occupy 1 Electronics Industries Association (EIA) unit 1 of space in a rack cabinet. You can install a console switch behind the tray to attach more than one server to the flat panel monitor and keyboard.

To install the 7042-CR6 HMC into a rack, complete the following steps:

Attention: Installing the rails in the rack is a complex procedure. To install the rails correctly, you must perform each task in the following order.

1. Complete a parts inventory. For instruction, see [Completing a parts inventory](#).
2. Locate the rack-mounting hardware kit and the system rail assemblies that were included with your system unit.



P7HA1520-0

Figure 71. Installation kit parts

Table 12. Installation kit parts content

Install Kit	Parts Content
A	One keyboard tray with built-in flat panel monitor
B	Outer rails (2)
C	Rail alignment spacer (1)
D	Right-side console-switch mounting bracket (1)
E	Left-side console-switch mounting bracket (1)
F	Keyboard with built-in pointing device (1)
G	Miscellaneous Hardware kit: 12 cage nuts, 12 clip nuts, 10 Phillips screws, 4 (8-32) screws, and 2 thumbscrews.
H	1.8 m (6 ft) power cord (1)
I	2.4 m (8 ft) International Electrotechnical Commission (IEC) connector power cable (1)
J	Keyboard extension cable (1)
K	Mouse extension cable (1)
L	The CD containing Windows keyboard and mouse drivers (not for use with Eserver pSeries systems or any AIX®, Linux, or OS/400-based system)
<p>Important: Use the following tools to install the flat panel rack-mounted monitor and keyboard:</p> <ul style="list-style-type: none"> • Scissors • Phillips screwdriver • Flat-head screwdriver 	

Completing a parts inventory

You might need to complete a parts inventory.

If you have not done so, complete a parts inventory before proceeding with the installation:

1. Locate the kitting report in an accessory box.
2. Ensure that you received all the parts that were ordered.

If there are incorrect, missing, or damaged parts, contact your IBM reseller or IBM sales and support.

Marking the location without using a rack-mounting template

You can mark the location without using a template.

A rack-mounting template is not included with this system. These systems are 1 EIA unit high.

To determine the mounting location, complete the following steps:

1. Determine to place the system in the rack. Record the EIA location.

Note: An EIA unit on your rack consists of a grouping of three holes.

2. Facing the front of the rack and working from the right side, place a supplied self-adhesive dot next to the top hole of the EIA unit.

Note: The self-adhesive dots are used to aid in identifying locations on the rack. If you no longer have any of the dots, use some other form of marking tool to aid you in identifying hole locations (for example, tape, a marker, or pencil). If you are installing slide rails, place a mark or self-adhesive dot on the lower and the middle hole of each EIA unit.

3. Place another self-adhesive dot next to the bottom hole of the above EIA unit.

Note: If you are counting the holes, begin with the hole identified by the first dot and count up two holes. Place the second dot next to the third hole.

4. Repeat step 1 on page 8 for the corresponding holes located on the left side of the rack.
5. Go to the rear of the rack.
6. On the right side, find the EIA unit that corresponds to the bottom EIA unit marked on the front of the rack.
7. Place a self-adhesive dot at the bottom EIA unit.
8. Place a self-adhesive dot at the top hole of the EIA unit.
9. Mark the corresponding holes on the left side of the rack.

Installing the monitor and keyboard into a rack

Learn how to install the monitor and keyboard that are shipped with the 7042-CR6 HMC into a rack.

The IBM 7316-TF3 17-inch, flat panel, rack-mounted, monitor and keyboard occupies 1.75 inches (1 EIA) of rack-mounting space in a rack cabinet. You can use the brackets that are provided with this kit to install an optional console switch in the same rack-mounting space as the monitor console kit.

To install the monitor and keyboard of the 7042-CR6 HMC into a rack, complete the following steps:

Attention: Remove the rack doors and side panels to provide easy access for installation.

Complete the following steps to install the monitor and keyboard into a rack:

1. Select a location in the rack for the monitor and keyboard tray. For more information, see Marking the location.
2. Install 4 cage nuts (on square-holed rack flanges) or 4 clip nuts (round-holed rack flanges) in the same EIA positions on the front and rear of the rack.

Note: If you plan to install the optional console switch, install a cage nut or clip nut in the center-rear position as shown in the following illustration.

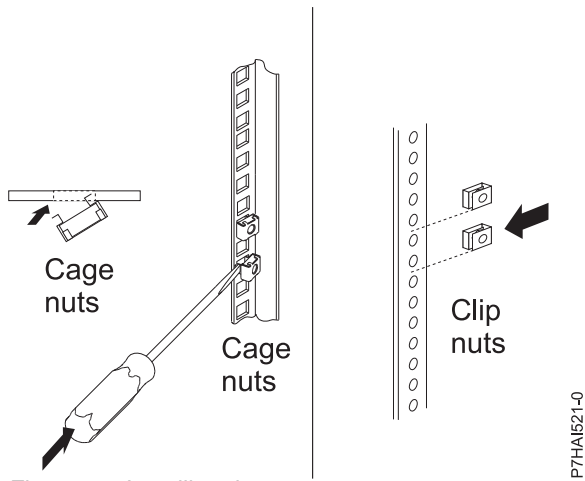


Figure 72. Installing the cage nuts

3. Loosen the two rail-adjustment screws that are located on each of the outer slide rails. Extend the rails to the maximum outward adjustment.
4. Adjust the outer slide-rail brackets to fit the depth of the rack cabinet. Then, attach the front of the slide-rail brackets to fit the depth of the rack cabinet by using four screws from the miscellaneous hardware kit. The screws should be finger-tight to allow adjustment of the rails.

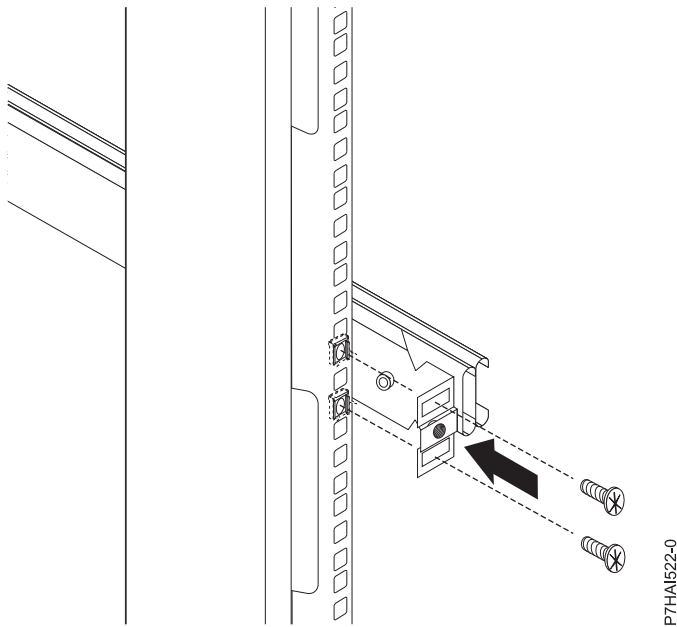


Figure 73. Adjusting the side-rail bracket

Note: Ensure that the slide-rail brackets extend outside of the rack-cabinet mounting flanges. Do not install screws in the middle holes on the front or rear of the slide-rail brackets. These holes will be used to attach thumbscrews or optional console-switch mounting brackets, respectively, later in this procedure.

5. Use the four screws from the miscellaneous hardware kit and finger-tight them from the rear of the slide-rail brackets to the rack cabinet. Ensure that the slide-rail brackets extend outside of the rack-cabinet mounting flanges.
6. Tighten the two rail-adjustment screws on each of the outer rails that you loosened in step 5

7. Insert the rail-alignment spacer into the slide-rail middle holes. Ensure that the rail-alignment spacer wraps around the rails. Tighten the front four screws and then, remove the spacer.

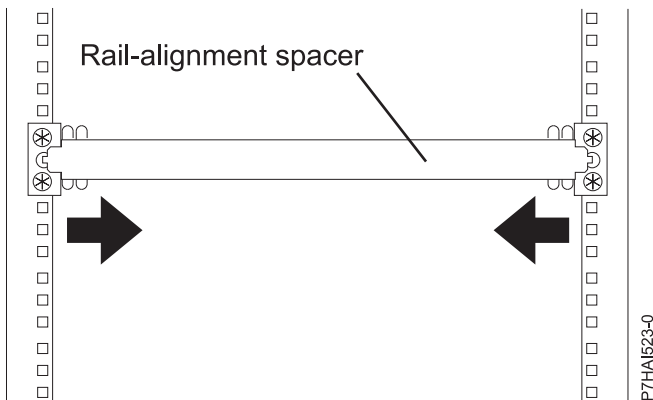


Figure 74. Inserting the rail-adjustment spacer

8. Extend the inner part of the rails mounted in the rack, and then, slide the ball-bearing assemblies forward to the front of the rails.
9. Slide the flat-panel monitor and keyboard tray into the ball-bearing assemblies in the rails.

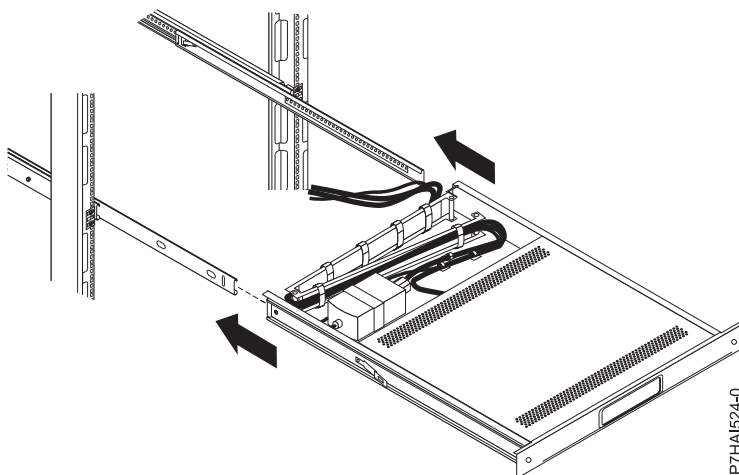


Figure 75. Sliding the monitor and keyboard

10. Press the release latches and push the flat-panel monitor and keyboard tray completely into the rack. You may experience some resistance initially, as the ball-bearing assemblies align between the inner and outer rails. Pull out the tray halfway, and then, push it back to seat the tray in the rails. Perform this a few times to ensure that the tray moves smoothly in the rails.

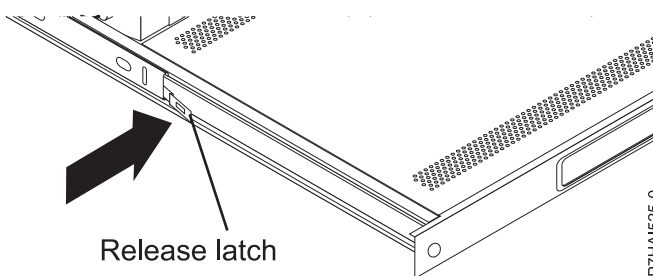


Figure 76. Using the release latch

Note:

The video cable is connected to the flat-panel monitor. When you install the tray in the rack cabinet, ensure that you do not pinch or cut the video cable.

11. Push the tray into the rack and tighten the four rear slide-rail bracket screws.
12. Place the keyboard on a stable flat surface and remove the two adhesive rubber pads located at each end of the bottom of the new keyboard. Do not leave the rubber pads on the keyboard, because the rubber pads might extend into the space below the tray.

Note:

Do not extend the keyboard feet. The flat-panel monitor screen might be damaged if the feet is extended when the monitor is closed.

13. Pull the tray out of the rack until it is extended fully on the rails.
14. Lift the front of the flat-panel monitor, then raise the monitor to the full upright position.

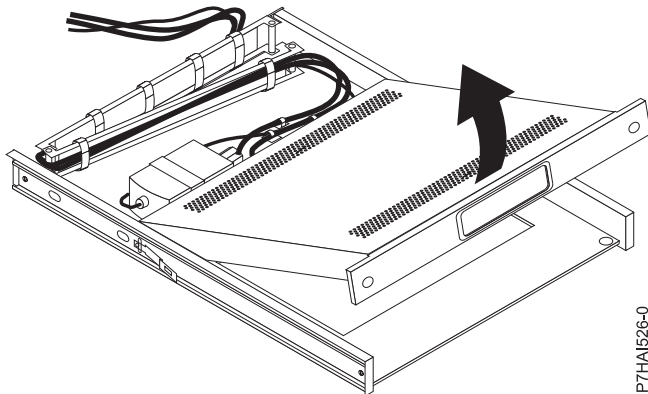


Figure 77. Raising the monitor to the full upright position

15. Insert the keyboard into the tray. Then, route the keyboard-and-mouse cable through the cord clip on the bottom of the tray, up through the opening on the right side of the tray, and toward the cable-management arm. Pull out the full length of the cable through the opening.
16. Place the keyboard and mouse cables on the tray behind the monitor. Ensure that the cables do not obstruct devices in the rack when the tray is pushed into its position. In the following steps, you will route the cables through the cable-management arm.
17. Lower the monitor to the down position and then push the tray all the way into the rack. Use the thumbscrews to secure the front of the tray into the rack.
18. From the rear of the rack, remove the shipping straps that holds the cable-management arm into the tray.
19. Route the keyboard and mouse cables through the cable-management arm. Use the existing cable straps to secure the cables.
20. Remove the rail-adjustment screw that is located closest to the rear of the rack from the left-slide rail. Use a screw to attach the cable-management arm to the rail.

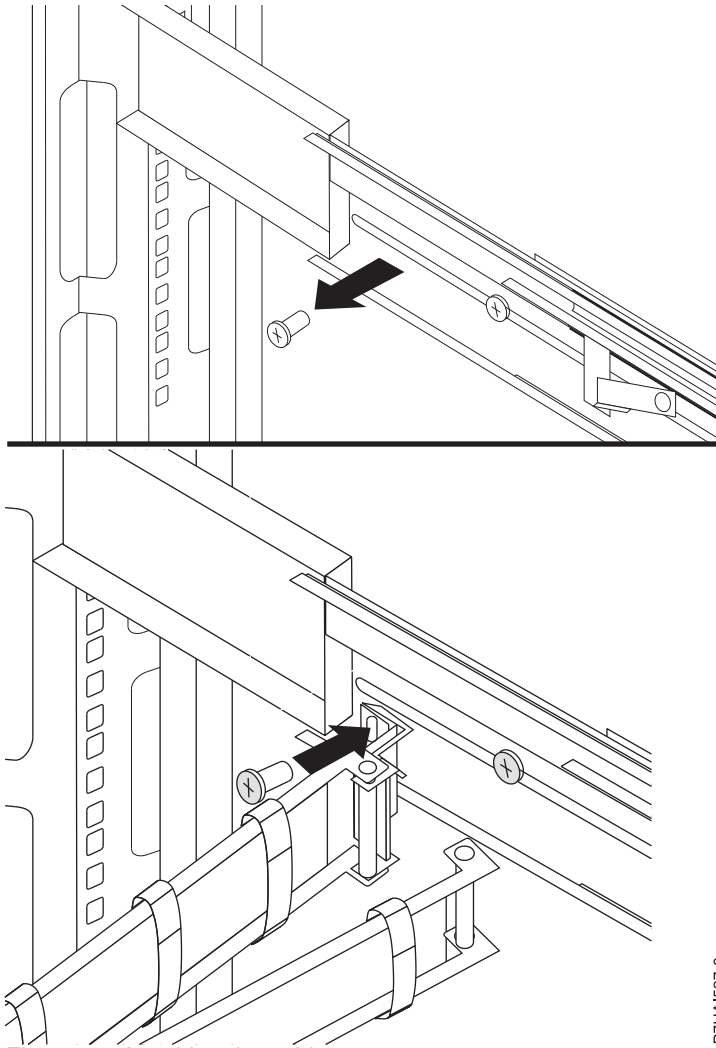


Figure 78. Attaching the cable-management arm

P7HA627-0

21. Connect the video, keyboard, and mouse connectors to either a server or optional console switch in the rack cabinet. If you are installing the optional console switch, see *Installing the Optional Console Switch* and complete the steps described. If not, follow the procedure from Step 21 to complete the installation of your monitor and keyboard tray.
22. Connect the power cord to the short jumper cord on the cable-management arm.
23. Connect all cables and signal connectors to the correct device or connector.
24. Ensure that all power switches are turned off. Connect the power cord to a grounded electrical outlet or power distribution unit (PDU).

Note: Ensure that the voltage of the local electrical supply is in the range 100 - 240 volt ac, before you connect the ac power cord to the dc adapter outlet.

25. Extend the tray from the front of the rack cabinet. Route cables within the rack cabinet, and secure them with cable straps.

Installing the console switch (optional)

Learn how to install the optional console switch.

You can use the console switch to connect more than one server to a single monitor and keyboard. The console switch option is available separately, but custom mounting brackets for the switch are available with the installation kit.

By installing the console switch behind the monitor and keyboard tray, both the monitor and keyboard tray can occupy the same space in the rack. To install the console switch behind the tray, use the brackets provided with the installation kit.

Complete the following steps to install the console switch behind the tray:

1. Use two 8-32 screws to attach the right and left side brackets to the right-side and left-side of the console switch respectively.

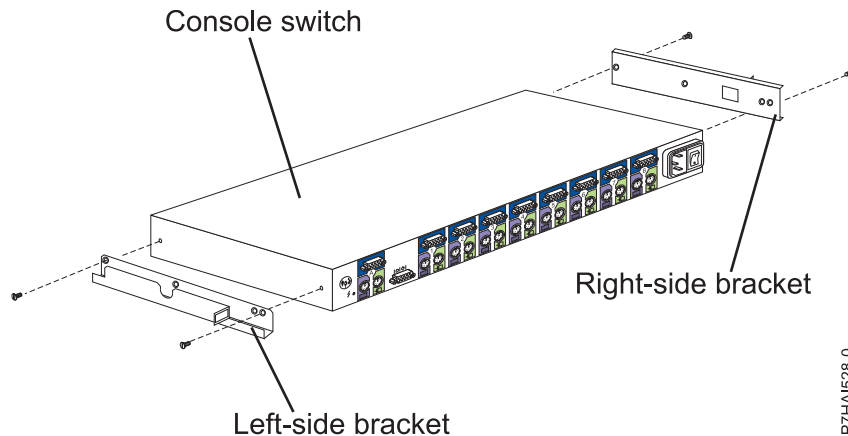


Figure 79. Installing the console switch

Note: The left-side bracket has a channel to route the power, video, keyboard, and mouse cables. Ensure that you attach the brackets to the console switch so that the channel on the left-side bracket faces upward.

2. Install the console switch behind the flat panel monitor and keyboard tray by using four (two on each side) philips screws supplied in your miscellaneous hardware kit.
3. Route the power, video, keyboard, and mouse cables through the channel in the left-side bracket on the console switch. Then, connect the video, keyboard, and mouse connectors to the console switch.

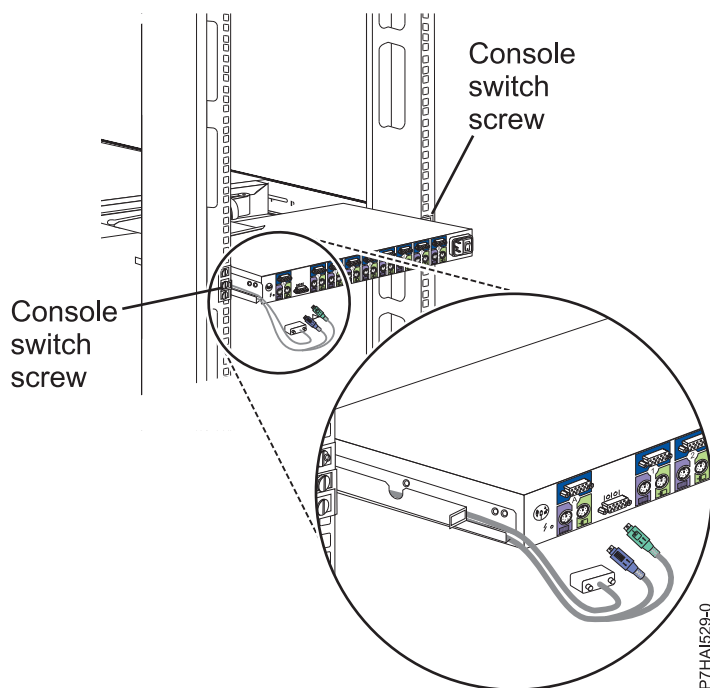


Figure 80. Routing cables

4. Connect the power cords, routing cables, and cable straps. For instruction, see [Connect the power cord to the short jumper cord on the cable-management arm](#).

Configuring the HMC by using the HMC Classic or HMC Enhanced interface

Learn how to set up your network connections, configure your HMC, perform postconfiguration steps, and upgrade and update your HMC by using the HMC Classic or HMC Enhanced interface.

Notes:

1. The HMC Classic interface is no longer available on Hardware Management Console (HMC) version 8.7.0, or later. The functions that were previously available with the HMC Classic interface are now available with the HMC Enhanced+ interface.
2. The HMC Enhanced GUI is available on the HMC Version 8.1.0.1 or 8.2.0 by choosing the HMC Enhanced option while logging into the HMC. As of HMC version 8.3.0, the procedures and functions of the HMC Enhanced interface are now a part of the HMC Enhanced+ interface.
3. Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to ease the setup of the HMC. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the available settings that the wizard guides you through. You can also perform the configuration steps without the aid of the wizard by Configuring the HMC using the HMC menus.

Choosing network settings on the HMC

Learn about the network settings you can use on the HMC.

HMC network connections

You can use different types of network connections to connect your HMC to managed systems. For more information about how to configure the HMC to connect to a network, see [“Configuring the HMC”](#) on page 89. For more information about using the HMC on a network, see the following:

Types of HMC network connections:

Learn how to use the HMC remote management and service functions by using your network.

The HMC supports the following types of logical communications:

HMC to managed system

Used to perform most of the hardware management functions, in which HMC issues control function requests through the service processor of the managed system. The connection between the HMC and the service processor is sometimes referred to as the *service network*. This connection is required for managed system management.

HMC to logical partition

Used to collect platform-related information (hardware error events, hardware inventory) from the operating systems that are running on logical partitions, and to coordinate certain platform activities (dynamic LPAR, concurrent repair) with those operating systems. If you want to use service and error notification features, you must create this connection.

HMC to BMC

Note: The baseboard management controller (BMC) connection is applicable only to HMC model 7063-CR1.

Used to perform service and maintenance tasks. The BMC connection is used to load and maintain the HMC firmware on the system. This connection is required for access to the BMC on the HMC.

HMC to remote users

Provides remote users with access to HMC functions. Remote users can access the HMC in the following ways:

- By using the web browser to access all the HMC GUI functions remotely.
- By using Secure Socket Shell (SSH) to access the HMC command line functions remotely.

HMC to service and support

Used to transmit data, such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communications path to make automatic service calls.

Your HMC can support up to four separate physical Ethernet interfaces, depending on the model. The stand-alone version of the HMC supports only three HMC interfaces, by using one integrated Ethernet adapter and up to two plug-in adapters. Use each of these interfaces in the following ways:

- One or more network interfaces can be used exclusively for HMC-to-managed system communications, which means that only the HMC and service processors of the managed systems are on that network. Even though the network interfaces into the service processors are encrypted for the Secure Sockets Layer (SSL) Protocol and password-protected, having a separate dedicated network can provide a higher level of security for these interfaces.
- An open network interface would typically be used for the network connection between the HMC and the logical partitions on the managed systems, for the HMC-to-logical partition communications. You can also use this open network interface to manage the HMC remotely.
- Optionally, you can use a third interface to connect to logical partitions and manage the HMC remotely. This interface can also be used as a separate HMC connection to different groups of logical partitions. For example, you might want to have an administrative LAN that is separate from the LAN on which all the usual business transactions are running. Remote administrators can access the HMC and other managed units by using this method. Sometimes the logical partitions are in different Network security domains, perhaps behind a firewall, and you might want to have different HMC network connections into each of those two domains.

Web browser requirements for HMC

The Hardware Management Console (HMC) version 8.7.0 is supported by Google Chrome version 57, Microsoft Internet Explorer (IE) version 11.0, Mozilla Firefox versions 45 and 52 Extended Support Release (ESR), and Safari version 10.1.

If your browser is configured to use an Internet proxy, a local IP addresses should be included in the exception list. Consult your network administrator for more information on the exception list. If you still need to use the proxy to get to the HMC, enable Use HTTP 1.1 through proxy connections under the Advanced tab in your Internet Options window.

Session cookies need to be enabled in order for ASMI to work when connected to HMC remotely. The asm proxy code saves session information and uses it. Follow the steps to enable the session cookies.

Enabling session cookies in Internet Explorer.

1. Select Tools and Click Internet Options.
2. Select Privacy and Click Advanced.
3. Ensure that the Always allow session cookies is checked. If not, select the Override automatic cookie handling and select Always allow session cookies.
4. Select Prompt under First-party Cookies and Third-party Cookies.
5. Click OK.

Enabling session cookies in Chrome.

1. Click Settings and then click Advanced.

2. From the Privacy and security section, click Content settings.
3. Click Cookies. Enable Allow sites to save and read cookie data.
4. Exit from the settings menu.

Enabling session cookies in Firefox.

1. Select Tools and click Options.
2. Click Cookies.
3. Select Allow sites to set cookies.
4. Select Exceptions and add HMC.
5. Click OK.

Enabling session cookies in Safari.

1. Click Safari and then click Preferences.
2. Click Privacy.
3. Click Cookies. Enable Allow sites to save and read cookie data.
4. Set the option Block cookies to Never.
5. Exit from the preferences menu.

Private and open networks in the HMC environment:

The HMC can be configured to use open and private networks. Private networks allow the use of a selected range of nonroutable IP-addresses. A *public*, or "open" network describes a network connection between the HMC to any logical partitions and to other systems on your regular network.

Private networks

The only devices on the HMC private network are the HMC itself and each of the managed systems to which that HMC is connected. The HMC is connected to each managed system's FSP (Flexible Service Processor).

On most systems, the FSP provides two Ethernet ports labeled **HMC1** and **HMC2**. This allows you to connect up to two HMCs.

Some systems have a dual-FSP option. In this situation, the second FSP acts as a "redundant" backup. The basic setup requirements for a system with two FSPs are essentially the same as those without a second FSP. The HMC must be connected to each FSP, so additional network hardware is required (for example, a LAN switch or hub) when there is more than one FSP or there are multiple managed systems.

Note: Each FSP port on the managed system must be connected to only one HMC.

Public networks

The open network can be connected to a firewall or router for connecting to the Internet. Connecting to the Internet allows the HMC to "call home" when there are any hardware errors that need to be reported.

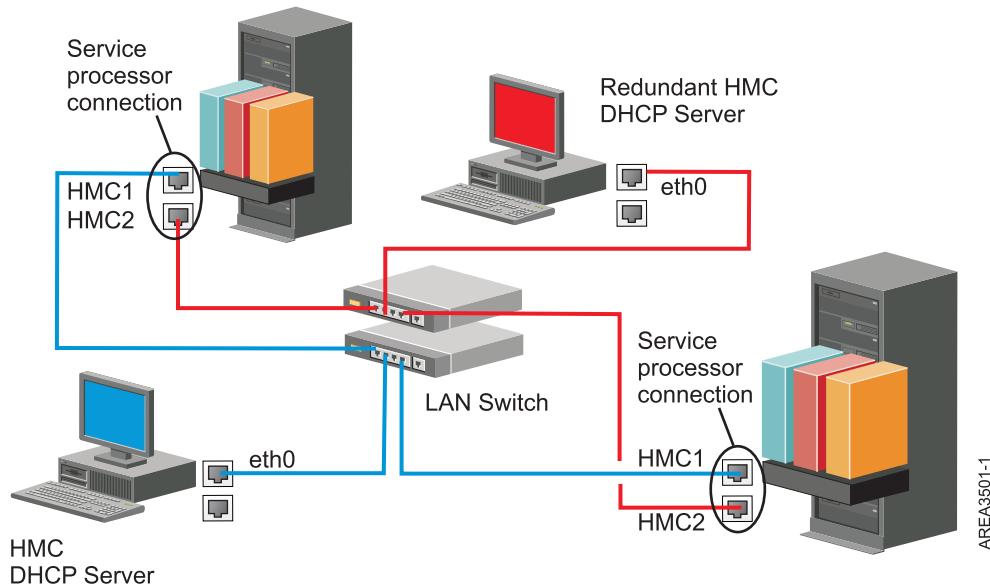
The HMC itself provides its own firewall on each of its network interfaces. A basic firewall is automatically configured when you run the HMC Guided Setup wizard, but you customize your firewall settings after the initial HMC installation and configuration.

HMC as a DHCP server:

You can use the HMC as a Dynamic Host Configuration Protocol (DHCP) server.

Note: If you are using IPv6, the discovery process must be done manually. For IPv6, there is no automatic discovery.

For more information about how to configure the HMC as a DHCP server, see “Configuring the HMC as a DHCP server” on page 97.

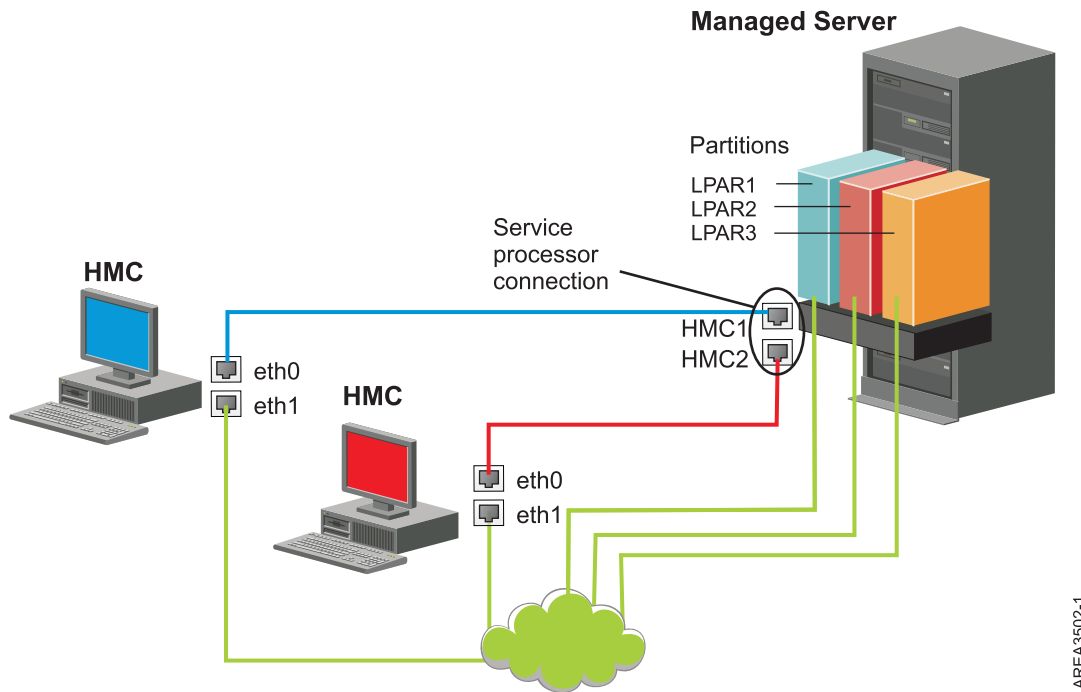


This figure shows a redundant HMC environment with two managed systems. The first HMC is connected to the first port on each FSP, and the redundant HMC is connected to the second port on each HMC. Each HMC is configured as a DHCP server, using a different range of IP addresses. The connections are on separate private networks. As such, it is important to ensure that no FSP port is connected to more than one HMC.

Each managed system's FSP port that is connected to an HMC requires a unique IP address. To ensure that each FSP has a unique IP address, use the HMC's built-in DHCP server capability. When the FSP detects the active network link, it issues a broadcast request to locate a DHCP server. When correctly configured, the HMC responds to that request by allocating one of a selected range of addresses.

If you have multiple FSPs, you must have your own LAN switch or hub for the HMC to FSP private network. Alternately, this private segment can exist as several ports in a private *virtual LAN* (VLAN) on a larger managed switch. If you have multiple private VLANs, you must ensure that they are isolated and that there is not any crossover traffic.

If you have more than one HMC, you must also connect each HMC to the logical partitions, and to each other, on the same open network.



AREA3502-1

This figure shows two HMCs connected to a single managed server on the private network and to three logical partitions on the public network. You can have an additional Ethernet adapter for the HMC to have three network interfaces. You can use this third network as a management network or connect it to the CSM (Cluster Systems Manager) Management Server.

For more information about how to configure the HMC as a DHCP server, see “Configuring the HMC as a DHCP server” on page 97.

Deciding which connectivity method to use for the call-home server:

Learn more about the connectivity options you have when you use the call-home server.

You can configure the HMC to send hardware service-related information to IBM by using a LAN-based Internet connection, or a dial-up connection over a modem.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

You have two communication choices when you configure the LAN-based Internet connection. The first choice is to use standard Secure Sockets Layer (SSL). The SSL communication can be enabled to connect to the Internet through your proxy server. SSL connectivity is more likely to be compliant with corporate security guidelines. Your second option is to use a VPN connection.

Note: If your open network interface connection uses only Internet Protocol Version 6 (IPv6), you cannot use Internet VPN to connect to support. For more information about the protocols that are used, see “Choosing an Internet Protocol” on page 79.

The advantages to using an Internet connection can include:

- Faster transmission speed
- Reduced customer expense (for example, the cost of a dedicated analog telephone line)
- Greater reliability

The following security characteristics are in effect, regardless of the connectivity method chosen:

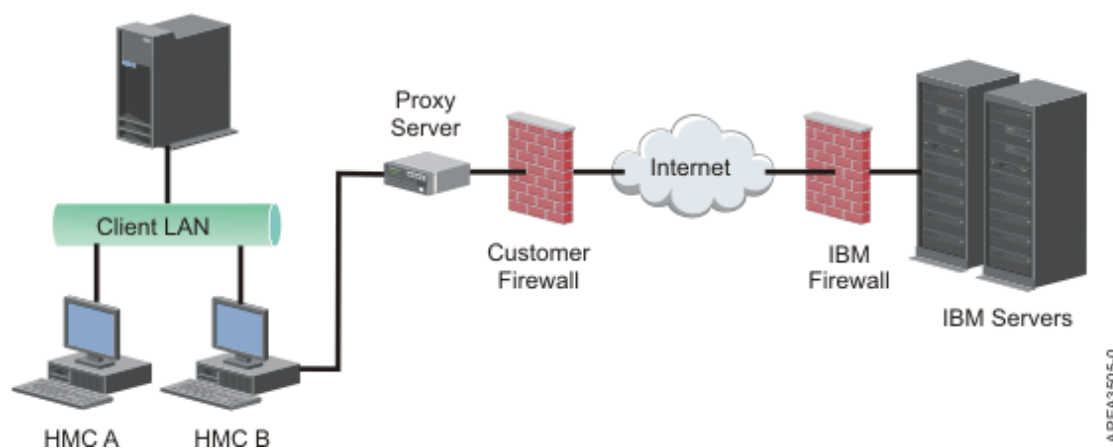
- Remote Support Facility requests are always initiated from the HMC to IBM. An inbound connection is never initiated from the IBM Service Support System.
- All data that is transferred between the HMC and the IBM Service Support System are encrypted by using a high-grade encryption. Depending upon the connectivity method that is chosen, it is encrypted by using either SSL or IPSec Encapsulating Security Payload (ESP).
- When you initialize the encrypted connection, the HMC authenticates the target destination as that of the IBM Service Support System.

Data sent to the IBM Service Support System consists solely of information about hardware problems and configuration. No application or customer data is transmitted to IBM.

Using an indirect Internet connection with a proxy server

If your installation requires the HMC to be on a private network, you might be able to connect indirectly to the Internet by using an SSL proxy, which can forward requests to the Internet. One of the other potential advantages of using an SSL proxy is that the proxy can support logging and audit facilities.

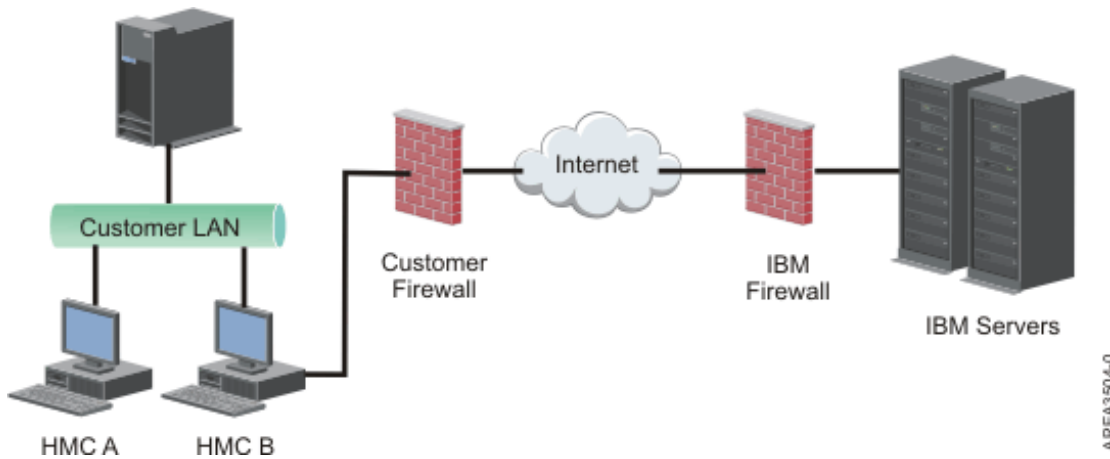
To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616) and the CONNECT method. Optionally, basic proxy authentication (RFC 2617) can be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.



For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. You can configure your proxy server to limit the specific IP addresses to which the HMC can connect. See "Internet SSL address lists" on page 79 for a list of IP addresses.

Using a direct Internet SSL connection

If your HMC can be connected to the Internet, and the external firewall can be set up to allow established TCP packets to flow outbound to the destinations described in "Internet SSL address lists" on page 79, you can use a direct Internet connection.



Simplified connectivity:

Learn about the IP addresses the HMC uses when it is using simplified connectivity.

A new call-home server environment is available that provides a front-end proxy to the current call-home infrastructure. This environment simplifies the information technology that is required by reducing the number of IBM servers, enabling IPv6 connectivity, and providing enhanced security by supporting NIST 800-131A. You have fewer IBM IP addresses to open on your firewall. All call-home internet traffic flows through the call-home proxy.

Note: Simplified connectivity is available on HMC version 8.3.0 or later.

The HMC uses the following IPv4 addresses to contact IBM service and support when it is configured to use simplified connectivity:

- 129.42.56.189
- 129.42.60.189
- 129.42.54.189

The HMC uses the following IPv6 addresses to contact IBM service and support when it is configured to use simplified connectivity:

- 2620:0:6c0:200:129:42:56:189
- 2620:0:6c2:200:129:42:60:189
- 2620:0:6c4:200:129:42:54:189

Using Internet SSL to connect to remote support:

All the communications are handled through TCP sockets initiated by the HMC and use a high-grade SSL to encrypt the data that is transmitted. The destination TCP/IP addresses are published (see “Internet SSL address lists” on page 79) so that external firewalls can be configured to allow these connections.

Note: The standard HTTPS port 443 is used for all communications.

The HMC can be enabled to connect directly to the Internet or to connect indirectly from a proxy server provided by the customer. The decision about which of these approaches works best for your installation depends on the security and networking requirements of your enterprise. The HMC (directly or through the SSL proxy) uses the following addresses when it is configured to use Internet SSL connectivity.

Choosing an Internet Protocol:

Determine the IP address version used when the HMC connects to your service provider.

Most users use Internet Protocol Version 4 (IPv4) to connect to a service provider. IPv4 addresses appear in the format representing the four bytes of the IPv4 address, separated by periods (for example, 9.60.12.123) to access the Internet. You can also use Internet Protocol Version 6 (IPv6) to connect to a service provider. IPv6 is often used by network administrators to ensure unique address space. If you are unsure of the Internet Protocol used by your installation, contact your network administrator. For more information about using each version, see “Setting the IPv4 address” on page 98 and “Setting the IPv6 address” on page 98.

Internet SSL address lists:

Learn about the addresses the HMC uses when it is using Internet SSL connectivity.

The HMC uses the following IPv4 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity.

The following IPv4 addresses are for all locations:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

The following IPv4 addresses are for the Americas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

The following IPv4 addresses are for all locations other than the Americas:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Note: When configuring a firewall to allow an HMC to connect to these servers, only the IP addresses specific to the geographic region are required.

The HMC uses the following IPv6 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity:

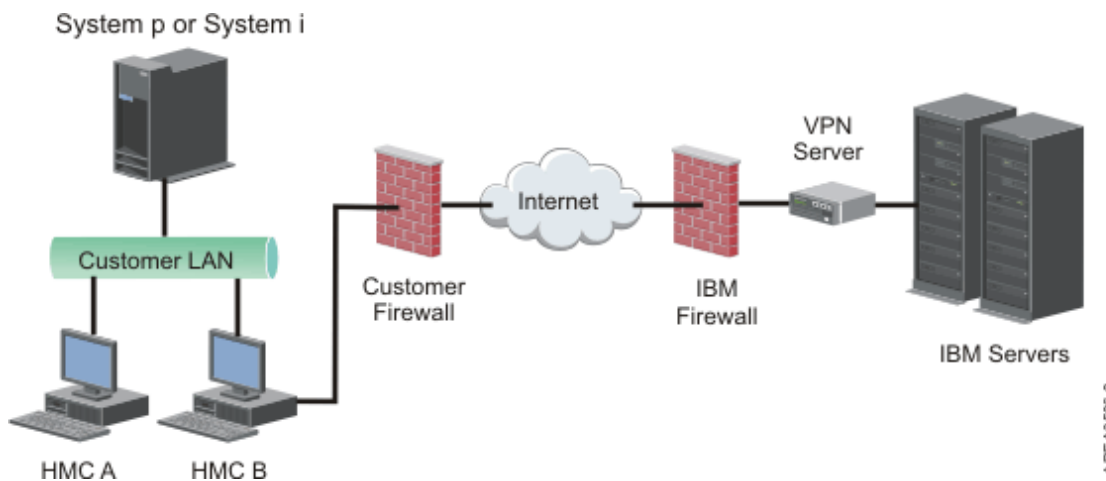
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

Using a virtual private network to connect to remote support:

A virtual private network (VPN) provides security when you connect to remote support.

Note: This connection type is available only on HMC version 8.2.0 or earlier.

A VPN gives users the privacy of a separate network over public lines by substituting encryption and other security measures for the physically separate network lines of traditional private networks. In addition to being able to be used for outbound connectivity, a VPN connection can also be configured on an as-needed basis to support remote service requests.



It is system administrator's responsibility to provide an Internet connection. The firewall can also limit the specific IP addresses to which the HMC can connect. If you need to configure your firewall to limit the IP addresses, see "VPN server address list" for a list of addresses you can use.

For more information about how to connect to the Internet by using a LAN-based VPN, see "Configuring the HMC network types" on page 93.

VPN server address list:

Lists the servers used by an HMC when the HMC is configured to use Internet VPN connectivity.

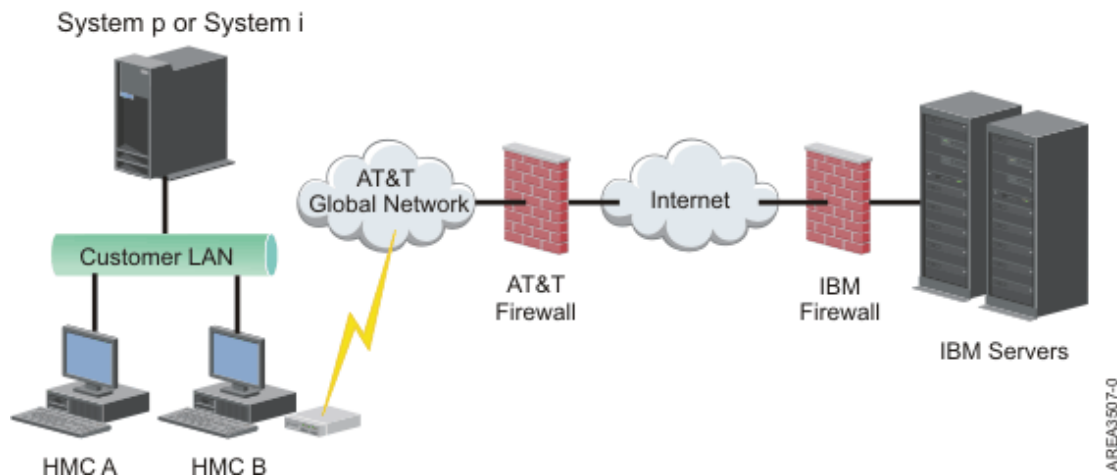
The following servers are used by an HMC when it is configured to use Internet VPN connectivity. All connections use ESP and UDP on port 500 and port 4500 when a Network Address Translation (NAT) firewall is being used.

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

Using the telephone and modems to connect to remote support:

If you want to use a modem to connect to remote support, you must provide a dedicated analog line to connect to the HMC modem. The HMC uses the modem to dial the global network and to connect to IBM service and support.

Note: This connection type is available only on HMC version 8.2.0 or earlier.



For more information about connecting to remote support by using the telephone and modems, see “Configuring the HMC network types” on page 93.

Using multiple call-home servers:

This topic describes what you need to know when you decide to use more than one call-home server.

To avoid a single point of failure, configure the HMC to use multiple call-home servers. The first available call-home server attempts to handle each service event. If the connection or transmission fails with this call-home server, the service request is retried using the other available call-home servers until one is successful or all have been tried.

The connected HMC that has been identified by problem analysis to be the primary analyzing console for a given managed system will report the problem. This primary console will also replicate the problem report to any secondary HMC. This secondary HMC must be recognized on the network by the primary HMC. A secondary HMC is recognized by the primary HMC as an additional call-home server when:

- The primary HMC is configured to use "discovered" call-home servers and the call-home server is either on the same subnet as the primary HMC or it manages the same system
- The call-home server has been manually added to the list of call-home server consoles available for outbound connectivity

Preparing for HMC configuration

Use this section to gather required configuration settings that you need to know before you begin the configuration steps.

To configure the HMC, you must understand the related concepts, make decisions and prepare information.

This section describes the information you will need to connect your HMC to the following:

- Service processors in your managed systems
- Logical partitions on those managed systems
- Remote workstations
- IBM Service, to implement “call-home” functions

Note: Additional connectivity and security information is available. For more information, see the **ESA for HMC Connectivity Security for IBM POWER6®, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000®** white paper available at: IBM Electronic Service Agent™ (<http://www-01.ibm.com/support/esa/security.htm>).

To prepare for HMC configuration, complete the following steps:

1. Obtain and install the latest level of the HMC code version you want to install.
2. Determine the physical location of the HMC in relation to the servers it will manage. If the HMC is more than 25 feet from its managed system, you must provide web browser access to the HMC from the managed system's location so that service personnel can access the HMC.
3. Identify the servers that the HMC will manage.
4. Determine whether you will use a private or an open network to manage servers. If you decide to use a private network, use DHCP, unless you are using a Cluster Systems Management (CSM) configuration. CSM does not support IPv6. To access CSM, you must have two networks. For more information about CSM, see the documentation that was provided with that feature. For more information about private and open networks, see "Private and open networks in the HMC environment" on page 74.
5. If you will use an open network to manage an FSP, you must set the FSP's address manually through the Advanced System Management Interface menus. A private, non-routable network is recommended.
6. If you have two HMCs, designate a primary and secondary HMC. The primary HMC should be physically closer to the machine, and should be the HMC that is configured to call home.
7. Determine the network settings that you will need to connect the HMC to remote workstations, logical partitions, and network devices.
8. Define how the HMC will "call home." Call home options include either over an outbound-only Secure Socket Layer (SSL) Internet connection, a modem, or a Virtual Private Network (VPN) connection.
9. Determine the HMC users that you will create and their passwords, as well which roles they will be given. You must assign the hscroot and hscpe users a password.
10. Document the following company contact information that will be needed when configuring call home:
 - Company name
 - Administrator contact
 - Email address
 - Telephone numbers
 - Fax numbers
 - The street address of the HMC's physical location
11. If you plan to use email to notify operators or systems administrators when information is sent to IBM Service through call-home, identify the Simple Mail Transfer Protocol (SMTP) server and the email addresses you will use.
12. You must define the following passwords:
 - The access password that will be used to authenticate the HMC to the FSP
 - The ASMI password that will be used for the **admin** user
 - The ASMI password that will be used for the **general** user

Create the passwords when you connect from the HMC to a new server for the first time. If the HMC is a redundant or second HMC, obtain the HMC User password and be prepared to enter it when connecting the first time to the managed server's FSP.

When you have completed these preparation steps, complete the "Preinstallation configuration worksheet for the HMC" on page 83.

Preinstallation configuration worksheet for the HMC

Use this worksheet to have the installation information you need ready for the installation.

Network Settings

LAN Interface: Choose the available adapters (such as eth0, eth1) that will be used by this HMC to connect to managed systems, logical partitions, service and support, and remote users. See “HMC network connections” on page 72 for more information. Connectivity from the HMC can either be on a private or open network.

Ethernet Adapter Speed and Duplex

Enter the desired Ethernet adapter speed and duplex mode. The autodetection option determines which option is optimal if you are not sure which speed and duplex would produce optimum results for your hardware. Default = Autodetection Media speed specifies the speed in duplex mode of an Ethernet adapter. Select Autodetection unless you have a requirement to specify a fixed media speed. Any device connected to the FSP (switches/HMC), must be set to Auto (Speed) / Auto (Duplex) mode, as it is the default FSP setting and cannot be changed.

Table 13. Ethernet Adapter Speed and Duplex

	eth0	eth1	eth2	eth3
Select speed and duplex mode				
Media speed (Autodetection, 10/100/1000 Full/Half Duplex)				

For more information about private and open networks, see “Private and open networks in the HMC environment” on page 74.

Table 14. Private networks and open networks

	eth0	eth1	eth2	eth3
Specify Private or Open network for each adapter				

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration. You can specify this HMC as a DHCP server. If this is the first or only HMC on the private network, enable the HMC as a DHCP server. When you do this, the managed systems on the network will be automatically configured and discovered by the HMC.

For Ethernet adapters specified as Private networks, complete the following table:

Table 15. Private networks

	eth0	eth1
Do you want to specify this HMC as a DHCP server? (yes/no)		
If "yes," record the IP address range you want to use		

If you are using the 7063-CR1 HMC, you must connect the Ethernet **IPMI** port to a network to access the baseboard management controller (BMC) on the HMC. For more information, see “Configure BMC connectivity” on page 142. Complete the following table for your BMC connection.

Table 16. BMC connection

	IPMI
Do you want to configure this connection through DHCP mode? (yes/no)	
If no, list the specified static addresses below:	
IP address:	
Subnet mask:	
Gateway:	

For Ethernet adapters specified as *open* networks, complete the following tables. For more information about the different Internet Protocol versions, see “Choosing an Internet Protocol” on page 79.

Using IPv6

If you are using IPv6, talk to your network administrator and decide how you want to obtain IP addresses. Then, complete the following tables:

Table 17. Using IPv6

	eth0	eth1	eth2	eth3
Are you using a statically-assigned IP address? If yes, record that address here.				

Table 18. Using IPv6

	eth0	eth1	eth2	eth3
Are you getting IP addresses from a DHCP server? (Yes/No)				

Table 19. Using IPv6

	eth0	eth1	eth2	eth3
Are you getting IP addresses from an IPv6 router?				

For more information about setting IPv6 addresses, see “Setting the IPv6 address” on page 98. For more information about using only IPv6 addresses, see “Using only IPv6 addresses” on page 98.

Using IPv4

Complete the following tables for Ethernet adapters specified as open networks using IPv4.

Table 20. Using IPv4

	eth0	eth1	eth2	eth3
Do you want to obtain an IP address automatically? (yes/no)				
If no, list the specified address below:				

Table 20. Using IPv4 (continued)

	eth0	eth1	eth2	eth3
TCP/IP Interface Address:				
TCP/IP Interface Network Mask:				
Firewall Settings:				
Would you like to configure HMC firewall settings? (yes/no)				
If yes, list the applications and IP addresses that should be allowed through the firewall:				

TCP/IP Information

A unique TCP/IP address is required for each node, both for Support Element (SE) and Hardware Management Console (HMC). The assigned network mask is used to generate a unique address, by default, for the local private LAN. If the nodes will be connected into a larger network with an administered TCP/IP address, you can specify the TCP/IP address to be used. The default is generated by the system.

Firewall Settings

HMC firewall settings create a security barrier that allows or denies access to specific network applications on the HMC. You can specify these control settings individually for each physical network interface, allowing you control over which HMC network applications can be accessed on each network.

If you have configured at least one adapter as an Open network adapter, you must provide the following additional information to enable your HMC to access the LAN:

Table 21. Local host information

Local host information	
HMC host name:	
Domain name:	
Description of HMC:	
Gateway information	
Gateway Address: (nnn.nnn.nnn.nnn)	
Gateway device:	
DNS enablement	
Do you want to use DNS? (yes/no)	
If "yes", specify DNS Server Search Order below:	
1.	
2.	

Table 21. Local host information (continued)

Local host information	
Domain suffix search order:	
1.	
2.	

Local Host Information

To identify your Hardware Management Console (HMC) to the network, enter the HMC's host name and domain name. Unless you are using only short host names on your network, enter a fully qualified host name. Domain name example: name.yourcompany.com

Gateway Information

To define a default gateway, fill in the TCP/IP address to be used for routing IP packets. The gateway address informs each computer or network device when to send data if the target station is not located on the same subnet as the source.

DNS Enablement

The Domain Name System (DNS) is used to provide a standard naming convention for locating IP-based computers. By defining DNS servers, you can use host names to identify servers and Hardware Management Consoles (HMCs) rather than IP addresses.

DNS Server Search Order

Enter the IP addresses of DNS servers to be searched for mapping the host names and IP addresses. This search order is available only when DNS is enabled.

Domain Suffix Search Order

Enter the domain suffixes you are using. The HMC uses domain suffixes to append to unqualified names for DNS searches. Suffixes are searched in the order in which they are listed. This search order is available only when DNS is enabled.

Email notification

List email contact information if you wish to be notified by email when hardware problem events occur on your system.

Table 22. Email notification

Fields	
Email Addresses:	
SMTP server:	
Port:	
Errors to be notified:	
Only call-home problem events	
All problem events	

SMTP server

Type the simple mail transfer Protocol (SMTP) address of the server to be notified of a system event. An example of an SMTP server name is relay.us.ibm.com.

SMTP is the Protocol used to send email. When using SMTP, a client sends a message and communicates with the SMTP server using the SMTP Protocol.

If you do not know the SMTP address of your server or are not sure, contact your network administrator.

Port Type the port number of the server to be notified of a system event, or use the default port.

Email addresses to be notified

Enter configured email addresses to be notified when a system event occurs.

- Select **Only call-home problem events** to only receive notification when events occur that create a call-home function.
- Select **All problem events** to receive notification when any events occur.

Service Contact Information

Table 23. Service Contact Information

Service Contact Information	
Company name	
Administrator name	
Email address	
Phone number	
Alternate phone number	
Fax number	
Alternate fax number	
Street address	
Street address 2	
City or locality	
State	
Postal code	
Country or region	
Location of HMC (if same as above administrator address, specify "same"):	
Street address	
Street address 2	
City of locality	
State	
Postal code	
Country or region	

Service authorization and connectivity

Select the type of connection to contact your service provider. For a description of these methods including security characteristics and configuration requirements, see "Deciding which connectivity method to use for the call-home server" on page 76.

Table 24. Type of connection

Type of connection	
	Secure Sockets Layer (SSL) through the Internet

Table 24. Type of connection (continued)

Type of connection	
	Dialup from the local HMC
	Virtual private network (VPN) through the Internet

Secure Sockets Layer (SSL) through the Internet:

If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by using encrypted Secure Sockets Layer (SSL) using the existing Internet connection. select **Use SSL Proxy** if you want to configure the use of encrypted SSL using an indirect connection using an SSL Proxy.

Table 25. Secure Sockets Layer (SSL) through the Internet

Secure Sockets Layer (SSL) through the Internet	
Use SSL proxy? (yes/no)	
If yes, list information below:	
Address:	
Port:	
Authenticate with the SSL Proxy?	
If yes, list information below:	
User:	
Password:	

Internet connection Protocol used

For more information about the different Internet Protocols, see “Choosing an Internet Protocol” on page 79.

- IPv4
- IPv6
- IPv4 and IPv6

Dial-up from the local HMC

Enter the dial-up information to configure your local modem. Specify which telephone numbers to use to dial your service provider. When you are connecting, the telephone numbers will be dialed in the order in which they are listed.

Table 26. Dial-up from the local HMC

Fields	
Dial prefix:	
Tone:	
Pulse:	
Wait for dial tone?	
Enable speaker?	

Virtual Private Network (VPN)

If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by virtual private network (VPN) using the existing Internet connection.

Note: If you select Virtual Private Network (VPN) through the Internet, you will not be directed to select any other options.

Call-home servers

Determine which HMCs you want to configure to connect to service and support as call-home servers. For more information about using multiple call-home servers, see “Using multiple call-home servers” on page 81.

This HMC

Another HMC

If you checked **Another HMC**, list the other HMCs that have been configured as call-home servers here:

Table 27. Other HMCs that have been configured as call-home servers

List of HMC host names or IP addresses that have been configured as call-home servers

Additional Support Benefits

My Systems and Premium Search

Table 28. Additional Support Benefits

Fields	
List your IBM ID	
List your IBM ID	

In order to access valuable, customized support information in the My Systems and Premium Search sections of the Electronic Services website, Customers must register their IBM ID with this system. If you do not already have one, you can register for an IBM ID at: www.ibm.com/account/profile.

Note: IBM provides personalized Web functions that use information collected by the IBM Electronic Service Agent application. To use these functions, you must first register on the IBM Registration website at <http://www.ibm.com/account/profile>.

To authorize users to use the Electronic Service Agent information to personalize the Web functions, enter your IBM ID that you registered on the IBM Registration website. Go to <http://www.ibm.com/support/electronic> to see the valuable support information available to customers that register an IBM ID with their systems.

Configuring the HMC

Learn how to configure network connections, security, service applications, and some user preferences.

Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to ease the setup of the HMC. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the available settings that

the wizard guides you through. You can also perform the configuration steps without the aid of the wizard by Configuring the HMC using the HMC menus.

Before you start, gather the required configuration information that you need to complete the steps successfully. See “Preparing for HMC configuration” on page 81 for a list of the required information. When you are finished preparing, ensure that you complete the “Preinstallation configuration worksheet for the HMC” on page 83 and then return to this section.

Configuring the HMC by using the fast path through the Guided Setup wizard

In most cases, the HMC can be set up to operate effectively using many of the default settings. Use this fast path checklist to prepare the HMC for service. When you have completed these steps, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

Start the HMC and complete the steps in the Guided Setup wizard:

Log in to the HMC interface and configure your HMC using the Guided Setup wizard.

Note: If this is a new installation, ensure that the managed system is not connected to a power source. For a rack-mounted HMC, this means that the only device plugged into the power distribution bus (PDB) before you plug in the main power supply is the HMC. If this is a second HMC that is connected to the same managed system, the managed system can be connected to a power source.

1. Turn on the HMC by pressing the power button.
2. Wait for the HMC to automatically select the default language and locale preference after 30 seconds.
3. Accept the Hardware Management Console license agreements. If you decline the Hardware Management Console license agreements, you cannot complete the HMC configuration.
4. Click **Log on and launch the Hardware Management Console web application**.
5. Log in to the HMC:

Note: If your system administrator (**hmcadmin**) has changed the password, enter it here.

- ID: hscroot
- Password: abc123


The Guided Setup wizard opens.

6. Click **OK** on the Guided Setup entry window.

Note: If the Guided Setup wizard did not display when you started the HMC, Click **Guided Setup Wizard** in the navigation area of the HMC welcome page.

7. Complete the steps in the Guided Setup wizard using the preinstallation configuration worksheet that you completed. Click **Yes** to continue and complete the steps in the Connectivity and Call-Home Servers wizard.
8. On the Summary window, click **Finish**.
9. If you haven't connected the Ethernet crossover cable to your managed system, do so now.



10. In the HMC navigation area, click the **Serviceability** icon , and then select **Service Management**.
11. In the content area, click **Authorize User**. The Authorize User window opens.
12. Enter your IBM ID in the field and click **OK**.

For HMC model 7063-CR1, you must configure the baseboard management controller (BMC) IP address. For more information, see Configure BMC connectivity.

Review your configuration:

On the Status window, monitor the progress of the different configuration settings you selected. This window might show a status of Pending for some tasks for several minutes. Click **View Log** to see status messages relating to each task. Click **Close** at any time to close the Guided Setup wizard. Tasks that are still running will continue to run. Your HMC is now configured.

Configuring the HMC by using the HMC menus

This section provides a complete list of all HMC configuration tasks, guiding you through the process of configuring your HMC. Choose this option if you prefer not to use the Guided Setup wizard.

You must restart your HMC for the configuration settings to take effect, so you might want to print this checklist and keep it with you as you configure your HMC.

This information contains references to tasks that are not included in this PDF. You can access additional support materials by referring to the **Additional Resources** section on the HMC Welcome page.

Prerequisites

Before you begin configuring the HMC using the HMC menus, be sure to complete the configuration preparation activity described in “Preparing for HMC configuration” on page 81.

Table 29. Manual HMC configuration tasks and where to find related information

Task	Where to find related information
1. Start the HMC.	“Starting the HMC” on page 92
2. Set the date and time.	
3. Change predefined passwords.	
4. Create additional users and return to this checklist when you have completed this step.	
5. Configure network connections.	“Configuring the HMC network types” on page 93
6. If you are using an open network and a fixed IP address, set identification information.	
7. If you are using an open network and a fixed IP address, configure a routing entry as the default gateway.	“Configuring a routing entry as the default gateway” on page 99
8. If you are using an open network and a fixed IP address, configure domain name services.	“Configuring domain name services” on page 100
9. If you are using a fixed IP address and have DNS enabled, configure domain suffixes.	“Configuring domain suffixes” on page 100
10. Configure your server to connect to IBM service and support and return to this checklist when you have completed this step.	“Configuring the HMC so that it can contact service and support” on page 101
11. Configure the Events Manager for Call Home.	“Configuring the Events Manager for Call Home” on page 106
12. Connect the managed system to a power source.	
13. Set passwords for the managed system, and each of the ASMI passwords (general and admin)	“Setting passwords for the managed system” on page 107
14. Access ASMI to set the date and time on the managed system.	
15. Start the managed system and return to this checklist when you have completed this step.	
16. Ensure that you have one logical partition on the managed system.	

Table 29. Manual HMC configuration tasks and where to find related information (continued)

Task	Where to find related information
17. Optional: add another managed system and return to this checklist when you have completed this step.	
18. Optional: If you are installing a new server with your HMC, configure the logical partitions and install the operating system.	
19. If you are not installing a new server at this time, perform optional postconfiguration tasks to further customize your configuration.	"Postconfiguration steps" on page 108

Starting the HMC:

You can log in to the HMC and choose which language you want to be displayed in the interface. Use the default User ID hscroot and password abc123 to log on to the HMC for the first time.

To start the HMC, do the following procedure:

1. Turn on the HMC by pressing the power button.
2. If English is your language preference, continue with step 4.
If your language preference is a language other than English, type the number **2** when you are prompted to change the locale.

Note: This prompt times out in 30 seconds if you do not act.

3. Select the locale that you want to display from the list in the Locale Selection window, and click **OK**. The locale identifies the language that the HMC interface uses.
4. Click **Log on and launch the Hardware Management Console web application**.
5. Log in to the HMC with the following default user ID and password:
ID: hscroot
Password: abc123

Note: On HMC Version 8.1.0.1, you can choose from the following login options:

Login: Last Login, HMC Classic, or HMC Enhanced

Select which software interface to use when you log in to the HMC. The HMC Classic interface provides access to all traditional functions of the HMC and the HMC Enhanced interface provides both redesigned and new virtualization tasks and functions.

Last Login

Displays the graphical user interface (GUI) that you selected from your previous login session.

HMC Enhanced

Displays the newer enhanced GUI with the enhanced PowerVM features.

HMC Classic

Displays the standard GUI without the enhanced PowerVM features.

Note: When the HMC is working as a DHCP server, the HMC uses the default password when it connects to the service processor for the first time.

6. Press Enter.

Changing the date and time:

The battery-operated clock keeps the date and time for the HMC. You might need to reset the console date and time if the battery is replaced, or if you physically move your system to a different time zone. Learn how to change the date and time for the HMC.

If you change the date and time information, the change does not affect the systems and logical partitions that the HMC manages.

To change the date and time for the HMC, do the following:

1. Ensure that you are a member of one of the following roles:
 - Super administrator
 - Service representative
 - Operator
 - Viewer
2. In the navigation area, click **HMC Management**.
3. In the content pane, click **Change Date and Time**.
4. If you select **UTC** in the **Clock** field, the time setting will adjust automatically for daylight saving time in the time zone you select. Enter the date, time, and time zone, and click **OK**.

Configuring the HMC network types:

Configure your HMC so that it can communicate to the managed system, logical partitions, remote users, and service and support.

Configuring HMC settings to use an open network to connect to the managed system:

Configure the HMC so that it can connect to and manage a managed system using an open network.

To configure the HMC network settings so that it can connect to the managed system using an open network, do the following:

Table 30. Configuring HMC settings to use an open network to connect to the managed system

Task	Where to find related information
1. Decide which interface you want to use for your managed system. eth0 is preferred.	"Preinstallation configuration worksheet for the HMC" on page 83
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0" on page 95
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 96
b. Select the open network type.	"Selecting a private or open network" on page 97
c. Set static addresses.	"Setting the IPv4 address" on page 98
d. Set the firewall.	"Changing HMC firewall settings" on page 98
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 99
f. Configure DNS.	"Configuring domain name services" on page 100
4. Configure additional adapters, if you have them.	
5. Test the connection between the managed server and the HMC.	"Testing the connection between the HMC and the managed system" on page 108

Configuring HMC settings to use a private network to connect to the managed system:

Configure the HMC so that it can connect to and manage a managed system using a private network.

To configure the HMC network settings so that it can connect to the managed system using a private network, do the following:

Table 31. Configuring HMC settings to use a private network to connect to the managed system

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	“Preinstallation configuration worksheet for the HMC” on page 83
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 95
3. Configure the HMC as a DHCP server.	“Configuring the HMC as a DHCP server” on page 97
4. Test the connection between the managed server and the HMC.	“Testing the connection between the HMC and the managed system” on page 108

Configuring HMC settings to use an open network to connect to logical partitions:

To configure the HMC network settings so that it can connect to logical partitions using an open network, do the following:

Table 32. Configuring HMC settings to use an open network to connect to logical partitions

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	“Preinstallation configuration worksheet for the HMC” on page 83
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 95
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	“Setting the media speed” on page 96
b. Select the open network type.	“Selecting a private or open network” on page 97
c. Set static addresses.	“Setting the IPv4 address” on page 98
d. Set the firewall.	“Changing HMC firewall settings” on page 98
e. Configure the default gateway.	“Configuring a routing entry as the default gateway” on page 99
f. Configure DNS.	“Configuring domain name services” on page 100
4. Configure additional adapters, if you have them.	
5. Test the connection between the managed server and the HMC.	“Testing the connection between the HMC and the managed system” on page 108

Configuring HMC settings to use an open network to connect to remote users:

To configure the HMC network settings so that it can connect to remote users using an open network, do the following:

Table 33. Configuring HMC settings to use an open network to connect to remote users

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	“Preinstallation configuration worksheet for the HMC” on page 83

Table 33. Configuring HMC settings to use an open network to connect to remote users (continued)

Task	Where to find related information
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0"
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 96
b. Select the open network type.	"Selecting a private or open network" on page 97
c. Set static addresses.	"Setting the IPv4 address" on page 98
d. Set the firewall.	"Changing HMC firewall settings" on page 98
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 99
f. Configure DNS.	"Configuring domain name services" on page 100
g. Configure suffixes.	"Configuring domain suffixes" on page 100
4. Configure additional adapters, if you have them.	

Configuring HMC call-home server settings:

To configure the HMC call-home server settings so that problems can be reported, do the following:

Table 34. Configuring HMC call-home server settings

Task	Where to find related information
1. Be sure you have all the required customer information	"Preinstallation configuration worksheet for the HMC" on page 83
2. Configure this HMC to report errors or choose an existing call-home server to report errors	"Configuring the local console to report errors to service and support" on page 102 "Choosing existing call-home servers to connect to service and support for this HMC" on page 105
3. Verify that your call-home configuration is working	"Verifying that your connection to service and support is working" on page 105
4. Authorize users to view collected system data	"Authorizing users to view collected system data" on page 105
5. Schedule transmission of system data	"Transmit service information" on page 105

Identifying the Ethernet port defined as eth0:

Your Ethernet connection to the managed server must be made using the Ethernet port that is defined as eth0 on your HMC.

If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, the primary integrated Ethernet port is always defined as eth0 or eth1 on your HMC, if you intend to use the HMC as a DHCP server for your managed systems.

If you have installed additional Ethernet adapters in the PCI slots, the port that is defined as eth0 depends on the location and type of Ethernet adapters you have installed.

Note: These are general rules and may not apply for all configurations.

The following table describes the rules for Ethernet placement by HMC type.

Table 35. HMC types and associated rules for Ethernet placement

HMC type	Rules for Ethernet placement
Rack-mounted HMCs with two integrated Ethernet ports	<p>The HMC supports only one additional Ethernet adapter.</p> <ul style="list-style-type: none"> • If an additional Ethernet adapter is installed, that port is defined as eth0. In this case, the primary integrated Ethernet port is then defined as eth1, and the secondary integrated Ethernet port is defined as eth2. • If the Ethernet adapter is a dual port Ethernet adapter then port labeled Act/Link A will normally be eth0. The port labeled Act/link B would be eth1. In this case, the primary integrated Ethernet port is then defined as eth2, and the secondary integrated Ethernet port is defined as eth3. • If no adapters are installed, the primary integrated Ethernet port is defined as eth0.
Stand-alone models with a single integrated Ethernet port	<p>The definitions depend upon the type of Ethernet adapter you have installed:</p> <ul style="list-style-type: none"> • If only one Ethernet adapter is installed, that adapter is defined as eth0. • If the Ethernet adapter is a dual port Ethernet adapter, then the port labeled Act/link A will be eth0. The port labeled Act/link B would be eth1. In this case, the primary integrated Ethernet port is then defined as eth2. • If no adapters are installed, the integrated Ethernet port is defined as eth0. • If multiple Ethernet adapters have been installed, see "Determining the interface name for an Ethernet adapter."

Determining the interface name for an Ethernet adapter:

If you configure the HMC as a DHCP server, that server can operate only on the network interface card (NIC) connectors that the HMC identifies as eth0 and eth1. You might also need to determine which NIC connector you need to plug the Ethernet cable into. Learn more about determining which NIC connectors the HMC identifies as eth0 and eth1.

To determine the name the HMC has assigned to an Ethernet adapter, do the following:

1. Open the restricted shell terminal. Select **HMC Management > Open Restricted Shell Terminal**.
2. Type the following at the command line: `tail -f /var/log/messages`. The messages log scrolls when new events occur.
3. Plug in your Ethernet cable. If the cable was already plugged in, then unplug it, wait 5 seconds, and plug in the cable again. The restricted shell scrolls to display a message when you plug-in the cable. The following example entry shows that this Ethernet port is identified as eth0: Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100.
4. Repeat this procedure for all other Ethernet ports, and record your results.
5. Type Ctrl+C to stop the **tail** command.

Setting the media speed:

Learn how to specify the media speed which includes the speed and duplex mode of the Ethernet adapter.

The default for the HMC adapter settings is **Autodetection**. If this adapter is connected to a LAN switch, you must match the switch port settings. To set the media speed and duplex, complete the following steps:

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter you want to work with and click **Details**.
5. In the Local area network information section, select **Autodetection** or the appropriate media speed and duplex combination.
6. Click **OK**.

Selecting a private or open network:

A *private service network* consists of the HMC and the managed systems. A private service network is restricted to consoles and the systems they manage, and is separate from your company network. An *open network* consists of your private service network and your company network. An open network might contain network endpoints in addition to consoles and managed systems, and might span across multiple subnets and network devices.

To select a private or public network, do the following:

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Lan Adapter** tab.
6. In the Local area network information page, select **Private** or **Open**.
7. Click **OK**.

Configuring the HMC as a DHCP server:

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration.

To configure the HMC as a DHCP server, do the following:

1. In the navigation area, click **HMC Management**.
2. In the Work area, click **Change network settings**. The Customize Network Settings window opens.
3. Select the LAN adapter that you want to work with and click **Details**.
4. Select **Private** and then select the network type.
5. In the DHCP Server section, select **Enable DHCP Server** to enable the HMC as a DHCP server.

Note: You can configure the HMC to be a DHCP server only on a private network. If you use an open network, you do not have the option to select the **Enable DHCP**.

6. Enter the address range of the DHCP server.
7. Click **OK**.

If you configured your HMC to be a DHCP server on a private network, you must verify that your HMC DHCP private network is configured correctly. For information about connecting your HMC to a private network, see “Selecting a private or open network.”

For more information, see “HMC as a DHCP server” on page 74.

Setting the IPv4 address:

Learn how to set your IPv4 address on the HMC.

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Basic Settings** tab.
6. Select an IPv4 address.
7. If you selected to specify an IP address, enter the TCP/IP interface address and the TCP/IP interface network mask.
8. Click **OK**.

Setting the IPv6 address:

Learn how to set your IPv6 address on the HMC.

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **IPv6 Settings** tab.
6. Select an Autoconfig option or add a static IP address.
7. If you added an IP address, enter the IPv6 address and the prefix length and click **OK**.
8. Click **OK**.

Using only IPv6 addresses:

Learn how to configure the HMC so that it uses only IPv6 addresses.

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Select **No IPv4 address**.
6. Click the **IPv6 Settings** tab.
7. Select **Use DHCPv6 to configure IP settings** or add static IP addresses. Then click **OK**.

After you click OK, you must reboot your HMC for these changes to take effect.

Changing HMC firewall settings:

In an open network, a firewall is used to control outside access to your company network. The HMC also has a firewall on each of its Ethernet adapters. To control the HMC remotely or give remote access to others, modify the firewall settings of the Ethernet adapter on the HMC that is connected to your open network.

To configure a firewall, use the following steps:

1. In the navigation area, click **HMC Management**.
2. Click **Change network settings**.
3. Click the **LAN Adapters** tab.

4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Firewall** tab.
6. Using one of the following methods, you can allow any IP address using a particular applications through the firewall, or you can specify one or more IP addresses:
 - Allow any IP address using a particular application through the firewall:
 - a. From the top box, highlight the application.
 - b. Click **Allow Incoming**. The application displays in the bottom box to signify that it has been selected.
 - Specify which IP addresses to allow through the firewall:
 - a. From the top box, highlight an application.
 - b. Click **Allow Incoming by IP Address**.
 - c. On the Hosts Allowed window, enter the IP address and the network mask.
 - d. Click **Add** and click **OK**.
7. Click **OK**.

Enabling remote restricted shell access:

You can enable remote restricted shell access when configuring a firewall.

To enable remote restricted shell access, do the following:

1. In the navigation area, click **HMC Management**.
2. Click **Remote Command Execution**.
3. Select **Enable remote command execution using the ssh facility** and then click **OK**.

Now remote restricted shell access is enabled.

Enabling remote web access:

You can enable remote web access to your HMC.

To enable remote web access, do the following:

1. In the navigation area, click **HMC Management**.
2. Click **Remote Operation**.
3. Select **Enable** and then click **OK**.

Now remote web access is enabled.

Configuring a routing entry as the default gateway:

Learn how to configure a routing entry as the default gateway. This task is available for those using an open network.

To configure a routing entry as the default gateway, do the following:

1. In the navigation area, click **HMC Management**.
2. In the Work area, click **Change network settings**. The Customize Network Settings window opens.
3. Click the **Routing** tab.
4. In the Default gateway information section, enter the gateway address and gateway device of the routing entry you want to set as the default gateway.
5. Click **OK**.

Configuring domain name services:

If you plan to set up an open network, configure domain name services.

If you plan to set up an open network, configure domain name services. Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Configuring domain name services includes enabling DNS and specifying the domain suffix search order.

1. In the navigation area, click **HMC Management**.
2. In the work area, click **Change network settings**. The Change Network Settings window opens.
3. Click the **Name Services** tab.
4. select **DNS enabled** to enable DNS.
5. Specify the DNS server and domain suffix search order and click **Add**.
6. Click **OK**.

Configuring domain suffixes:

The list of domain suffixes is used to resolve an IP address starting with the first entry in the list.

The domain suffix is a string appended to a host name that is used to help resolve its IP address. For example, a host name of `myname` might not be resolved. However, if the string `myloc.mycompany.com` is an element in the domain suffix table, then there will be an attempt to resolve `myname.mloc.mycompany.com` also.

To configure a domain suffix entry, use these steps:

1. In the navigation area, click **HMC Management**.
2. In the work area, click **Change network settings**. The Customize Network Settings window opens.
3. Click the **Name Services** tab.
4. Enter a string to be used as a domain suffix entry.
5. Click **Add** to add it to the list.

Configuring the HMC so that it uses LDAP remote authentication:

You can configure your HMC so that it uses LDAP (Lightweight Directory Access Protocol) remote authentication.

When a user logs in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote LDAP server for authentication. You must configure your HMC so that it uses LDAP remote authentication.

Note: Before you configure the HMC so that it uses LDAP authentication, you must ensure that a working network connection exists between the HMC and the LDAP servers. For more information about configuring HMC network connections, see “Configuring the HMC network types” on page 93.

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

1. In the navigation area, click **HMC Management**.
2. In the content area, click **Configure LDAP**. The **LDAP Server Definition** window opens.
3. Select **Enable LDAP**.
4. Define an LDAP server to use for authentication (for example, Microsoft Active Directory, Tivoli®, and Open LDAP).
5. Define the LDAP attribute that is used to identify the authenticated user. The default is **uid**, but you can use your own attributes. For Microsoft Active Directory, use **sAMAccountName** as the attribute.

6. Define the distinguished name tree, also known as the search base, for the LDAP server.
7. Click **OK**.
8. If a user wants to use LDAP authentication, the user must configure their profile so that it uses LDAP remote authentication instead of local authentication.

Configuring the HMC so that it uses Key Distribution Center servers for Kerberos remote authentication:

You can configure the HMC so that it uses Key Distribution Center (KDC) servers for Kerberos remote authentication.

When a user logs in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote Kerberos server for authentication. You must configure your HMC so that it uses Kerberos remote authentication.

Note: Before you configure the HMC so that it uses KDC servers for Kerberos remote authentication, you must ensure that a working network connection exists between the HMC and the KDC servers. For more information about configuring HMC network connections, see “Configuring the HMC network types” on page 93.

To configure the HMC so that it uses KDC servers for Kerberos remote authentication, do the following:

1. Enable the Network Time Protocol (NTP) service on the HMC and set the HMC and the KDC servers to synchronize time with the same NTP server. To enable the NTP service on the HMC, do the following:
 - a. In the navigation area, select **HMC Management**.
 - b. In the content area, select **Change Date and Time**.
 - c. Select the **NTP Configuration** tab.
 - d. Select **Enable NTP service on this HMC**.
 - e. Click **OK**.
2. Configure each remote HMC user's profile so that it uses Kerberos remote authentication instead of local authentication.
3. Optional: you can import a service-key file into this HMC. The service-key file contains the host principal that identifies the HMC to the KDC server. Service-key files are also known as *keytabs*. To import a service-key file into this HMC, do the following:
 - a. In the navigation area, select **HMC Management**.
 - b. In the content area, select **Configure KDC**. The Key Distribution Center Configuration window opens.
 - c. Select **Actions > Import Service Key**. The Import Service Key window opens.
 - d. Type the location of the service key file.
 - e. Click **OK**.
4. Add a new KDC server to this HMC. To add a new KDC server to this HMC, do the following:
 - a. In the navigation area, select **HMC Management**.
 - b. In the content area, select **Configure KDC**. The Key Distribution Center Configuration window opens.
 - c. Select **Actions > Add KDC Server**. The Import Service Key window opens.
 - d. Type the realm and the host name or IP address of the KDC server.
 - e. Click **OK**.

Configuring the HMC so that it can contact service and support:

Configure your HMC so that it can notify you when problems occur.

Configuring the HMC so that it can connect to service and support using the call-home setup wizard:

Configure the HMC so that it is a call-home server using the call-home wizard.

This procedure describes how to configure the HMC as a call-home server using direct (LAN-based) and indirect (SSL) connections to the Internet.

Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- If you are configuring Internet support through a proxy server, you must also have the following:
 - The IP address and port of the proxy server
 - The proxy authentication information
- The adapter designated as **eth1** (the one that is designated as an open network) is used. For more information, see “Choosing network settings on the HMC” on page 72.
- An Ethernet cable physically connects the HMC to the LAN.

To configure the HMC so that it is a call-home server using the call-home wizard, do the following:

1. In the navigation area, select **Service Management**.
2. In the content area, select **Call-Home Setup Wizard**. The Connectivity and Call-Home Servers wizard opens. Follow the instructions in the wizard to configure call-home.

Configuring the local console to report errors to service and support:

Configure this HMC so that it can call-home errors by using LAN connectivity.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

Configuring an HMC to contact service and support using LAN-based Internet and SSL:

Describes how to configure the HMC as a call-home server using direct (LAN-based) and indirect (SSL) connections to the Internet.

Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- Customer contact information has been configured. Verify this by going to the HMC interface and clicking **Service Management > Manage Customer Information**.
- If you are configuring internet support through a proxy server, you must also have the following:
 - The IP address and port of the proxy server
 - The proxy authentication information
- You need at least one open network interface configured. For more information, see “Private and open networks in the HMC environment” on page 74.
- An Ethernet cable physically connects the HMC to the LAN.

To configure the HMC as a Call Home server using LAN-based Internet and SSL, do the following:

1. In the navigation area, click **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**. The Call-home Server Consoles window opens.
3. Click **Configure**.

4. In the Outbound Connectivity Settings window, check **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, select the **Internet** page.
7. Check the **Allow an existing internet connections for service** box.
8. If you are using an SSL proxy, check the **Use SSL proxy** box.
9. If you are using an SSL proxy, fill in the proxy's address and port. Obtain this information from the network administrator.
10. If you checked **Use SSL proxy** and the proxy requires user ID and password authentication, check the **Authenticate with the SSL proxy** box. Type the userid and password. Obtain the user ID and password from the network administrator.
11. Select the **Protocol to Internet** you want to use.
12. On the **Internet** page, click **Test**.
13. In the Test Internet window, click **Start**.
14. Verify that the test completes successfully.
15. In the Test Internet window, click **Cancel**.
16. In the Outbound Connectivity Settings window, click **OK**.

Connecting to service and support using the telephone and modems:

Describes how to configure the HMC as a call-home server using modem access to IBM support.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

Before you begin this task, ensure that:

- You have an dedicated analog telephone line available.
- You have the information required to configure the modem. For more information, see “Preparing for HMC configuration” on page 81.
- Customer contact information has been configured. You may verify this by going to the HMC interface and clicking **Service Management > Manage Customer Information**.
- Ensure you have the following information available:
 - The type of analog line; that is, tone or pulse. Most lines are tone, but some are in use that are the older rotary or pulse type.
 - Whether the line presents a dial tone when the telephone is picked up. Most telephones do, but some are in use that do not.
 - Whether a dial prefix string is required. A dial prefix string is a number or series of numbers that allow access to an outside line.

To configure the HMC as a call-home server using modem access to IBM support, do the following:

1. In the navigation area, click **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**.
3. Click **Configure**
4. In the Outbound Connectivity Settings window, select **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, click the **Local Modem** tab.
7. On the Local Modem page, select the **Allow local modem dial for service** checkbox.
8. On the Local Modem page, select the **Modem Configuration** checkbox.

9. In the Customize Modem Settings window, click **Dial type, Tone or Pulse**. If the line presents a dial tone when the receiver is taken off the hook, select the **Wait for dial tone** checkbox. Fill in any dial prefix string that is required to obtain an outside line.
10. Click **OK**.
11. On the Local Modem page, click **Add**.
12. Select a number from the list.
13. If this is a local number, remove the area code from the **Telephone number** field.
14. In the Add Telephone Number panel, click **Add**.
15. In the In the Customize Modem Settings panel, click **Test**.
16. In the Test Telephone Number panel, click **Start**.
17. Verify that the test completes successfully.
18. In the Test Telephone Number window, click **Cancel**.
19. You can configure up to five telephone numbers. Configure at least two telephone numbers (a primary and a backup). The numbers will be attempted in the order that they are configured. To add additional numbers to the callable list, repeat the steps in this procedure.
20. In the Outbound Connectivity Settings window, click **OK**.

Connecting to service and support using a LAN-based VPN:

Configure the call-home server using VPN.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- The adapter designated as **eth1** (the one that is designated as an open network) is used. For more information, see “Choosing network settings on the HMC” on page 72.
- An Ethernet cable physically connects the HMC to the LAN.
- Customer contact information has been configured. Verify this situation by clicking **Service Management > Manage Customer Information** on the HMC interface.

To configure the call-home server using VPN, do the following:

1. In the navigation area, click **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**.
3. Click **Configure**
4. In the Outbound Connectivity Settings window, select **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, click the **Internet VPN** tab.
7. On the Internet VPN page, select the **Allow A VPN and an existing Internet connections for service**.
8. On the Internet VPN page, click **Test** checkbox.
9. In the Test Internet VPN window, click **Start**.
10. Verify that the test completes successfully.
11. In the Test Internet VPN window, click **Cancel**.
12. In the Outbound Connectivity Settings window, click **OK**.

Choosing existing call-home servers to connect to service and support for this HMC:

Choose existing HMC call-home servers that have been recognized, or "discovered" by this HMC to report errors.

Discovered HMCs are HMCs that are enabled as call-home servers and are either on the same subnet or manage the same managed system as this HMC.

To choose a discovered HMC to call home when this HMC reports errors, do the following:

1. In the navigation area, click **Service Management**.
2. In the content area, click **Manage Outbound Connectivity**. The Call-Home Server Consoles window opens.
3. Click the **Use discovered call-home server consoles** . The HMC displays the IP address or host name of the HMCs configured for call-home.
4. Click **OK**.

You can also manually add existing HMC call-home servers that are on a different subnet. Select the IP address or host name of the HMC that is configured for call home and click **Add**. Then click **OK**.

Verifying that your connection to service and support is working:

Test problem reporting to ensure that connection to service and support is working.

To verify that your call-home configuration is working, do the following:

1. In the navigation area, click **Service Management**.
2. In the Work area, click **Create Event**.
3. select **Test Automatic problem Reporting** and type a comment.
4. Click **Request Service**. Wait a few minutes for the request to be sent.
5. In the Service Management window, select **Manage Events**.
6. Select **All open problems**.
7. Verify that there is a PMH event and number assigned to the problem number you opened.
8. select that event and select **Close**.
9. On the Close window, type your name and a brief comment.

Authorizing users to view collected system data:

You must authorize users to view data about your systems.

Before you authorize users to view collected system data, you must obtain an IBM ID. For more information about obtaining an IBM ID, see "Preinstallation configuration worksheet for the HMC" on page 83.

To authorize users to view collected system data, do the following:

1. In the navigation area, select **Service Management**.
2. In the content area, select **Authorize User**.
3. Enter your IBM ID.
4. Click **OK**.

Transmit service information:

Transmit service information so that it can be used for problem determination.

IBM provides personalized Web functions that use information collected by IBM Electronic Service Agent. To use these functions, you must first register on the IBM Registration website at <http://www.ibm.com/account/profile>. To authorize users to use the Electronic Service Agent information to personalize the Web functions, see “Authorizing users to view collected system data” on page 105. For more information about the benefits of registering an IBM ID with your systems, see <http://www.ibm.com/support/electronic>.

Note: You should transmit service provider information as soon as the HMC is installed and configured for use.

To transmit service information, complete the following steps:

1. In the navigation area, click **Service Management**.
2. In the content area, click **Transmit Service Information**.
3. Click one of the following tabs:
 - **Transmit.** Use this page to schedule when to transmit service data to your service provider (specifying frequency in days and time of day) and how you want to transmit the service and performance management information.
 - **FTP.** Use this page to configure the File Transfer Protocol (FTP) information for the FTP server, with or without a firewall, for off loading a copy of the service information. The service information contains extended error data that consists of problem related-data that are opened on the Hardware Management Console (HMC) for the HMC or managed system. The HMC auto-fills the FTP panel. This FTP panel is not used for uploading data to IBM.
 - **Transmit Service Data to IBM.** Use this page to provide the ability to send information that is stored on the HMC hard disk that can be used for problem determination. The data may be traces, logs, or dumps and the destination for the data may be the IBM Service Support System, a diskette, USB flash memory drive, or a DVD-RAM. Before you can send information to the IBM Service Support System, Phone Server and Remote Service must be enabled.
4. Complete the tasks in the Transmit Service Information window, and click **OK**.

Configuring the Events Manager for Call Home:

Learn how to configure the Events Manager for Call Home task. You can monitor and approve any data that is being transmitted from an HMC to IBM through this task.

The Events Manager for Call Home mode (enabled or disabled) is set by using the HMC command-line interface. Enabling the Events Manager for Call Home task blocks the HMC from automatically calling home events as they occur. To prevent events that are called home without approval, all HMCs running in this environment must have the Events Manager for Call Home enabled.

To enable or disable the Events Manager for Call Home task, run the following command:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

Note: Enabling the Events Manager for Call Home task holds call home events until they have been approved for the call home task. If you disable the Events Manager for Call Home task, it does not automatically enable the call home feature. This setup prevents any unintended call home of data back to IBM. Choose from the following command options to set up the required configuration:

- To enable the Events Manager for Call Home task: **chhmc -c emch -s enable**

- To disable the Events Manager for Call Home task and to re-enable automatic call home: **chhmc -c emch -s disable --callhome enable**
- To disable the Events Manager for Call Home task and not re-enable automatic call home: **chhmc -c emch -s disable --callhome disable**

Ensure that the HMC can communicate with other HMCs deployed in this environment. The Events Manager for Call Home has a test connection function when an HMC is registered.

You can register the HMC with the Events Manager for Call Home. After you register the HMC, the events manager queries the registered HMC for any events that are waiting to be called home to IBM. The Events Manager shows what data is being sent back to IBM and approves these events. After approval, the Event Manager notifies the registered HMC that it can proceed with the call home operation.

The Events Manager for Call Home task can be run from any HMC or from multiple HMCs. To register a management console with the Events Manager for Call Home task, complete the following steps:

1. In the navigation area, select **Service Management**.
2. In the contents area, select **Events Manager for Call Home**.
3. From the **Events Manager for Call Home** window, click **Manage Consoles**.
4. From the **Manage Registered Consoles** window, click **Add Console** to enter information to register a management console with the Events Manager for Call Home task.
5. Click **OK** to commit the changes to the list of registered management console.

Note: The Events Manager for Call Home can be used with the event manager mode disabled. You can still register the HMC and view events in the events manager, but Events Manager does not control when the events are called home.

Setting passwords for the managed system:

You must set passwords for both your server and Advanced System Management (ASM). Read more about how to use the HMC interface to set these passwords.

If you received the message Authentication Pending, the HMC prompts you to set the passwords for the managed system.

If you did not receive the message Authentication Pending, complete the following steps to set the passwords for the managed system.

Updating your server password:

To update your server password, do the following:

1. In the navigation area, select the managed system.
2. In the Tasks area, click **Operations**.
3. Click **Change Password**. The Update Password window opens.
4. Type the required information and click **OK**.

Updating your Advanced System Management (ASM) general password:

Note: The default password for the general user ID is general, and the default password for the administrator ID is admin.

To update your ASM general password, do the following:

1. In the navigation area of the HMC, select the managed system.
2. In the Tasks area, click **Operations**.

3. Click **Advanced System Management (ASM)**. The Launch ASM Interface window opens.
4. Select a Service Processor IP Address and click **OK**. The ASM interface opens.
5. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
6. In the navigation area, expand **Login Profile**.
7. Select **Change Password**.
8. Specify the required information, and click **Continue**.

Resetting the Advanced System Management (ASM) administrator password:

To reset the administrator password, contact an authorized service provider.

Testing the connection between the HMC and the managed system:

This option enables you to verify that you are properly connected to the network.

To test network connectivity, you must be a member of one of the following roles:

- Super administrator
- Service representative

To test the connection between the HMC and the managed system, do the following:

1. In the navigation area, click **HMC Management**.
2. Click **Test Network Connectivity**.
3. In the Ping tab, type the host name or IP address of any system to which you want to connect. To test an open network, type the gateway. Click **Ping**.

If you have not yet created any logical partitions, you will not be able to ping the addresses. You can use the HMC to create logical partitions on your server. For more information, see Logical partitioning.

To understand how the HMC can be used in a network, see “HMC network connections” on page 72.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC by using the HMC menus” on page 91.

Postconfiguration steps

After you have installed and configured the HMC, back up HMC data as necessary.

Backing up critical HMC data

You can back up important console information to a USB Flash Memory Device, a remote system mounted to the HMC file system (such as Network File System (NFS)), or a remote site by using File Transfer Protocol (FTP).

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

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

The Backup function saves the HMC data stored on the HMC hard disk to the following:

- USB Flash Memory Device
- Remote system mounted to the HMC file system (such as NFS)
- Remote site through FTP

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

Note: Before data can be saved to removable media, the media must be formatted. To format media, click **HMC Management > Format Media** and follow the steps.

To back up the HMC, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

To back up the HMC critical data, do the following:

1. In the navigation area, click **HMC Management**.
2. Select **Back up HMC Data**.
3. Select an archive option. You can back up to media on the local system, back up to a mounted remote system, or send backup data to a remote site.
4. Follow the instructions on the window to back up the data.

Backing up the entire HMC hard disk drive to a remote system

You can use your HMC to back up the entire hard disk drive of your HMC to a remote system.

Your remote system must have Network File System (NFS) or Secure Shell (ssh) configured, and this network must be accessible from the HMC. To complete this task, you must shut down and reboot the HMC. Use only the HMC to perform these tasks.

To back up the HMC hard disk drive to a remote system, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

To back up the HMC hard drive to a remote system, do the following:

1. Record the interface number (eth0, eth1, etc), MAC address and IP address of each of the network adapters on the HMC. To do this, click **HMC Management > Change Network Settings > LAN Adapters**.
2. Shut down and power off the HMC.
3. Power on the HMC console with the HMC recovery media in the DVD drive. If you want to start the HMC interface from a configured network boot server, make sure the network interface is one of the devices in your startup sequence. To view the list of startup devices, press F12 when the HMC powers on, and select the network interface from which you want to boot.
4. Select the backup option and click **Next**.
5. Select the network interface to use for communicating with the remote server. If you are starting the HMC by contacting a network boot server, and this server is also the remote server to which you want to back up the data, then select the default settings. Then click **Next** and go to step 7. If you do not select the default settings, continue with the next step.

Note: The interface numbering (eth0, eth1) may not match the numbering recorded in Step 1. The MAC address listed can be used to identify the desired interface. For more information, see “Identifying the Ethernet port defined as eth0” on page 95.

6. If you do not select the Default settings, you must select the network Protocol to use with the selected interface. You can choose to obtain an IP address from a DHCP server in your network or assign a static IP address to the selected network interface. Make your selection and click **Next**.

7. If you did not select the default settings, type the IP address or host name of your remote server. The backup file will be created using the gzip compression utility and the **tar** command. Specify a file with the .tgz extension in the **File on remote host** field. If you have selected the default network settings, you must use the directory setup in your network boot configuration. This information is displayed in the **File on remote host** field. After you have completed all the required information, click **Next**.
8. Select the method you want to use to transfer the data from your HMC to the remote server. If you choose to encrypt the data, your remote host must have Secure Shell (SSH) server running. If you choose to transfer the data without encryption, your remote host must have Network File Server (NFS) running, and the directory to which you want to back up data must be exported for write access. Make your selection and click **Next**.
9. If you select to transfer the data using encryption, you must type the remote server's user ID and password.
10. Verify the information you entered is correct and click **Finish**. When the backup completes, the HMC interface is displayed.

If you have modified the startup sequence by pressing F1 when you powered on the HMC, you must reboot the HMC and change the settings again. When you change the startup sequence, ensure that your hard disk is listed in the startup sequence before the network interface.

Updating, upgrading, and migrating your HMC machine code

Updates and upgrades are periodically released for the HMC to add new functionality and to improve existing features. Learn more about the differences between updating, upgrading, and migrating your HMC machine code. Also learn how to perform an HMC machine code update, upgrade, or migration.

When you are finished with each of these tasks, the HMC reboots but the partitions do not.

Updating HMC code

Applies maintenance to an existing HMC level

Does not require that you perform the **Save upgrade data** task

Upgrading HMC code

Replaces HMC software with a new release or fix level of the same program

Requires that you boot from recovery media

Migrating HMC code

Moves HMC data from one HMC version to another

A migration is a type of upgrade.

Determining your HMC machine code version and release

Find out how to view the HMC machine code version and release.

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

To view the HMC machine code version and release, do the following:

1. In the navigation area, click **Updates**.
2. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.

Obtaining and applying machine code updates for the HMC with an Internet connection

Learn how to obtain machine code updates for the HMC when the HMC has an Internet connection.

To obtain machine code updates for the HMC, perform steps 1 through 5.

Step 1. Ensure that you have an Internet connection:

To download updates from the service and support system or website to your HMC or server, you must have one of the following:

- SSL connectivity with or without a SSL proxy
- Internet VPN

To ensure that you have an Internet connection, do the following:

1. In the navigation area, click **Service Management**.
2. Select **Manage Outbound Connectivity**.
3. Select the tab for the type of outbound connectivity that you chose for your HMC (Internet VPN or SSL connectivity).

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see *Setting up your server to connect to IBM service and support*.

4. Click **Test**.
5. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on DVD.
6. Continue with “Step 2. View the existing HMC machine code level.”

Step 2. View the existing HMC machine code level:

To view the existing HMC machine code level, do the following:

1. In the navigation area, click **Updates**.
2. In the Work area, view and record the information that appears under the HMC Code Level heading, including the HMC version, release, maintenance level, build level, and base versions.
3. Continue with “Step 3. View the available HMC machine code levels.”

Step 3. View the available HMC machine code levels:

To view the available HMC machine code levels, do the following:

1. From a computer or server with an Internet connection, go to <http://www.ibm.com/eserver/support/fixes>.
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact service and support.

6. Continue with “Step 4. Apply the HMC machine code update.”

Step 4. Apply the HMC machine code update:

To apply the HMC machine code update, do the following:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see “Backing up critical HMC data” on page 108. Then continue with the next step.

2. In the navigation area, click **Updates**.
3. Click **Update HMC**. The Install Corrective Service Wizard opens.
4. Follow the instructions in the Wizard to install the update.
5. Shut down and then restart the HMC for the update to take effect.
6. Click **Log on and launch the Hardware Management Console web application**.
7. Log in to the HMC interface.

Step 5. Verify that the HMC machine code update installed successfully:

To verify that the HMC machine code update installed correctly, do the following:

1. In the navigation area, click **Updates**.
2. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
3. Verify that the version and release match the update that you installed.
4. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. select the network connection on the HMC.
 - b. Retry the firmware update using a different repository.
 - c. If the problem persists, contact your next level of support.

Obtaining and applying machine code updates for the HMC using DVD or an FTP server

Learn how to obtain machine code updates for the HMC using DVD or an FTP server.

To obtain HMC machine code updates, perform steps 1-5.

Step 1. View the existing HMC machine code level:

To view the existing HMC machine code level, do the following:

1. In the navigation area, click **Updates**.
2. In the Work area, view and record the information that appears under the HMC Code Level heading, including the HMC version, release, maintenance level, build level, and base versions.
3. Continue with “Step 2. View the available HMC machine code levels.”

Step 2. View the available HMC machine code levels:

To view the available HMC machine code levels, do the following:

1. From a computer or server with an Internet connection, go to the Hardware Management Console Web site at <http://www-933.ibm.com/support/fixcentral/>.
2. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact IBM service and support.

3. Continue with “Step 3. Obtain the HMC machine code update.”

Step 3. Obtain the HMC machine code update:

To obtain the HMC machine code update, do the following:

You can order the HMC machine code update through the Fix Central website, contact service and support, or download it to an FTP server.

Ordering the HMC machine code update through the Fix Central Web site

1. From a computer or server with an Internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>
2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File name(s) / Package area and locate the update you want to order.

4. In the Order column, select **Go**.
5. Click **Continue** to sign in with your IBM ID.
6. Follow the on-screen prompts to submit your order.

Downloading the HMC machine code update to removable media

1. From a computer or server with an Internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>
2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File name(s) / Package area and locate the update you want to download.
4. Click the update you want to download.
5. Accept the license agreement, and save the update to your removable media.

When you are finished, continue with “Step 4. Apply the HMC machine code update.”

Step 4. Apply the HMC machine code update:

To apply the HMC machine code update, do the following:

1. Before you install updates to the HMC machine code, back up HMC data. For more information, see “Backing up critical HMC data” on page 108
2. If you obtained or created the update on DVD-RAM, insert it into the DVD drive on the HMC. If you obtained or created the update on a USB memory device, insert the memory device.
3. In the navigation area, click **Updates**.
4. Click **Update HMC**. The Install HMC Corrective Service Wizard opens.
5. Follow the instructions in the Wizard to install the update.
6. Shut down, restart, and log back in to the HMC for the update to take effect.
7. Continue with “Step 5. Verify that the HMC machine code update installed successfully.”

Step 5. Verify that the HMC machine code update installed successfully:

To verify that the HMC machine code update installed successfully, do the following:

1. In the navigation area, click **Updates**. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
2. Verify that the version and release match the update that you installed.
3. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Retry the machine code update. If you created a DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Upgrading your HMC software

Learn how to upgrade the software on an HMC from one release to the next while maintaining your HMC configuration data.

To upgrade machine code on an HMC, perform steps 1-9.

Step 1. Obtain the upgrade:

You can order the HMC machine code upgrade through the Fix Central website.

To obtain the upgrade through the Fix Central website, do the following:

1. From a computer or server with an Internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>.
2. Click **Continue**. The Hardware Management Console site is displayed.
3. Navigate to the HMC version you want to upgrade to.
4. Locate the download and ordering section.

Note: If you do not have access to the Internet, contact IBM service and support to order the upgrade on DVD.

5. Follow the on-screen prompts to submit your order.
6. After you have the upgrade, continue with “Step 2. View the existing HMC machine code level.”

Step 2. View the existing HMC machine code level:

To determine the existing level of machine code on an HMC, follow these steps:

1. In the navigation area, click **Updates**.
2. In the Work area, view and record the information that appears under the HMC Code Level heading, including the HMC version, release, maintenance level, build level, and base versions.
3. Continue with “Step 3. Back up the managed system's profile data.”

Step 3. Back up the managed system's profile data:

To back up the managed system's profile data, do the following:

1. In the navigation area, select **Systems Management**.
2. Select **Servers**.
3. Select the server and ensure the state is *Operating* or *Standby*.
4. Under Tasks, select **Configuration > Manage Partition Data > Backup**.
5. Type a backup file name and record this information.
6. Click **OK**.
7. Repeat these steps for each managed system.
8. Continue with “Step 4. Back up HMC data.”

Step 4. Back up HMC data:

Back up HMC data before installing a new version of HMC software so that previous levels can be restored in the event of a problem while upgrading the software. Do not use this critical console data after a successful upgrade to a new version of the HMC software.

Note: To back up to removable media, you will need to have that media available.

To back up HMC data, do the following:

1. If you plan to back up to media, perform the following steps to format the media:
 - a. Insert the media into the drive.
 - b. In the navigation area, select **Service Management**
 - c. Select **Format Media**.
 - d. Select the media type.
 - e. Select the format type.
 - f. Click **OK**.
2. In the navigation area, select **HMC Management**.
3. Select **Back up HMC Data**. The Back up HMC Data window opens.
4. Select an archive option. You can back up to media on a local system, a remote system mounted to the HMC file system (for example, NFS), or send the backup to a remote site using File Transfer Protocol (FTP).
 - To back up to a local system, choose **Back up to media on local system** and follow the instructions.
 - To back up to a mounted remote system, choose **Back up to mounted remote system** and follow the instructions.
 - To back up to a remote FTP site, choose **Send back up critical data to remote site** and follow the instructions.

5. Continue with “Step 5. Record the current HMC configuration information.”

Step 5. Record the current HMC configuration information:

Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information.

To record the current HMC configuration, do the following:

1. To view scheduled operations for a managed system or its logical partitions, open **Systems Management**. If you want to record scheduled operations for the HMC itself, select **HMC Management** and skip to step 3.
2. Select a managed system and any partitions for which you want to record HMC configuration information.
3. In the tasks list, select **Schedule Operations**. All scheduled operations for the target you selected are displayed.
4. Select **Sort > By Object**.
5. Select each object and record the following details:
 - Object Name
 - Schedule date
 - Operation Time (displayed in 24-hour format)
 - Repetitive (if Yes, perform the following steps):
 - a. Select **View > Schedule Details**.
 - b. Record the interval information.
 - c. Close the scheduled operations window.
 - d. Repeat for each scheduled operation.
6. Close the Customize Scheduled Operations window.
7. Continue with “Step 6. Record remote command status.”

Step 6. Record remote command status:

To record remote command status, do the following:

1. In the navigation area, select **HMC Management**.
2. In the tasks list, click **Remote Command Execution**.
3. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
4. Click **Cancel**.
5. Continue with “Step 7. Save upgrade data.”

Step 7. Save upgrade data:

You can save the current HMC configuration in a designated disk partition on the HMC or to local media. Save upgrade data only immediately prior to upgrading your HMC software to a new release. This action allows you to restore HMC configuration settings after upgrading.

Note: Only one level of backup data is allowed. Each time you save upgrade data, the previous level is overwritten.

To save upgrade data, do the following:

1. In the navigation area, select **HMC Management**.
2. In the content area under Operations, select **Save Upgrade Data**. The Save Upgrade Data Wizard opens.
3. Select the media on which you want to save the upgrade data. If you choose to save to removable media, insert the media now. Click **Next**.
4. Click **Finish**.

5. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

Note: If the save upgrade data task fails, do not continue the upgrade process.

6. Click **OK**.
7. Continue with “Step 8. Upgrade the HMC software.”

Step 8. Upgrade the HMC software:

To upgrade the HMC software, restart the system with the removable media in the DVD drive.

1. Insert the HMC Product Installation media into the DVD drive.
2. In the navigation bar, select **HMC Management**.
3. In the content area, select **Shutdown or Restart HMC**.
4. Ensure **Restart the HMC** is selected.
5. Click **OK**. The HMC restarts and system information scrolls on the window.
6. Select **Upgrade** and click **Next**.
7. Choose from the following options:
 - If you have saved upgrade data during the previous task, continue with the next step.
 - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue.
8. Select **Upgrade from media** and click **Next**.
9. Confirm the settings and click **Finish**.
10. Follow the prompts.

Note:

- If the screen goes blank, press the space bar to view the information.
 - The first DVD can take approximately 20 minutes to install.
11. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
 12. Continue with “Step 9. Verify that the HMC machine code upgrade installed successfully.”

Step 9. Verify that the HMC machine code upgrade installed successfully:

To verify that the HMC upgrade installed successfully, do the following:

1. In the navigation area, click **Updates**. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
2. Verify that the version and release match the update that you installed.
3. If the level of code displayed is not the level that you installed, retry the upgrade task using a new DVD. If the problem persists, contact your next level of support.

Upgrading HMC from remote location using network upgrade images

Learn how to upgrade the software on an HMC from a remote location using network upgrade images.

Learn how to upgrade the software on an HMC from a remote location using network upgrade images. Use the following procedure to upgrade HMC at level V6R1.2 or higher, which includes all HMC V7 levels.

1. From a computer or server with an Internet connection, go to the Hardware Management Console website (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. Download the appropriate HMC V7 network images and save them on an FTP server. You cannot download these files directly to the HMC. You must download the image files to a server that accepts FTP requests.
3. Ensure that you download the following files:

- img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. Save the upgrade data on the HMC. Execute the following command lines to save the upgrade data:
 - To save data on both DVD and HDD, execute the following commands:


```
mount /media/cdrom
saveupgdata -r diskdvd
```
 - To save data on the HDD, execute the following command:


```
saveupgdata -r disk
```
 5. Copy the upgrade files to the bootable disk partition on the HMC. Run the **getupgfiles** command to copy the files.

Example: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**

Where,

 - **ftp server** is the host name or ip address of the FTP server where you have downloaded the HMC network images.
 - **user id** is a valid user id on the FTP server. If you do not specify the password with the `--passwd` argument, you will be prompted for a password.
 - **remote directory** is the directory on your FTP server where the HMC network images are saved.
 6. Reboot the HMC to upgrade the code copied to the bootable disk partition. Run the **chhmc -c altdiskboot -s enable --mode upgrade** to reboot the HMC.
 7. Reboot the HMC and start the upgrade. Run the **hmcshutdown -r -t now** command to start the upgrade.

Configuring the HMC by using the HMC Enhanced+ interface

Learn how to set up your network connections, configure your HMC, perform postconfiguration steps, and upgrade and update your HMC by using the HMC Enhanced+ interface.

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

Choosing network settings on the HMC

Learn about the network settings you can use on the HMC.

HMC network connections

You can use different types of network connections to connect your HMC to managed systems. For more information about how to configure the HMC to connect to a network, see “Configuring the HMC” on page 89. For more information about using the HMC on a network, see the following:

Types of HMC network connections:

Learn how to use the HMC remote management and service functions by using your network.

The HMC supports the following types of logical communications:

HMC to managed system

Used to perform most of the hardware management functions, in which HMC issues control function requests through the service processor of the managed system. The connection between

the HMC and the service processor is sometimes referred to as the *service network*. This connection is required for managed system management.

HMC to logical partition

Used to collect platform-related information (hardware error events, hardware inventory) from the operating systems that are running on logical partitions, and to coordinate certain platform activities (dynamic LPAR, concurrent repair) with those operating systems. If you want to use service and error notification features, you must create this connection.

HMC to BMC

Note: The baseboard management controller (BMC) connection is applicable only to HMC model 7063-CR1.

Used to perform service and maintenance tasks. The BMC connection is used to load and maintain the HMC firmware on the system. This connection is required for access to the BMC on the HMC.

HMC to remote users

Provides remote users with access to HMC functions. Remote users can access the HMC in the following ways:

- By using the web browser to access all the HMC GUI functions remotely.
- By using Secure Socket Shell (SSH) to access the HMC command line functions remotely.

HMC to service and support

Used to transmit data, such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communications path to make automatic service calls.

Your HMC can support up to four separate physical Ethernet interfaces, depending on the model. The stand-alone version of the HMC supports only three HMC interfaces, by using one integrated Ethernet adapter and up to two plug-in adapters. Use each of these interfaces in the following ways:

- One or more network interfaces can be used exclusively for HMC-to-managed system communications, which means that only the HMC and service processors of the managed systems are on that network. Even though the network interfaces into the service processors are encrypted for the Secure Sockets Layer (SSL) Protocol and password-protected, having a separate dedicated network can provide a higher level of security for these interfaces.
- An open network interface would typically be used for the network connection between the HMC and the logical partitions on the managed systems, for the HMC-to-logical partition communications. You can also use this open network interface to manage the HMC remotely.
- Optionally, you can use a third interface to connect to logical partitions and manage the HMC remotely. This interface can also be used as a separate HMC connection to different groups of logical partitions. For example, you might want to have an administrative LAN that is separate from the LAN on which all the usual business transactions are running. Remote administrators can access the HMC and other managed units by using this method. Sometimes the logical partitions are in different Network security domains, perhaps behind a firewall, and you might want to have different HMC network connections into each of those two domains.

Web browser requirements for HMC

The Hardware Management Console (HMC) version 8.7.0 is supported by Google Chrome version 57, Microsoft Internet Explorer (IE) version 11.0, Mozilla Firefox versions 45 and 52 Extended Support Release (ESR), and Safari version 10.1.

If your browser is configured to use an Internet proxy, a local IP addresses should be included in the exception list. Consult your network administrator for more information on the exception list. If you still need to use the proxy to get to the HMC, enable Use HTTP 1.1 through proxy connections under the Advanced tab in your Internet Options window.

Session cookies need to be enabled in order for ASMI to work when connected to HMC remotely. The asm proxy code saves session information and uses it. Follow the steps to enable the session cookies.

Enabling session cookies in Internet Explorer.

1. Select Tools and Click Internet Options.
2. Select Privacy and Click Advanced.
3. Ensure that the Always allow session cookies is checked. If not, select the Override automatic cookie handling and select Always allow session cookies.
4. Select Prompt under First-party Cookies and Third-party Cookies.
5. Click OK.

Enabling session cookies in Chrome.

1. Click Settings and then click Advanced.
2. From the Privacy and security section, click Content settings.
3. Click Cookies. Enable Allow sites to save and read cookie data.
4. Exit from the settings menu.

Enabling session cookies in Firefox.

1. Select Tools and click Options.
2. Click Cookies.
3. Select Allow sites to set cookies.
4. Select Exceptions and add HMC.
5. Click OK.

Enabling session cookies in Safari.

1. Click Safari and then click Preferences.
2. Click Privacy.
3. Click Cookies. Enable Allow sites to save and read cookie data.
4. Set the option Block cookies to Never.
5. Exit from the preferences menu.

Private and open networks in the HMC environment:

The HMC can be configured to use open and private networks. Private networks allow the use of a selected range of nonroutable IP-addresses. A *public*, or "open" network describes a network connection between the HMC to any logical partitions and to other systems on your regular network.

Private networks

The only devices on the HMC private network are the HMC itself and each of the managed systems to which that HMC is connected. The HMC is connected to each managed system's FSP (Flexible Service Processor).

On most systems, the FSP provides two Ethernet ports labeled **HMC1** and **HMC2**. This allows you to connect up to two HMCs.

Some systems have a dual-FSP option. In this situation, the second FSP acts as a "redundant" backup. The basic setup requirements for a system with two FSPs are essentially the same as those without a second FSP. The HMC must be connected to each FSP, so additional network hardware is required (for example, a LAN switch or hub) when there is more than one FSP or there are multiple managed systems.

Note: Each FSP port on the managed system must be connected to only one HMC.

Public networks

The open network can be connected to a firewall or router for connecting to the Internet. Connecting to the Internet allows the HMC to "call home" when there are any hardware errors that need to be reported.

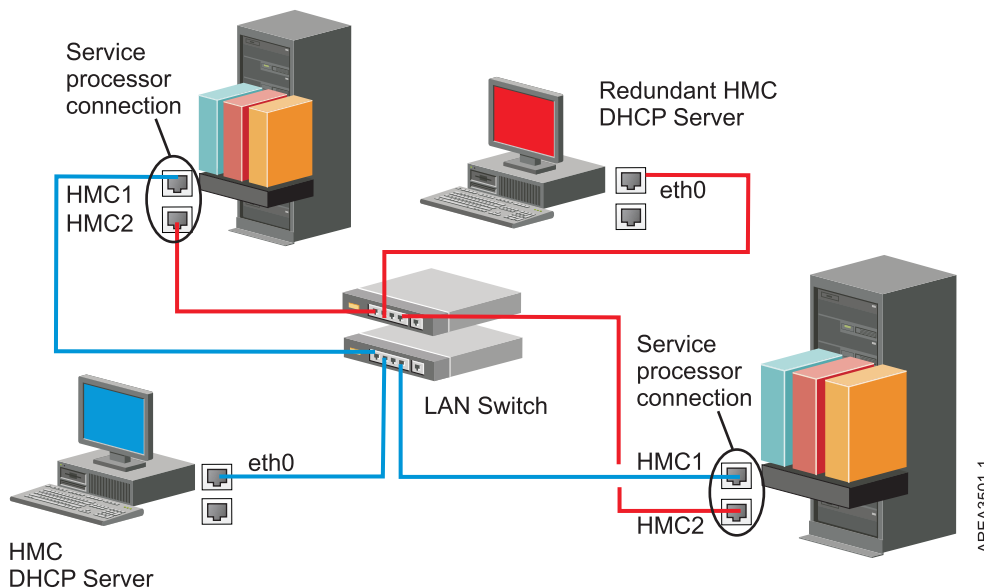
The HMC itself provides its own firewall on each of its network interfaces. A basic firewall is automatically configured when you run the HMC Guided Setup wizard, but you customize your firewall settings after the initial HMC installation and configuration.

HMC as a DHCP server:

You can use the HMC as a Dynamic Host Configuration Protocol (DHCP) server.

Note: If you are using IPv6, the discovery process must be done manually. For IPv6, there is no automatic discovery.

For more information about how to configure the HMC as a DHCP server, see "Configuring the HMC as a DHCP server" on page 97.

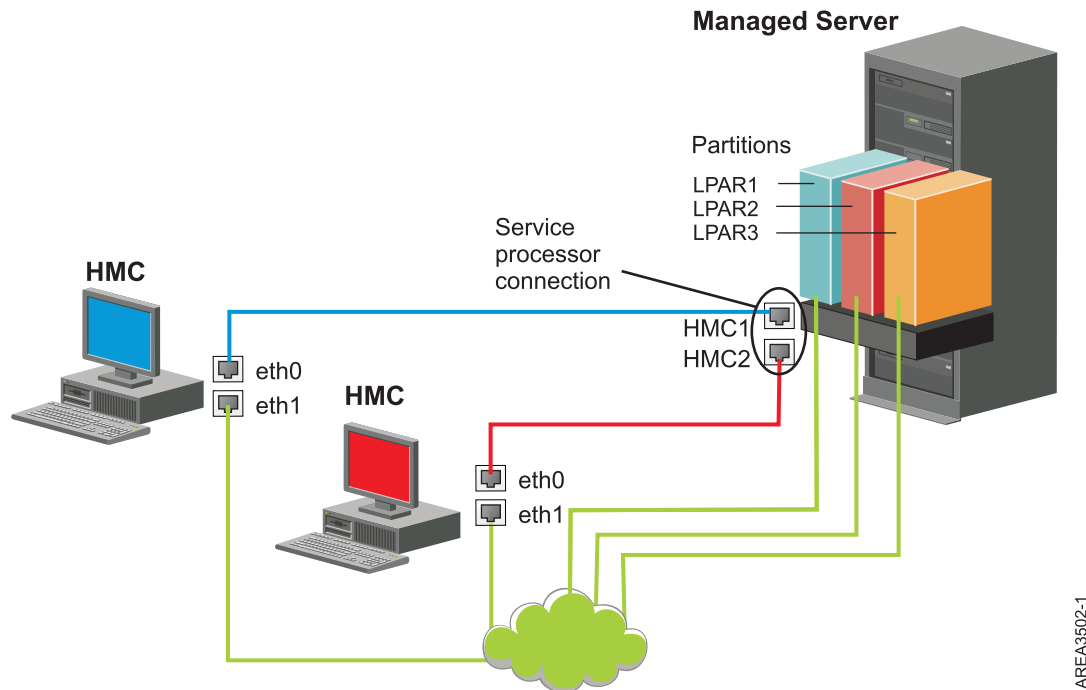


This figure shows a redundant HMC environment with two managed systems. The first HMC is connected to the first port on each FSP, and the redundant HMC is connected to the second port on each HMC. Each HMC is configured as a DHCP server, using a different range of IP addresses. The connections are on separate private networks. As such, it is important to ensure that no FSP port is connected to more than one HMC.

Each managed system's FSP port that is connected to an HMC requires a unique IP address. To ensure that each FSP has a unique IP address, use the HMC's built-in DHCP server capability. When the FSP detects the active network link, it issues a broadcast request to locate a DHCP server. When correctly configured, the HMC responds to that request by allocating one of a selected range of addresses.

If you have multiple FSPs, you must have your own LAN switch or hub for the HMC to FSP private network. Alternately, this private segment can exist as several ports in a private *virtual LAN* (VLAN) on a larger managed switch. If you have multiple private VLANs, you must ensure that they are isolated and that there is not any crossover traffic.

If you have more than one HMC, you must also connect each HMC to the logical partitions, and to each other, on the same open network.



This figure shows two HMCs connected to a single managed server on the private network and to three logical partitions on the public network. You can have an additional Ethernet adapter for the HMC to have three network interfaces. You can use this third network as a management network or connect it to the CSM (Cluster Systems Manager) Management Server.

For more information about how to configure the HMC as a DHCP server, see “Configuring the HMC as a DHCP server” on page 97.

Deciding which connectivity method to use for the call-home server:

Learn more about the connectivity options you have when you use the call-home server.

You can configure the HMC to send hardware service-related information to IBM by using a LAN-based Internet connection, or a dial-up connection over a modem.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

You have two communication choices when you configure the LAN-based Internet connection. The first choice is to use standard Secure Sockets Layer (SSL). The SSL communication can be enabled to connect to the Internet through your proxy server. SSL connectivity is more likely to be compliant with corporate security guidelines. Your second option is to use a VPN connection.

Note: If your open network interface connection uses only Internet Protocol Version 6 (IPv6), you cannot use Internet VPN to connect to support. For more information about the protocols that are used, see “Choosing an Internet Protocol” on page 79.

The advantages to using an Internet connection can include:

- Faster transmission speed
- Reduced customer expense (for example, the cost of a dedicated analog telephone line)
- Greater reliability

The following security characteristics are in effect, regardless of the connectivity method chosen:

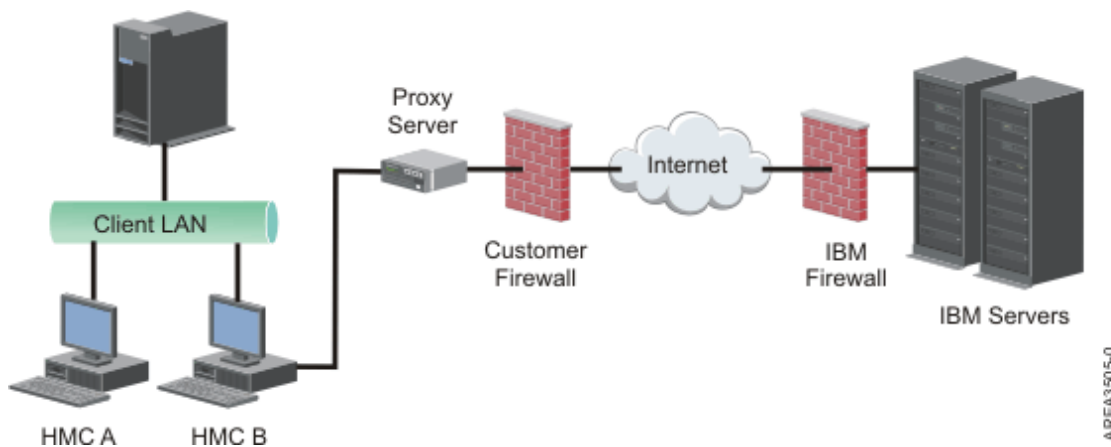
- Remote Support Facility requests are always initiated from the HMC to IBM. An inbound connection is never initiated from the IBM Service Support System.
- All data that is transferred between the HMC and the IBM Service Support System are encrypted by using a high-grade encryption. Depending upon the connectivity method that is chosen, it is encrypted by using either SSL or IPSec Encapsulating Security Payload (ESP).
- When you initialize the encrypted connection, the HMC authenticates the target destination as that of the IBM Service Support System.

Data sent to the IBM Service Support System consists solely of information about hardware problems and configuration. No application or customer data is transmitted to IBM.

Using an indirect Internet connection with a proxy server

If your installation requires the HMC to be on a private network, you might be able to connect indirectly to the Internet by using an SSL proxy, which can forward requests to the Internet. One of the other potential advantages of using an SSL proxy is that the proxy can support logging and audit facilities.

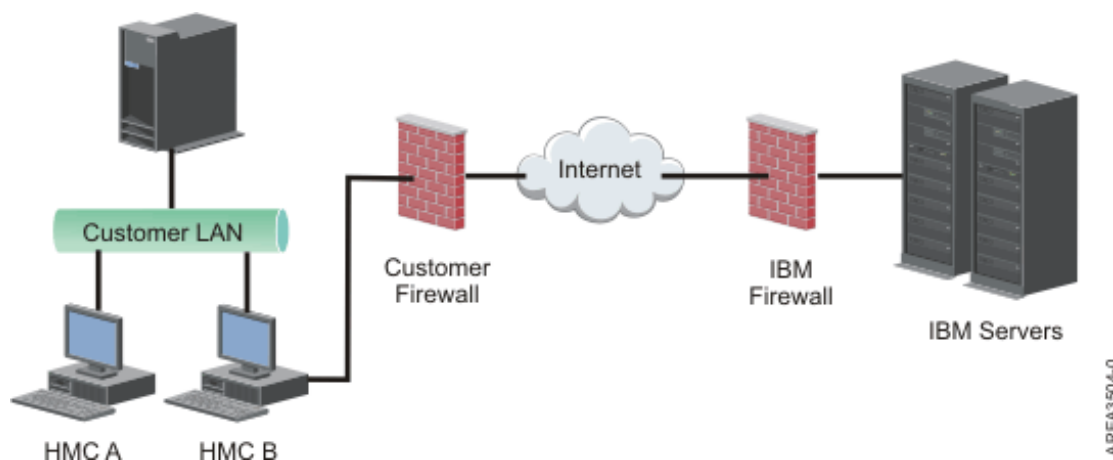
To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616) and the CONNECT method. Optionally, basic proxy authentication (RFC 2617) can be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.



For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. You can configure your proxy server to limit the specific IP addresses to which the HMC can connect. See “Internet SSL address lists” on page 79 for a list of IP addresses.

Using a direct Internet SSL connection

If your HMC can be connected to the Internet, and the external firewall can be set up to allow established TCP packets to flow outbound to the destinations described in “Internet SSL address lists” on page 79, you can use a direct Internet connection.



Using Internet SSL to connect to remote support:

All the communications are handled through TCP sockets initiated by the HMC and use a high-grade SSL to encrypt the data that is transmitted. The destination TCP/IP addresses are published (see “Internet SSL address lists” on page 79) so that external firewalls can be configured to allow these connections.

Note: The standard HTTPS port 443 is used for all communications.

The HMC can be enabled to connect directly to the Internet or to connect indirectly from a proxy server provided by the customer. The decision about which of these approaches works best for your installation depends on the security and networking requirements of your enterprise. The HMC (directly or through the SSL proxy) uses the following addresses when it is configured to use Internet SSL connectivity.

Choosing an Internet Protocol:

Determine the IP address version used when the HMC connects to your service provider.

Most users use Internet Protocol Version 4 (IPv4) to connect to a service provider. IPv4 addresses appear in the format representing the four bytes of the IPv4 address, separated by periods (for example, 9.60.12.123) to access the Internet. You can also use Internet Protocol Version 6 (IPv6) to connect to a service provider. IPv6 is often used by network administrators to ensure unique address space. If you are unsure of the Internet Protocol used by your installation, contact your network administrator. For more information about using each version, see “Setting the IPv4 address” on page 98 and “Setting the IPv6 address” on page 98.

Internet SSL address lists:

Learn about the addresses the HMC uses when it is using Internet SSL connectivity.

The HMC uses the following IPv4 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity.

The following IPv4 addresses are for all locations:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

- 170.225.15.41

The following IPv4 addresses are for the Americas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

The following IPv4 addresses are for all locations other than the Americas:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Note: When configuring a firewall to allow an HMC to connect to these servers, only the IP addresses specific to the geographic region are required.

The HMC uses the following IPv6 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity:

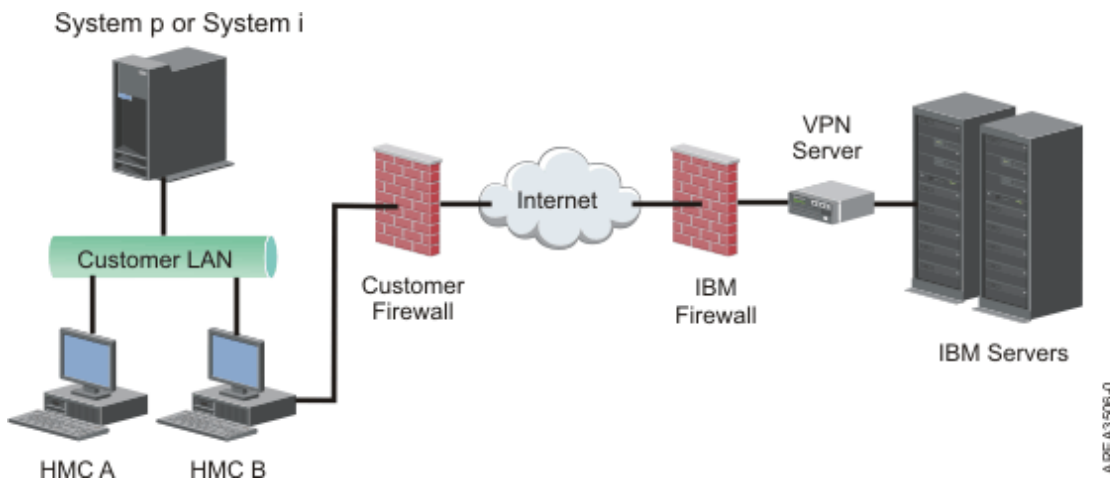
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

Using a virtual private network to connect to remote support:

A virtual private network (VPN) provides security when you connect to remote support.

Note: This connection type is available only on HMC version 8.2.0 or earlier.

A VPN gives users the privacy of a separate network over public lines by substituting encryption and other security measures for the physically separate network lines of traditional private networks. In addition to being able to be used for outbound connectivity, a VPN connection can also be configured on an as-needed basis to support remote service requests.



It is system administrator's responsibility to provide an Internet connection. The firewall can also limit the specific IP addresses to which the HMC can connect. If you need to configure your firewall to limit the IP addresses, see "VPN server address list" on page 80 for a list of addresses you can use.

For more information about how to connect to the Internet by using a LAN-based VPN, see "Configuring the HMC network types" on page 93.

VPN server address list:

Lists the servers used by an HMC when the HMC is configured to use Internet VPN connectivity.

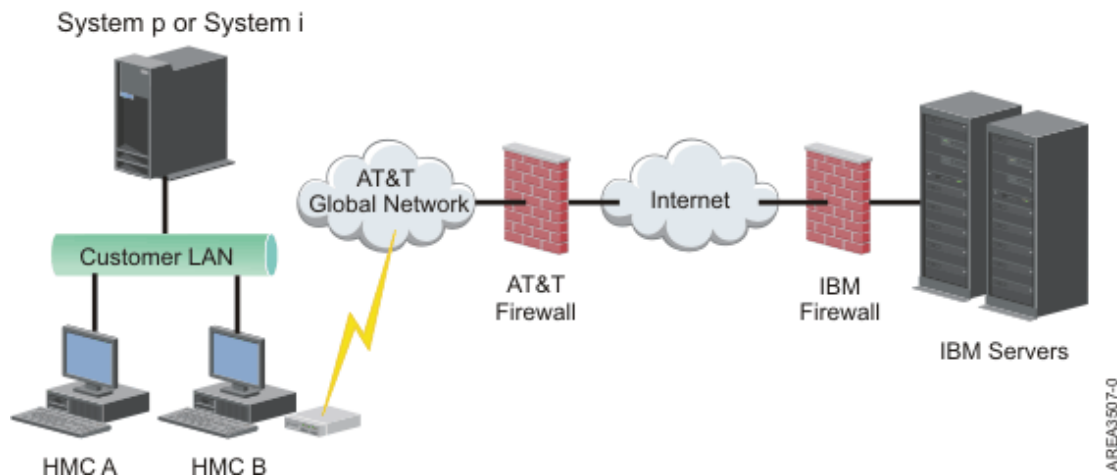
The following servers are used by an HMC when it is configured to use Internet VPN connectivity. All connections use ESP and UDP on port 500 and port 4500 when a Network Address Translation (NAT) firewall is being used.

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

Using the telephone and modems to connect to remote support:

If you want to use a modem to connect to remote support, you must provide a dedicated analog line to connect to the HMC modem. The HMC uses the modem to dial the global network and to connect to IBM service and support.

Note: This connection type is available only on HMC version 8.2.0 or earlier.



For more information about connecting to remote support by using the telephone and modems, see "Configuring the HMC network types" on page 93.

Using multiple call-home servers:

This topic describes what you need to know when you decide to use more than one call-home server.

To avoid a single point of failure, configure the HMC to use multiple call-home servers. The first available call-home server attempts to handle each service event. If the connection or transmission fails with this call-home server, the service request is retried using the other available call-home servers until one is successful or all have been tried.

The connected HMC that has been identified by problem analysis to be the primary analyzing console for a given managed system will report the problem. This primary console will also replicate the problem report to any secondary HMC. This secondary HMC must be recognized on the network by the primary HMC. A secondary HMC is recognized by the primary HMC as an additional call-home server when:

- The primary HMC is configured to use "discovered" call-home servers and the call-home server is either on the same subnet as the primary HMC or it manages the same system
- The call-home server has been manually added to the list of call-home server consoles available for outbound connectivity

Preparing for HMC configuration

Use this section to gather required configuration settings that you need to know before you begin the configuration steps.

To configure the HMC, you must understand the related concepts, make decisions and prepare information.

This section describes the information you will need to connect your HMC to the following:

- Service processors in your managed systems
- Logical partitions on those managed systems
- Remote workstations
- IBM Service, to implement "call-home" functions

Note: Additional connectivity and security information is available. For more information, see the **ESA for HMC Connectivity Security for IBM POWER6, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000** white paper available at: IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>).

To prepare for HMC configuration, complete the following steps:

1. Obtain and install the latest level of the HMC code version you want to install.
2. Determine the physical location of the HMC in relation to the servers it will manage. If the HMC is more than 25 feet from its managed system, you must provide web browser access to the HMC from the managed system's location so that service personnel can access the HMC.
3. Identify the servers that the HMC will manage.
4. Determine whether you will use a private or an open network to manage servers. If you decide to use a private network, use DHCP, unless you are using a Cluster Systems Management (CSM) configuration. CSM does not support IPv6. To access CSM, you must have two networks. For more information about CSM, see the documentation that was provided with that feature. For more information about private and open networks, see "Private and open networks in the HMC environment" on page 74.
5. If you will use an open network to manage an FSP, you must set the FSP's address manually through the Advanced System Management Interface menus. A private, non-routable network is recommended.
6. If you have two HMCs, designate a primary and secondary HMC. The primary HMC should be physically closer to the machine, and should be the HMC that is configured to call home.
7. Determine the network settings that you will need to connect the HMC to remote workstations, logical partitions, and network devices.
8. Define how the HMC will "call home." Call home options include either over an outbound-only Secure Socket Layer (SSL) Internet connection, a modem, or a Virtual Private Network (VPN) connection.
9. Determine the HMC users that you will create and their passwords, as well which roles they will be given. You must assign the hscroot and hscpe users a password.

10. Document the following company contact information that will be needed when configuring call home:
 - Company name
 - Administrator contact
 - Email address
 - Telephone numbers
 - Fax numbers
 - The street address of the HMC's physical location
11. If you plan to use email to notify operators or systems administrators when information is sent to IBM Service through call-home, identify the Simple Mail Transfer Protocol (SMTP) server and the email addresses you will use.
12. You must define the following passwords:
 - The access password that will be used to authenticate the HMC to the FSP
 - The ASMI password that will be used for the **admin** user
 - The ASMI password that will be used for the **general** user

Create the passwords when you connect from the HMC to a new server for the first time. If the HMC is a redundant or second HMC, obtain the HMC User password and be prepared to enter it when connecting the first time to the managed server's FSP.

When you have completed these preparation steps, complete the "Preinstallation configuration worksheet for the HMC" on page 83.

Preinstallation configuration worksheet for the HMC

Use this worksheet to have the installation information you need ready for the installation.

Network Settings

LAN Interface: Choose the available adapters (such as eth0, eth1) that will be used by this HMC to connect to managed systems, logical partitions, service and support, and remote users. See "HMC network connections" on page 72 for more information. Connectivity from the HMC can either be on a private or open network.

Ethernet Adapter Speed and Duplex

Enter the desired Ethernet adapter speed and duplex mode. The autodetection option determines which option is optimal if you are not sure which speed and duplex would produce optimum results for your hardware. Default = Autodetection Media speed specifies the speed in duplex mode of an Ethernet adapter. Select Autodetection unless you have a requirement to specify a fixed media speed. Any device connected to the FSP (switches/HMC), must be set to Auto (Speed) / Auto (Duplex) mode, as it is the default FSP setting and cannot be changed.

Table 36. Ethernet Adapter Speed and Duplex

	eth0	eth1	eth2	eth3
Select speed and duplex mode				
Media speed (Autodetection, 10/100/1000 Full/Half Duplex)				

For more information about private and open networks, see "Private and open networks in the HMC environment" on page 74.

Table 37. Private networks and open networks

	eth0	eth1	eth2	eth3
Specify Private or Open network for each adapter				

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration. You can specify this HMC as a DHCP server. If this is the first or only HMC on the private network, enable the HMC as a DHCP server. When you do this, the managed systems on the network will be automatically configured and discovered by the HMC.

For Ethernet adapters specified as Private networks, complete the following table:

Table 38. Private networks

	eth0	eth1
Do you want to specify this HMC as a DHCP server? (yes/no)		
If "yes," record the IP address range you want to use		

If you are using the 7063-CR1 HMC, you must connect the Ethernet **IPMI** port to a network to access the baseboard management controller (BMC) on the HMC. For more information, see “Configure BMC connectivity” on page 142. Complete the following table for your BMC connection.

Table 39. BMC connection

	IPMI
Do you want to configure this connection through DHCP mode? (yes/no)	
If no, list the specified static addresses below:	
IP address:	
Subnet mask:	
Gateway:	

For Ethernet adapters specified as *open* networks, complete the following tables. For more information about the different Internet Protocol versions, see “Choosing an Internet Protocol” on page 79.

Using IPv6

If you are using IPv6, talk to your network administrator and decide how you want to obtain IP addresses. Then, complete the following tables:

Table 40. Using IPv6

	eth0	eth1	eth2	eth3
Are you using a statically-assigned IP address? If yes, record that address here.				

Table 41. Using IPv6

	eth0	eth1	eth2	eth3
Are you getting IP addresses from a DHCP server? (Yes/No)				

Table 42. Using IPv6

	eth0	eth1	eth2	eth3
Are you getting IP addresses from an IPv6 router?				

For more information about setting IPv6 addresses, see “Setting the IPv6 address” on page 98.
 For more information about using only IPv6 addresses, see “Using only IPv6 addresses” on page 98.

Using IPv4

Complete the following tables for Ethernet adapters specified as open networks using IPv4.

Table 43. Using IPv4

	eth0	eth1	eth2	eth3
Do you want to obtain an IP address automatically? (yes/no)				
If no, list the specified address below:				
TCP/IP Interface Address:				
TCP/IP Interface Network Mask:				
Firewall Settings:				
Would you like to configure HMC firewall settings? (yes/no)				
If yes, list the applications and IP addresses that should be allowed through the firewall:				

TCP/IP Information

A unique TCP/IP address is required for each node, both for Support Element (SE) and Hardware Management Console (HMC). The assigned network mask is used to generate a unique address, by default, for the local private LAN. If the nodes will be connected into a larger network with an administered TCP/IP address, you can specify the TCP/IP address to be used. The default is generated by the system.

Firewall Settings

HMC firewall settings create a security barrier that allows or denies access to specific network applications on the HMC. You can specify these control settings individually for each physical network interface, allowing you control over which HMC network applications can be accessed on each network.

If you have configured at least one adapter as an Open network adapter, you must provide the following additional information to enable your HMC to access the LAN:

Table 44. Local host information

Local host information	
HMC host name:	
Domain name:	
Description of HMC:	
Gateway information	
Gateway Address: (nnn.nnn.nnn.nnn)	
Gateway device:	
DNS enablement	
Do you want to use DNS? (yes/no)	
If "yes", specify DNS Server Search Order below:	
1.	
2.	
Domain suffix search order:	
1.	
2.	

Local Host Information

To identify your Hardware Management Console (HMC) to the network, enter the HMC's host name and domain name. Unless you are using only short host names on your network, enter a fully qualified host name. Domain name example: name.yourcompany.com

Gateway Information

To define a default gateway, fill in the TCP/IP address to be used for routing IP packets. The gateway address informs each computer or network device when to send data if the target station is not located on the same subnet as the source.

DNS Enablement

The Domain Name System (DNS) is used to provide a standard naming convention for locating IP-based computers. By defining DNS servers, you can use host names to identify servers and Hardware Management Consoles (HMCs) rather than IP addresses.

DNS Server Search Order

Enter the IP addresses of DNS servers to be searched for mapping the host names and IP addresses. This search order is available only when DNS is enabled.

Domain Suffix Search Order

Enter the domain suffixes you are using. The HMC uses domain suffixes to append to unqualified names for DNS searches. Suffixes are searched in the order in which they are listed. This search order is available only when DNS is enabled.

Email notification

List email contact information if you wish to be notified by email when hardware problem events occur on your system.

Table 45. Email notification

Fields	
Email Addresses:	
SMTP server:	
Port:	
Errors to be notified:	
Only call-home problem events	
All problem events	

SMTP server

Type the simple mail transfer Protocol (SMTP) address of the server to be notified of a system event. An example of an SMTP server name is relay.us.ibm.com.

SMTP is the Protocol used to send email. When using SMTP, a client sends a message and communicates with the SMTP server using the SMTP Protocol.

If you do not know the SMTP address of your server or are not sure, contact your network administrator.

Port Type the port number of the server to be notified of a system event, or use the default port.

Email addresses to be notified

Enter configured email addresses to be notified when a system event occurs.

- Select **Only call-home problem events** to only receive notification when events occur that create a call-home function.
- Select **All problem events** to receive notification when any events occur.

Service Contact Information

Table 46. Service Contact Information

Service Contact Information	
Company name	
Administrator name	
Email address	
Phone number	
Alternate phone number	
Fax number	
Alternate fax number	
Street address	
Street address 2	
City or locality	
State	

Table 46. Service Contact Information (continued)

Service Contact Information	
Postal code	
Country or region	
Location of HMC (if same as above administrator address, specify "same"):	
Street address	
Street address 2	
City of locality	
State	
Postal code	
Country or region	

Service authorization and connectivity

Select the type of connection to contact your service provider. For a description of these methods including security characteristics and configuration requirements, see "Deciding which connectivity method to use for the call-home server" on page 76.

Table 47. Type of connection

Type of connection	
	Secure Sockets Layer (SSL) through the Internet
	Dialup from the local HMC
	Virtual private network (VPN) through the Internet

Secure Sockets Layer (SSL) through the Internet:

If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by using encrypted Secure Sockets Layer (SSL) using the existing Internet connection. select **Use SSL Proxy** if you want to configure the use of encrypted SSL using an indirect connection using an SSL Proxy.

Table 48. Secure Sockets Layer (SSL) through the Internet

Secure Sockets Layer (SSL) through the Internet	
Use SSL proxy? (yes/no)	
If yes, list information below:	
Address:	
Port:	
Authenticate with the SSL Proxy?	
If yes, list information below:	
User:	
Password:	

Internet connection Protocol used

For more information about the different Internet Protocols, see “Choosing an Internet Protocol” on page 79.

IPv4

IPv6

IPv4 and IPv6

Dial-up from the local HMC

Enter the dial-up information to configure your local modem. Specify which telephone numbers to use to dial your service provider. When you are connecting, the telephone numbers will be dialed in the order in which they are listed.

Table 49. Dial-up from the local HMC

Fields	
Dial prefix:	
Tone:	
Pulse:	
Wait for dial tone?	
Enable speaker?	

Virtual Private Network (VPN)

If you have an existing Internet connection from your HMC, you can use it to call your service provider. You can connect directly to your service provider by virtual private network (VPN) using the existing Internet connection.

Note: If you select Virtual Private Network (VPN) through the Internet, you will not be directed to select any other options.

Call-home servers

Determine which HMCs you want to configure to connect to service and support as call-home servers. For more information about using multiple call-home servers, see “Using multiple call-home servers” on page 81.

This HMC

Another HMC

If you checked **Another HMC**, list the other HMCs that have been configured as call-home servers here:

Table 50. Other HMCs that have been configured as call-home servers

List of HMC host names or IP addresses that have been configured as call-home servers

Additional Support Benefits

My Systems and Premium Search

Table 51. Additional Support Benefits

Fields	
List your IBM ID	
List your IBM ID	

In order to access valuable, customized support information in the My Systems and Premium Search sections of the Electronic Services website, Customers must register their IBM ID with this system. If you do not already have one, you can register for an IBM ID at: www.ibm.com/account/profile.

Note: IBM provides personalized Web functions that use information collected by the IBM Electronic Service Agent application. To use these functions, you must first register on the IBM Registration website at <http://www.ibm.com/account/profile>.

To authorize users to use the Electronic Service Agent information to personalize the Web functions, enter your IBM ID that you registered on the IBM Registration website. Go to <http://www.ibm.com/support/electronic> to see the valuable support information available to customers that register an IBM ID with their systems.

Configuring the HMC

Learn how to configure network connections, security, service applications, and some user preferences.

Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to ease the setup of the HMC. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the available settings that the wizard guides you through. You can also perform the configuration steps without the aid of the wizard by Configuring the HMC using the HMC menus.

Before you start, gather the required configuration information that you need to complete the steps successfully. See “Preparing for HMC configuration” on page 81 for a list of the required information. When you are finished preparing, ensure that you complete the “Preinstallation configuration worksheet for the HMC” on page 83 and then return to this section.

Configuring the HMC by using the fast path through the Guided Setup wizard

In most cases, the HMC can be set up to operate effectively using many of the default settings. Use this fast path checklist to prepare the HMC for service. When you have completed these steps, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

Start the HMC and complete the steps in the Guided Setup wizard:

Log in to the HMC interface and configure your HMC using the Guided Setup wizard.

Note: If this is a new installation, ensure that the managed system is not connected to a power source. For a rack-mounted HMC, this means that the only device plugged into the power distribution bus (PDB) before you plug in the main power supply is the HMC. If this is a second HMC that is connected to the same managed system, the managed system can be connected to a power source.

1. Turn on the HMC by pressing the power button.
2. Wait for the HMC to automatically select the default language and locale preference after 30 seconds.

3. Accept the Hardware Management Console license agreements. If you decline the Hardware Management Console license agreements, you cannot complete the HMC configuration.
4. Click **Log on and launch the Hardware Management Console web application**.
5. Log in to the HMC:

Note: If your system administrator (**hmcadmin**) has changed the password, enter it here.

- ID: hscroot
- Password: abc123


The Guided Setup wizard opens.

6. Click **OK** on the Guided Setup entry window.

Note: If the Guided Setup wizard did not display when you started the HMC, Click **Guided Setup Wizard** in the navigation area of the HMC welcome page.

7. Complete the steps in the Guided Setup wizard using the preinstallation configuration worksheet that you completed. Click **Yes** to continue and complete the steps in the Connectivity and Call-Home Servers wizard.
8. On the Summary window, click **Finish**.
9. If you haven't connected the Ethernet crossover cable to your managed system, do so now.



10. In the HMC navigation area, click the **Serviceability** icon  , and then select **Service Management**.
11. In the content area, click **Authorize User**. The Authorize User window opens.
12. Enter your IBM ID in the field and click **OK**.

For HMC model 7063-CR1, you must configure the baseboard management controller (BMC) IP address. For more information, see Configure BMC connectivity.

Review your configuration:

On the Status window, monitor the progress of the different configuration settings you selected. This window might show a status of Pending for some tasks for several minutes. Click **View Log** to see status messages relating to each task. Click **Close** at any time to close the Guided Setup wizard. Tasks that are still running will continue to run. Your HMC is now configured.

Configuring the HMC by using the HMC Enhanced+ interface menus

This section provides a complete list of all HMC configuration tasks, guiding you through the process of configuring your HMC. Choose this option if you prefer not to use the Guided Setup wizard.

You must restart your HMC for the configuration settings to take effect, so you might want to print this checklist and keep it with you as you configure your HMC.

This information contains references to tasks that are not included in this PDF. You can access additional support materials by referring to the **Additional Resources** section on the HMC Welcome page.

Prerequisites

Before you begin configuring the HMC using the HMC menus, be sure to complete the configuration preparation activity described in “Preparing for HMC configuration” on page 81.

Table 52. Manual HMC configuration tasks and where to find related information

Task	Where to find related information
1. Start the HMC.	"Starting the HMC"
2. Set the date and time.	
3. Change predefined passwords.	
4. Create additional users and return to this checklist when you have completed this step.	
5. Configure network connections.	"Configuring the HMC network types" on page 138
6. For HMC model 7063-CR1, you must configure the baseboard management controller (BMC) IP address.	"Configure BMC connectivity" on page 142
7. If you are using an open network and a fixed IP address, set identification information.	
8. If you are using an open network and a fixed IP address, configure a routing entry as the default gateway.	"Configuring a routing entry as the default gateway" on page 145
9. If you are using an open network and a fixed IP address, configure domain name services.	"Configuring domain name services" on page 145
10. If you are using a fixed IP address and have DNS enabled, configure domain suffixes.	"Configuring domain suffixes" on page 146
11. Configure your server to connect to IBM service and support and return to this checklist when you have completed this step.	"Configuring the local console to report errors to service and support" on page 148
12. Configure the Events Manager for Call Home.	"Configuring the Events Manager for Call Home" on page 153
13. Connect the managed system to a power source.	
14. Set passwords for the managed system, and each of the ASMI passwords (general and admin)	"Setting passwords for the managed system" on page 154
15. Access ASMI to set the date and time on the managed system.	
16. Start the managed system and return to this checklist when you have completed this step.	
17. Ensure that you have one logical partition on the managed system.	
18. Optional: add another managed system and return to this checklist when you have completed this step.	
19. Optional: If you are installing a new server with your HMC, configure the logical partitions and install the operating system.	
20. If you are not installing a new server at this time, perform optional postconfiguration tasks to further customize your configuration.	"Postconfiguration steps" on page 155

Starting the HMC:

You can log in to the Hardware Management Console (HMC) and choose which language you want to be displayed in the interface. Use the default User ID hscroot and password abc123 to log on to the HMC for the first time.

To start the HMC, complete the following steps:

1. Turn on the HMC by pressing the power button.

2. If English is your language preference, continue with step 4.
If your language preference is a language other than English, type the number **2** when you are prompted to change the locale.

Note: This prompt times out in 30 seconds if you do not act.

3. Select the locale that you want to display from the list in the Locale Selection window, and click **OK**. The locale identifies the language that the HMC interface uses.
4. Log in to the HMC with the following default user ID and password:

User name: hscroot

Password: abc123

On the login page, you can view the status of systems, partitions, and virtual I/O servers. You can also see the number of Attention LEDs and serviceable events. You can learn more about the HMC and available features by clicking the various social media and IBM developerWorks® links from the login page.

Note: On HMC Version 8.6.0.1, you can choose from the following login options:

Login: HMC Classic or HMC Enhanced+

Select the HMC Enhanced+ interface to continue. The HMC Classic interface provides access to all traditional functions of the HMC and the HMC Enhanced+ interface provides graphical views of systems, partitions, and virtual I/O servers and simplified navigation.

HMC Classic

Displays the standard GUI without the enhanced PowerVM features.

HMC Enhanced+

Displays a new view of an entirely redesigned HMC management interface that provides an intuitive interface work environment with graphical views of systems, partitions, and virtual I/O servers and simplified navigation.

Note: When the HMC is working as a DHCP server, the HMC uses the default password when it connects to the service processor for the first time.

5. Click **Sign In**.

Changing the date and time:

The battery-operated clock keeps the date and time for the HMC. You might need to reset the console date and time if the battery is replaced, or if you physically move your system to a different time zone. Learn how to change the date and time for the HMC.

If you change the date and time information, the change does not affect the systems and logical partitions that the HMC manages.

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

1. Ensure that you are a member of one of the following roles:
 - Super administrator
 - Service representative
 - Operator
 - Viewer

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

3. In the content pane, click **Change Date and Time**.
4. If you select **UTC** in the **Clock** field, the time setting will adjust automatically for daylight saving time in the time zone you select. Enter the date, time, and time zone, and click **OK**.

Configuring the HMC network types:

Configure your HMC so that it can communicate to the managed system, logical partitions, remote users, and service and support.

Configuring HMC settings to use an open network to connect to the managed system:

Configure the HMC so that it can connect to and manage a managed system using an open network.

To configure the HMC network settings so that it can connect to the managed system using an open network, do the following:

Table 53. Configuring HMC settings to use an open network to connect to the managed system

Task	Where to find related information
1. Decide which interface you want to use for your managed system. eth0 is preferred.	"Preinstallation configuration worksheet for the HMC" on page 83
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0" on page 95
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 141
b. Select the open network type.	"Selecting a private or open network" on page 142
c. Set static addresses.	"Setting the IPv6 address" on page 143
d. Set the firewall.	"Changing HMC firewall settings" on page 144
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 145
f. Configure DNS.	"Configuring domain name services" on page 145
4. Configure additional adapters, if you have them.	
5. Test the connection between the managed server and the HMC.	"Testing the connection between the HMC and the managed system" on page 155

Configuring HMC settings to use a private network to connect to the managed system:

Configure the HMC so that it can connect to and manage a managed system using a private network.

To configure the HMC network settings so that it can connect to the managed system using a private network, do the following:

Table 54. Configuring HMC settings to use a private network to connect to the managed system

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	"Preinstallation configuration worksheet for the HMC" on page 83
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0" on page 95
3. Configure the HMC as a DHCP server.	"Configuring the HMC as a DHCP server" on page 142
4. Test the connection between the managed server and the HMC.	"Testing the connection between the HMC and the managed system" on page 155

Configuring HMC settings to use an open network to connect to logical partitions:

To configure the HMC network settings so that it can connect to logical partitions using an open network, do the following:

Table 55. Configuring HMC settings to use an open network to connect to logical partitions

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	"Preinstallation configuration worksheet for the HMC" on page 83
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0" on page 95
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 141
b. Select the open network type.	"Selecting a private or open network" on page 142
c. Set static addresses.	"Setting the IPv6 address" on page 143
d. Set the firewall.	"Changing HMC firewall settings" on page 144
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 145
f. Configure DNS.	"Configuring domain name services" on page 145
4. Configure additional adapters, if you have them.	
5. Test the connection between the managed server and the HMC.	"Testing the connection between the HMC and the managed system" on page 155

Configuring HMC settings to use an open network to connect to remote users:

To configure the HMC network settings so that it can connect to remote users using an open network, do the following:

Table 56. Configuring HMC settings to use an open network to connect to remote users

Task	Where to find related information
1. Decide which interface you want to use for your managed system.	"Preinstallation configuration worksheet for the HMC" on page 83
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port defined as eth0" on page 95
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 141
b. Select the open network type.	"Selecting a private or open network" on page 142
c. Set static addresses.	"Setting the IPv6 address" on page 143
d. Set the firewall.	"Changing HMC firewall settings" on page 144
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 145
f. Configure DNS.	"Configuring domain name services" on page 145
g. Configure suffixes.	"Configuring domain suffixes" on page 146
4. Configure additional adapters, if you have them.	

Configuring HMC call-home server settings:

To configure the HMC call-home server settings so that problems can be reported, do the following:

Table 57. Configuring HMC call-home server settings

Task	Where to find related information
1. Be sure you have all the required customer information	"Preinstallation configuration worksheet for the HMC" on page 83
2. Configure this HMC to report errors or choose an existing call-home server to report errors	"Configuring the local console to report errors to service and support" on page 148 "Choosing existing call-home servers to connect to service and support for this HMC" on page 151
3. Verify that your call-home configuration is working	"Verifying that your connection to service and support is working" on page 151
4. Authorize users to view collected system data	"Authorizing users to view collected system data" on page 152
5. Schedule transmission of system data	"Schedule Service Information" on page 152

Identifying the Ethernet port defined as eth0:

Your Ethernet connection to the managed server must be made using the Ethernet port that is defined as eth0 on your HMC.

If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, the primary integrated Ethernet port is always defined as eth0 or eth1 on your HMC, if you intend to use the HMC as a DHCP server for your managed systems.

If you have installed additional Ethernet adapters in the PCI slots, the port that is defined as eth0 depends on the location and type of Ethernet adapters you have installed.

Note: These are general rules and may not apply for all configurations.

The following table describes the rules for Ethernet placement by HMC type.

Table 58. HMC types and associated rules for Ethernet placement

HMC type	Rules for Ethernet placement
Rack-mounted HMCs with two integrated Ethernet ports	The HMC supports only one additional Ethernet adapter. <ul style="list-style-type: none"> • If an additional Ethernet adapter is installed, that port is defined as eth0. In this case, the primary integrated Ethernet port is then defined as eth1, and the secondary integrated Ethernet port is defined as eth2. • If the Ethernet adapter is a dual port Ethernet adapter then port labeled Act/Link A will normally be eth0. The port labeled Act/link B would be eth1. In this case, the primary integrated Ethernet port is then defined as eth2, and the secondary integrated Ethernet port is defined as eth3. • If no adapters are installed, the primary integrated Ethernet port is defined as eth0.

Table 58. HMC types and associated rules for Ethernet placement (continued)


HMC type	Rules for Ethernet placement
Stand-alone models with a single integrated Ethernet port	<p>The definitions depend upon the type of Ethernet adapter you have installed:</p> <ul style="list-style-type: none"> • If only one Ethernet adapter is installed, that adapter is defined as eth0. • If the Ethernet adapter is a dual port Ethernet adapter, then the port labeled Act/link A will be eth0. The port labeled Act/link B would be eth1. In this case, the primary integrated Ethernet port is then defined as eth2. • If no adapters are installed, the integrated Ethernet port is defined as eth0. • If multiple Ethernet adapters have been installed, see “Determining the interface name for an Ethernet adapter” on page 96.

Determining the interface name for an Ethernet adapter:

If you configure the HMC as a DHCP server, that server can operate only on the network interface card (NIC) connectors that the HMC identifies as eth0 and eth1. You might also need to determine which NIC connector you need to plug the Ethernet cable into. Learn more about determining which NIC connectors the HMC identifies as eth0 and eth1.

To determine the name the HMC has assigned to an Ethernet adapter, complete the following steps:




1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change Network Settings**.
3. From the **Change Network Settings** window, click the **LAN adapters** tab. The following example entry shows that this Ethernet port is identified as eth0: Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>).
4. Record your results. If you need to view or change the LAN adapter settings, click **Details**.
5. Click **OK**.

Setting the media speed:

Learn how to specify the media speed which includes the speed and duplex mode of the Ethernet adapter.

The default for the HMC adapter settings is **Autodetection**. If this adapter is connected to a LAN switch, you must match the switch port settings. To set the media speed and duplex, complete the following steps:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter you want to work with and click **Details**.


5. In the Local area network information section, select **Autodetection** or the appropriate media speed and duplex combination.
6. Click **OK**.

Selecting a private or open network:

A *private service network* consists of the HMC and the managed systems. A private service network is restricted to consoles and the systems they manage, and is separate from your company network. An *open network* consists of your private service network and your company network. An open network might contain network endpoints in addition to consoles and managed systems, and might span across multiple subnets and network devices.

To select a private or public network, do the following:




1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Lan Adapter** tab.
6. In the Local area network information page, select **Private** or **Open**.
7. Click **OK**.

Configuring the HMC as a DHCP server:

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration.

To configure the HMC as a DHCP server, do the following:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change network settings**. The Customize Network Settings window opens.
3. Select the LAN adapter that you want to work with and click **Details**.
4. Select **Private** and then select the network type.
5. In the DHCP Server section, select **Enable DHCP Server** to enable the HMC as a DHCP server.

Note: You can configure the HMC to be a DHCP server only on a private network. If you use an open network, you do not have the option to select the **Enable DHCP**.

6. Enter the address range of the DHCP server.
7. Click **OK**.

If you configured your HMC to be a DHCP server on a private network, you must verify that your HMC DHCP private network is configured correctly. For information about connecting your HMC to a private network, see “Selecting a private or open network” on page 97.

For more information, see “HMC as a DHCP server” on page 74.


Configure BMC connectivity:

You can configure or view the network settings on the BMC for the management console.

Note: This task applies only to the 7063-CR1. This connection is required to access the baseboard management controller (BMC) on the HMC.

To configure the BMC connection, complete the following steps:




1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change BMC/IPMI network settings**.
3. Select the connection mode (**DHCP** or **Static**).
If you select **Static** mode, complete the following addresses:
 - **IP address**
 - **Subnet mask**
 - **Gateway**
4. Click **OK**.

You can also configure the BMC network connection by using the Petitboot bootloader interface. For more information, see [Configuring the firmware IP address](#).

Setting the IPv4 address:

Learn how to set your IPv4 address on the HMC.




1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Basic Settings** tab.
6. Select an IPv4 address.
7. If you selected to specify an IP address, enter the TCP/IP interface address and the TCP/IP interface network mask.
8. Click **OK**.

Setting the IPv6 address:

Learn how to set your IPv6 address on the HMC.




1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **IPv6 Settings** tab.
6. Select an Autoconfig option or add a static IP address.
7. If you added an IP address, enter the IPv6 address and the prefix length and click **OK**.
8. Click **OK**.

Using only IPv6 addresses:

Learn how to configure the HMC so that it uses only IPv6 addresses.



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Select **No IPv4 address**.
6. Click the **IPv6 Settings** tab.
7. Select **Use DHCPv6 to configure IP settings** or add static IP addresses. Then click **OK**.


After you click OK, you must reboot your HMC for these changes to take effect.

Changing HMC firewall settings:

In an open network, a firewall is used to control outside access to your company network. The HMC also has a firewall on each of its Ethernet adapters. To control the HMC remotely or give remote access to others, modify the firewall settings of the Ethernet adapter on the HMC that is connected to your open network.

To configure a firewall, use the following steps:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Firewall** tab.
6. Using one of the following methods, you can allow any IP address using a particular applications through the firewall, or you can specify one or more IP addresses:
 - Allow any IP address using a particular application through the firewall:
 - a. From the top box, highlight the application.
 - b. Click **Allow Incoming**. The application displays in the bottom box to signify that it has been selected.
 - Specify which IP addresses to allow through the firewall:
 - a. From the top box, highlight an application.
 - b. Click **Allow Incoming by IP Address**.
 - c. On the Hosts Allowed window, enter the IP address and the network mask.
 - d. Click **Add** and click **OK**.
7. Click **OK**.

Enabling remote restricted shell access:

You can enable remote restricted shell access when you configure a firewall.

To enable remote restricted shell access, complete the following steps:



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

Now remote restricted shell access is enabled.

Enabling remote web access:

You can enable remote web access to your HMC.

To enable remote web access, complete the following steps:



1. In the navigation area, select the managed system and click the **Users and Security** icon and then select **Systems and Console Security**.
2. In the content pane, click **Enable Remote Operation**.
3. From the **Enable Remote Operation** window, select **Enabled**.
4. Click **OK**.

Now remote web access is enabled.

Configuring a routing entry as the default gateway:

Learn how to configure a routing entry as the default gateway. This task is available for those using an open network.

To configure a routing entry as the default gateway, do the following:




1. In the navigation area, click the **HMC Management** icon and then select **Console Settings**.
2. In the content pane, click **Change network settings**. The **Customize Network Settings** window opens.
3. Click the **Routing** tab.
4. In the **Default gateway** information section, enter the gateway address and gateway device of the routing entry you want to set as the default gateway.
5. Click **OK**.

Configuring domain name services:

If you plan to set up an open network, configure domain name services.

If you plan to set up an open network, configure domain name services. Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Configuring domain name services includes enabling DNS and specifying the domain suffix search order.



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change network settings**. The Change Network Settings window opens.
3. Click the **Name Services** tab.
4. select **DNS enabled** to enable DNS.
5. Specify the DNS server and domain suffix search order and click **Add**.
6. Click **OK**.


Configuring domain suffixes:

The list of domain suffixes is used to resolve an IP address starting with the first entry in the list.

The domain suffix is a string appended to a host name that is used to help resolve its IP address. For example, a host name of `myname` might not be resolved. However, if the string `myloc.mycompany.com` is an element in the domain suffix table, then there will be an attempt to resolve `myname.mloc.mycompany.com` also.

To configure a domain suffix entry, use these steps:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
2. In the content pane, click **Change network settings**. The Customize Network Settings window opens.
3. Click the **Name Services** tab.
4. Enter a string to be used as a domain suffix entry.
5. Click **Add** to add it to the list.

Configuring the HMC so that it uses LDAP remote authentication:


You can configure your Hardware Management Console (HMC) so that it uses LDAP (Lightweight Directory Access Protocol) remote authentication.

When a user logs in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote LDAP server for authentication. You must configure your HMC so that it uses LDAP remote authentication.

Note: Before you configure the HMC so that it uses LDAP authentication, you must ensure that a working network connection exists between the HMC and the LDAP servers. For more information about configuring HMC network connections, see “Configuring the HMC network types” on page 93.

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



1. In the navigation area, click the **Users and Security** icon  , and then select **Systems and Console Security**.
2. In the content pane, select **Manage LDAP**. The LDAP Server Definition window opens.
3. Select **Enable LDAP**.
4. Define an LDAP server to use for authentication.
5. Define the LDAP attribute used to identify the user being authenticated. The default is **uid**, but you can use your own attributes.

6. Define the distinguished name tree, also known as the search base, for the LDAP server.
7. Click **OK**.
8. If a user wants to use LDAP authentication, the user must configure his profile so that it uses LDAP remote authentication instead of local authentication.

Configuring the HMC so that it uses Key Distribution Center servers for Kerberos remote authentication:

You can configure the HMC so that it uses Key Distribution Center (KDC) servers for Kerberos remote authentication.


When a user logs in to the HMC, authentication is first performed against a local password file. If a local password file is not found, the HMC can contact a remote Kerberos server for authentication. You must configure your HMC so that it uses Kerberos remote authentication.

Note: Before you configure the HMC so that it uses KDC servers for Kerberos remote authentication, you must ensure that a working network connection exists between the HMC and the KDC servers. For more information about configuring HMC network connections, see “Configuring the HMC network types” on page 93.


To configure the HMC so that it uses KDC servers for Kerberos remote authentication, do the following:

1. Enable the Network Time Protocol (NTP) service on the HMC and set the HMC and the KDC servers to synchronize time with the same NTP server. To enable the NTP service on the HMC, do the following:




- a. In the navigation area, click the **HMC Management** icon  , and then select **Console Settings**.
 - b. In the content pane, select **Change Date and Time**.
 - c. Select the **NTP Configuration** tab.
 - d. Select **Enable NTP service on this HMC**.
 - e. Click **OK**.
2. Configure each remote HMC user's profile so that it uses Kerberos remote authentication instead of local authentication.
 3. Optional: you can import a service-key file into this HMC. The service-key file contains the host principal that identifies the HMC to the KDC server. Service-key files are also known as *keytabs*. To import a service-key file into this HMC, do the following:



- a. In the navigation area, click the **Users and Security** icon  , and then select **Systems and Console Security**.
 - b. In the content pane, select **Manage KDC**.
 - c. Select **Actions > Import Service Key**. The Import Service Key window opens.
 - d. Type the location of the service key file.
 - e. Click **OK**.
4. Add a new KDC server to this HMC. To add a new KDC server to this HMC, do the following:



- a. In the navigation area, click the **Users and Security** icon  , and then select **Systems and Console Security**.
- b. In the content pane, select **Manage KDC**.
- c. Select **Actions > Add KDC Server**. The Import Service Key window opens.
- d. Type the realm and the host name or IP address of the KDC server.
- e. Click **OK**.

Configuring the local console to report errors to service and support:

Configure this HMC so that it can call-home errors by using LAN connectivity.

Configuring the HMC so that it can connect to service and support using the call-home setup wizard:

Configure the HMC so that it is a call-home server using the call-home wizard.


This procedure describes how to configure the HMC as a call-home server using direct (LAN-based) and indirect (SSL) connections to the Internet.

Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- If you are configuring Internet support through a proxy server, you must also have the following:
 - The IP address and port of the proxy server
 - The proxy authentication information
- The adapter designated as **eth1** (the one that is designated as an open network) is used. For more information, see “Choosing network settings on the HMC” on page 72.
- An Ethernet cable physically connects the HMC to the LAN.

To configure the HMC so that it is a call-home server using the call-home wizard, do the following:



1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, click **Call-Home Setup Wizard**. The Connectivity and Call-Home Servers wizard opens. Follow the instructions in the wizard to configure call-home.

Configuring the local console to report errors to service and support:

Configure this HMC so that it can call-home errors by using LAN connectivity.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.

Configuring an HMC to contact service and support using LAN-based Internet and SSL:


Describes how to configure the HMC as a call-home server using direct (LAN-based) and indirect (SSL) connections to the Internet.

Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- Customer contact information has been configured. Verify this by going to the HMC interface and clicking **Serviceability>Service Management > Manage Customer Information**.
- If you are configuring internet support through a proxy server, you must also have the following:
 - The IP address and port of the proxy server
 - The proxy authentication information
- You need at least one open network interface configured. For more information, see “Private and open networks in the HMC environment” on page 74.
- An Ethernet cable physically connects the HMC to the LAN.

To configure the HMC as a Call Home server using LAN-based Internet and SSL, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**. The Call-home Server Consoles window opens.
3. Click **Configure**.
4. In the Outbound Connectivity Settings window, check **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, select the **Internet** page.
7. Check the **Allow an existing internet connections for service** box.
8. If you are using an SSL proxy, check the **Use SSL proxy** box.
9. If you are using an SSL proxy, fill in the proxy's address and port. Obtain this information from the network administrator.
10. If you checked **Use SSL proxy** and the proxy requires user ID and password authentication, check the **Authenticate with the SSL proxy** box. Type the userid and password. Obtain the user ID and password from the network administrator.
11. Select the **Protocol to Internet** you want to use.
12. On the **Internet** page, click **Test**.
13. In the Test Internet window, click **Start**.
14. Verify that the test completes successfully.
15. In the Test Internet window, click **Cancel**.
16. In the Outbound Connectivity Settings window, click **OK**.

Connecting to service and support using the telephone and modems:

Describes how to configure the HMC as a call-home server using modem access to IBM support.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.


Before you begin this task, ensure that:

- You have an dedicated analog telephone line available.
- You have the information required to configure the modem. For more information, see “Preparing for HMC configuration” on page 81.
- Customer contact information has been configured. You may verify this by going to the HMC interface and clicking **Serviceability>Service Management > Manage Customer Information**.
- Ensure you have the following information available:

- The type of analog line; that is, tone or pulse. Most lines are tone, but some are in use that are the older rotary or pulse type.
- Whether the line presents a dial tone when the telephone is picked up. Most telephones do, but some are in use that do not.
- Whether a dial prefix string is required. A dial prefix string is a number or series of numbers that allow access to an outside line.

To configure the HMC as a call-home server using modem access to IBM support, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**.
3. Click **Configure**.
4. In the Outbound Connectivity Settings window, select **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, click the **Local Modem** tab.
7. On the Local Modem page, select the **Allow local modem dial for service** checkbox.
8. On the Local Modem page, select the **Modem Configuration** checkbox.
9. In the Customize Modem Settings window, click **Dial type, Tone or Pulse**. If the line presents a dial tone when the receiver is taken off the hook, select the **Wait for dial tone** checkbox. Fill in any dial prefix string that is required to obtain an outside line.
10. Click **OK**.
11. On the Local Modem page, click **Add**.
12. Select a number from the list.
13. If this is a local number, remove the area code from the **Telephone number** field.
14. In the Add Telephone Number panel, click **Add**.
15. In the In the Customize Modem Settings panel, click **Test**.
16. In the Test Telephone Number panel, click **Start**.
17. Verify that the test completes successfully.
18. In the Test Telephone Number window, click **Cancel**.
19. You can configure up to five telephone numbers. Configure at least two telephone numbers (a primary and a backup). The numbers will be attempted in the order that they are configured. To add additional numbers to the callable list, repeat the steps in this procedure.
20. In the Outbound Connectivity Settings window, click **OK**.

Connecting to service and support using a LAN-based VPN:

Configure the call-home server using VPN.

Note: Internet virtual private network (VPN) and dial-up connection types are available only on HMC version 8.2.0 or earlier.


Before you begin this task, ensure that:

- The network administrator has verified that connectivity is allowed. For more information, see “Preparing for HMC configuration” on page 81.
- The adapter designated as **eth1** (the one that is designated as an open network) is used. For more information, see “Choosing network settings on the HMC” on page 72.
- An Ethernet cable physically connects the HMC to the LAN.

- Customer contact information has been configured. Verify this situation by clicking **Serviceability>Service Management > Manage Customer Information** on the HMC interface.

To configure the call-home server using VPN, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**.
3. Click **Configure**.
4. In the Outbound Connectivity Settings window, select **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, click the **Internet VPN** tab.
7. On the Internet VPN page, click **Allow A VPN and an existing Internet connections for service**.
8. On the Internet VPN page, select the **Test** check box.
9. In the Test Internet VPN window, click **Start**.
10. Verify that the test completes successfully.
11. In the Test Internet VPN window, click **Cancel**.
12. In the Outbound Connectivity Settings window, click **OK**.


Choosing existing call-home servers to connect to service and support for this HMC:

Choose existing HMC call-home servers that have been recognized, or "discovered" by this HMC to report errors.

Discovered HMCs are HMCs that are enabled as call-home servers and are either on the same subnet or manage the same managed system as this HMC.

To choose a discovered HMC to call home when this HMC reports errors, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the content pane, click **Manage Outbound Connectivity**. The Call-Home Server Consoles window opens.
3. Click **Use discovered call-home server consoles**. The HMC displays the IP address or host name of the HMCs configured for call-home.
4. Click **OK**.


You can also manually add existing HMC call-home servers that are on a different subnet. Select the IP address or host name of the HMC that is configured for call home and click **Add**. Then click **OK**.

Verifying that your connection to service and support is working:

Test problem reporting to ensure that connection to service and support is working.

To verify that your call-home configuration is working, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the content pane, click **Create Event**.

3. Select **Test Automatic problem Reporting** and type a comment.
4. Click **Request Service**. Wait a few minutes for the request to be sent.
5. In the Service Management window, select **Manage Events**.
6. Select **All open problems**.
7. Verify that there is a PMH event and number assigned to the problem number you opened.
8. Select that event and click **Close**.
9. On the Close window, type your name and a brief comment.


Authorizing users to view collected system data:

You must authorize users to view data about your systems.

Before you authorize users to view collected system data, you must obtain an IBM ID. For more information about obtaining an IBM ID, see “Preinstallation configuration worksheet for the HMC” on page 83.

To authorize users to view collected system data, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the content pane, select **Authorize User**.
3. Enter your IBM ID.
4. Click **OK**.

Transmitting service information:


You can transmit information to your service provider immediately, or you can schedule the information to be sent on a regular basis.

IBM provides personalized Web functions that use information collected by IBM Electronic Service Agent. To use these functions, you must first register on the IBM Registration website at <http://www.ibm.com/account/profile>. To authorize users to use the Electronic Service Agent information to personalize the Web functions, see “Authorizing users to view collected system data” on page 105. For more information about the benefits of registering an IBM ID with your systems, see <http://www.ibm.com/support/electronic>.

Note: You should transmit service provider information as soon as the HMC is installed and configured for use.

To transmit service information, do the following:



1. In the navigation area, click the **Serviceability** icon , and then select **Service Management**.
2. In the content pane, click **Transmit Service Information**.
3. Complete the tasks in the Transmit Service Information window, and click **OK**.


Schedule Service Information:

Schedule when to transmit service information to use for problem determination.

Note: You should transmit service provider information as soon as the Hardware Management Console (HMC) is installed and configured for use.

To schedule service information, complete the following steps:



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

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

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

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

Configuring the Events Manager for Call Home:

Learn how to configure the Events Manager for Call Home task. You can monitor and approve any data that is being transmitted from an HMC to IBM through this task.

The Events Manager for Call Home mode (enabled or disabled) is set by using the HMC command-line interface. Enabling the Events Manager for Call Home task blocks the HMC from automatically calling home events as they occur. To prevent events that are called home without approval, all HMCs running in this environment must have the Events Manager for Call Home enabled.

To enable or disable the Events Manager for Call Home task, run the following command:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

Note: Enabling the Events Manager for Call Home task holds call home events until they have been approved for the call home task. If you disable the Events Manager for Call Home task, it does not automatically enable the call home feature. This setup prevents any unintended call home of data back to IBM. Choose from the following command options to set up the required configuration:


- To enable the Events Manager for Call Home task: **chhmc -c emch -s enable**
- To disable the Events Manager for Call Home task and to re-enable automatic call home: **chhmc -c emch -s disable --callhome enable**
- To disable the Events Manager for Call Home task and not re-enable automatic call home: **chhmc -c emch -s disable --callhome disable**

Ensure that the HMC can communicate with other HMCs deployed in this environment. The Events Manager for Call Home has a test connection function when an HMC is registered.

You can register the HMC with the Events Manager for Call Home. After you register the HMC, the events manager queries the registered HMC for any events that are waiting to be called home to IBM. The Events Manager shows what data is being sent back to IBM and approves these events. After approval, the Event Manager notifies the registered HMC that it can proceed with the call home operation.

The Events Manager for Call Home task can be run from any HMC or from multiple HMCs. To register a management console with the Events Manager for Call Home task, complete the following steps:



1. In the navigation area, click the **Serviceability** icon , and then select **Events Manager for Call Home**.
2. From the **Events Manager for Call Home** pane, click **Manage Consoles**.
3. From the **Manage Registered Consoles** window, click **Add Console** to enter information to register a management console with the Events Manager for Call Home task.
4. Click **OK** to commit the changes to the list of registered management console.

Note: The Events Manager for Call Home can be used with the event manager mode disabled. You can still register the HMC and view events in the events manager, but Events Manager does not control when the events are called home.

Setting passwords for the managed system:

You must set passwords for both your server and Advanced System Management (ASM). Read more about how to use the HMC interface to set these passwords.


If you received the message Authentication Pending, the HMC prompts you to set the passwords for the managed system.

If you did not receive the message Authentication Pending, complete the following steps to set the passwords for the managed system.

Updating your server password:

To update your server password, do the following:



1. In the navigation area, select the managed system and click the **Users and Security** icon , and then select **Users and Roles**.
2. Click **Change Password**. The Update Password window opens.

3. Type the required information and click **OK**.

Updating your Advanced System Management (ASM) general password:

Note: The default password for the general user ID is `general`, and the default password for the administrator ID is `admin`.

To update your ASM general password, do the following:

1. In the navigation area of the HMC, select the managed system.
2. In the Tasks area, click **Operations**.
3. Click **Advanced System Management (ASM)**. The Launch ASM Interface window opens.
4. Select a Service Processor IP Address and click **OK**. The ASM interface opens.
5. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
6. In the navigation area, expand **Login Profile**.
7. Select **Change Password**.
8. Specify the required information, and click **Continue**.

Resetting the Advanced System Management (ASM) administrator password:

To reset the administrator password, contact an authorized service provider.

Testing the connection between the HMC and the managed system:


This option enables you to verify that you are properly connected to the network.

To test network connectivity, you must be a member of one of the following roles:

- Super administrator
- Service representative

To test the connection between the HMC and the managed system, do the following:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Settings**.
2. In the content pane, click **Test Network Connectivity**.
3. In the Ping tab, type the host name or IP address of any system to which you want to connect. To test an open network, type the gateway. Click **Ping**.

If you have not yet created any logical partitions, you will not be able to ping the addresses. You can use the HMC to create logical partitions on your server. For more information, see *Logical partitioning*.

To understand how the HMC can be used in a network, see “HMC network connections” on page 72.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC by using the HMC menus” on page 91.

Postconfiguration steps

After you have installed and configured the HMC, back up HMC data as necessary.

Backing up management console data

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

Your remote system must have Network File System (NFS) or Secure Shell (ssh) configured, and this network must be accessible from the HMC. To complete this task, you must shut down and reboot the HMC. Use only the HMC to perform these tasks.

To back up the HMC hard disk drive to a remote system, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

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


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

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

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

To back up the HMC hard drive to a remote system, complete the following steps:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
2. In the content pane, click **Backup Management Console Data**.
3. From the **Backup Management Console Data** window, select the archive option you want to perform.
4. Click **Next**, then follow the appropriate instructions depending on the option you chose.
5. Click **OK** to continue with the backup process.

Updating, upgrading, and migrating your HMC machine code

Updates and upgrades are periodically released for the HMC to add new functionality and to improve existing features. Learn more about the differences between updating, upgrading, and migrating your HMC machine code. Also learn how to perform an HMC machine code update, upgrade, or migration.

When you are finished with each of these tasks, the HMC reboots but the partitions do not.

Updating HMC code

Applies maintenance to an existing HMC level

Does not require that you perform the **Save upgrade data** task

Upgrading HMC code

Replaces HMC software with a new release or fix level of the same program

Requires that you boot from recovery media

Migrating HMC code

Moves HMC data from one HMC version to another

A migration is a type of upgrade.

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.


Determining your HMC machine code version and release

Find out how to view the HMC machine code version and release.

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

To view the HMC machine code version and release, do the following:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.

Obtaining and applying machine code updates for the HMC with an Internet connection

Learn how to obtain machine code updates for the HMC when the HMC has an Internet connection.

To obtain machine code updates for the HMC, perform steps 1 through 5.


Step 1. Ensure that you have an Internet connection:

To download updates from the service and support system or website to your HMC or server, you must have one of the following:

- SSL connectivity with or without a SSL proxy
- Internet VPN

To ensure that you have an Internet connection, do the following:



1. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
2. In the content pane, **Manage Outbound Connectivity**.
3. Select the tab for the type of outbound connectivity that you chose for your HMC (Internet VPN or SSL connectivity).

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see *Setting up your server to connect to IBM service and support*.

4. Click **Test**.
5. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on DVD.


Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

6. Continue with “Step 2. View the existing HMC machine code level.”

Step 2. View the existing HMC machine code level:

To view the existing HMC machine code level, do the following:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with “Step 3. View the available HMC machine code levels.”

Step 3. View the available HMC machine code levels:

To view the available HMC machine code levels, do the following:

1. From a computer or server with an Internet connection, go to <http://www.ibm.com/eserver/support/fixes>.
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact service and support.


6. Continue with “Step 4. Apply the HMC machine code update.”

Step 4. Apply the HMC machine code update:

To apply the HMC machine code update, do the following:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see “Backing up critical HMC data” on page 108. Then continue with the next step.




2. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
3. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.
4. Follow the instructions in the Wizard to install the update.
5. Shut down and then restart the HMC for the update to take effect.
6. Click **Log on and launch the Hardware Management Console web application**.
7. Log in to the HMC interface.

Step 5. Verify that the HMC machine code update installed successfully:

To verify that the HMC machine code update installed correctly, do the following:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.

5. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Select the network connection on the HMC.
 - b. Retry the firmware update using a different repository.
 - c. If the problem persists, contact your next level of support.

Obtaining and applying machine code updates for the HMC using DVD or an FTP server

Learn how to obtain machine code updates for the HMC using DVD or an FTP server.


To obtain HMC machine code updates, perform steps 1-5.

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

Step 1. View the existing HMC machine code level:

To view the existing HMC machine code level, do the following:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with “Step 2. View the available HMC machine code levels.”

Step 2. View the available HMC machine code levels:

To view the available HMC machine code levels, do the following:

1. From a computer or server with an Internet connection, go to the Hardware Management Console Web site at <http://www-933.ibm.com/support/fixcentral/>.
2. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact IBM service and support.

3. Continue with “Step 3. Obtain the HMC machine code update.”

Step 3. Obtain the HMC machine code update:

To obtain the HMC machine code update, do the following:

You can order the HMC machine code update through the Fix Central website, contact service and support, or download it to an FTP server.

Ordering the HMC machine code update through the Fix Central Web site

1. From a computer or server with an Internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>
2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File name(s) / Package area and locate the update you want to order.
4. In the Order column, select **Go**.
5. Click **Continue** to sign in with your IBM ID.
6. Follow the on-screen prompts to submit your order.

Downloading the HMC machine code update to removable media

1. From a computer or server with an Internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>

2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File name(s) / Package area and locate the update you want to download.
4. Click the update you want to download.
5. Accept the license agreement, and save the update to your removable media.


When you are finished, continue with “Step 4. Apply the HMC machine code update.”

Step 4. Apply the HMC machine code update:

To apply the HMC machine code update, do the following:

1. Before you install updates to the HMC machine code, back up HMC data. For more information, see “Backing up critical HMC data” on page 108
2. If you obtained or created the update on DVD-RAM, insert it into the DVD drive on the HMC. If you obtained or created the update on a USB memory device, insert the memory device.
3. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see “Backing up critical HMC data” on page 108. Then continue with the next step.




4. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
5. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.
6. Follow the instructions in the Wizard to install the update.
7. Shut down, restart, and log back in to the HMC for the update to take effect.
8. Continue with “Step 5. Verify that the HMC machine code update installed successfully.”

Step 5. Verify that the HMC machine code update installed successfully:

To verify that the HMC machine code update installed successfully, do the following:



1. In the navigation area, click the **HMC Management** icon , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Retry the machine code update. If you created a DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Upgrading your HMC software

Learn how to upgrade the software on an HMC from one release to the next while you maintain your HMC configuration data.

To upgrade the machine code on an HMC, complete steps 1-9.

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

Step 1. Obtain the upgrade:

You can order the HMC machine code upgrade through the Fix Central website.

To obtain the upgrade through the Fix Central website, complete the following steps:

1. From a computer or server with an internet connection, go to the Hardware Management Console website at <http://www-933.ibm.com/support/fixcentral/>.
2. Click **Continue**. The Hardware Management Console site is displayed.
3. Navigate to the HMC version you want to upgrade to.
4. Locate the download and ordering section.


Note: If you do not have access to the internet, contact IBM service and support to order the upgrade on DVD.

5. Follow the on-screen prompts to submit your order.
6. After you have the upgrade, continue with “Step 2. View the existing HMC machine code level.”

Step 2. View the existing HMC machine code level:

To determine the existing level of machine code on an HMC, follow these steps:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**. In the navigation area, click **Updates**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Continue with “Step 3. Back up the managed system's profile data.”

Step 3. Back up the managed system's profile data:

To back up the managed system's profile data, complete the following steps:

1. In the navigation area, select **Systems Management**.
2. Select **Servers**.
3. Select the server and ensure that the state is *Operating* or *Standby*.
4. Under Tasks, select **Configuration > Manage Partition Data > Backup**.
5. Type a backup file name and record this information.
6. Click **OK**.
7. Repeat these steps for each managed system.
8. Continue with “Step 4. Back up HMC data.”

Step 4. Back up HMC data:


Back up HMC data before you install a new version of HMC software so that previous levels can be restored in the event of a problem while you upgrade the software. Do not use this critical console data after a successful upgrade to a new version of the HMC software.

Note: To back up to removable media, you need to have that media available.


To back up HMC data, complete the following steps:

1. If you plan to back up to media, perform the following steps to format the media:
 - a. Insert the media into the drive.



- b. In the navigation area, click the **Serviceability** icon  , and then select **Service Management**.
- c. In the content pane, click **Format Media**.
- d. Select the media type.
- e. Select the format type.
- f. Click **OK**.



2. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
3. In the content pane, click **Backup Management Console Data**. The **Backup Management Console Data** window opens.
4. Select an archive option. You can back up to media on a local system, a remote system that is mounted to the HMC file system (for example, NFS), or send the backup to a remote site by using File Transfer Protocol (FTP).
 - To back up to a local system, choose **Back up to media on local system** and follow the instructions.
 - To back up to a mounted remote system, choose **Back up to mounted remote system** and follow the instructions.
 - To back up to a remote FTP site, choose **Send back up critical data to remote site** and follow the instructions.
5. Continue with “Step 5. Record the current HMC configuration information.”

Step 5. Record the current HMC configuration information:

Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information.


To record the current HMC configuration, complete the following steps:

1. Select a managed system or any partitions that you want to record HMC configuration information.
2. From the menu pod, select **Actions > Schedule Operations**. All scheduled operations for the target that you selected are displayed.
3. Select **Sort > By Object**.
4. Select each object and record the following details:
 - Object Name
 - Schedule date
 - Operation Time (displayed in 24-hour format)
 - Repetitive (if Yes, complete the following steps):
 - a. Select **View > Schedule Details**.
 - b. Record the interval information.
 - c. Close the scheduled operations window.
 - d. Repeat for each scheduled operation.
5. Close the **Customize Scheduled Operations** window.
6. Continue with “Step 6. Record remote command status.”

Step 6. Record remote command status:

To record remote command status, complete the following steps:



1. In the navigation area, click the **Users and Security** icon  , and then select **Systems and Console Security**.
2. In the content pane, click **Enable Remote Command Execution**.
3. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
4. Click **Cancel**.
5. Continue with “Step 7. Save upgrade data.”


Step 7. Save upgrade data:

You can save the current HMC configuration in a designated disk partition on the HMC or to local media. Save upgrade data only immediately before you upgrade your HMC software to a new release. You can restore the HMC configuration settings after you upgrade.

Note: Only one level of backup data is allowed. Each time that you save upgrade data, the previous level is overwritten.

To save upgrade data, complete the following steps:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
2. In the content pane, click **Save Upgrade Data**. The **Save Upgrade Data** wizard opens.
3. Select the media on which you want to save the upgrade data. If you choose to save to removable media, insert the media now. Click **Next**.
4. Click **Finish**.
5. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

Note: If the save upgrade data task fails, do not continue the upgrade process.


6. Click **OK**.
7. Continue with “Step 8. Upgrade the HMC software.”

Step 8. Upgrade the HMC software:

To upgrade the HMC software, restart the system with the removable media in the DVD drive.

1. Insert the HMC Product Installation media into the DVD drive.



2. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
3. In the content pane, select **Shutdown or Restart the Management Console**.
4. Ensure **Restart the HMC** is selected.
5. Click **OK**. The HMC restarts and system information scrolls on the window.
6. Select **Upgrade** and click **Next**.
7. Choose from the following options:
 - If you saved the upgrade data during the previous task, continue with the next step.
 - If you did not save the upgrade data previously in this procedure, you must save the upgrade data now before you continue.

8. Select **Upgrade from media** and click **Next**.
9. Confirm the settings and click **Finish**.
10. Follow the prompts.


Note:

- If the screen goes blank, press the space bar to view the information.
 - The first DVD can take approximately 20 minutes to install.
11. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
 12. Continue with “Step 9. Verify that the HMC machine code upgrade installed successfully.”

Step 9. Verify that the HMC machine code upgrade installed successfully:

To verify that the HMC upgrade is installed successfully, complete the following steps:



1. In the navigation area, click the **HMC Management** icon  , and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code that is displayed is not the level that you installed, retry the upgrade task by using a new DVD. If the problem persists, contact your next level of support.

Upgrading HMC from remote location using network upgrade images

Learn how to upgrade the software on an HMC from a remote location using network upgrade images.

Learn how to upgrade the software on an HMC from a remote location using network upgrade images. Use the following procedure to upgrade HMC at level V6R1.2 or higher, which includes all HMC V7 levels.

1. From a computer or server with an Internet connection, go to the Hardware Management Console website (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. Download the appropriate HMC V7 network images and save them on an FTP server. You cannot download these files directly to the HMC. You must download the image files to a server that accepts FTP requests.
3. Ensure that you download the following files:
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. Save the upgrade data on the HMC. Execute the following command lines to save the upgrade data:
 - To save data on both DVD and HDD, execute the following commands:


```
mount /media/cdrom
saveupgdata -r diskdvd
```
 - To save data on the HDD, execute the following command:


```
saveupgdata -r disk
```

5. Copy the upgrade files to the bootable disk partition on the HMC. Run the **getupgfiles** command to copy the files.

Example: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**

Where,

- **ftp server** is the host name or ip address of the FTP server where you have downloaded the HMC network images.
 - **user id** is a valid user id on the FTP server. If you do not specify the password with the `--passwd` argument, you will be prompted for a password.
 - **remote directory** is the directory on your FTP server where the HMC network images are saved.
6. Reboot the HMC to upgrade the code copied to the bootable disk partition. Run the **chhmc -c altdiskboot -s enable --mode upgrade** to reboot the HMC.
 7. Reboot the HMC and start the upgrade. Run the **hmcshutdown -r -t now** command to start the upgrade.

Securing the HMC

Learn more about how to enhance the security of your HMC based on your corporate security standards.

The default configuration of HMC provides ample security for most enterprise users. With the Hardware Management Console (HMC) Version 8.4.0, or later, you can further enhance the security of the HMC based on your corporate security standards. To enhance the security of HMC, you must set the HMC to minimum of Level 1 security. You may choose to go to Level 2 and Level 3 security depending on your environment and the corporate security requirements.

Note: Before changing the security level, ensure that you check with your corporate security compliance team.

To secure the HMC, do the following procedure:

Level 1 security

1. Change the default hscroot predefined password. For more information about password policy, see Enhanced password policy.
2. If the HMC is not in a physically secure environment, set the grub password by running the following command: **chhmc -c grubpasswd -s enable --passwd <new grub password>**
3. If you have configured Integrated Management Module (IMM) on HMC, set a strong IMM password.
4. Set strong password for *admin* users and general users on all servers.
5. Update the HMC with all the released security fixes. For more details about the security fixes, see IBM Fix Central.

Level 2 security (Optional)

If you have multiple users, complete the following steps to enhance the security:

6. Create account for each user on the HMC and assign the required roles and resources to users that are created. For more information about the various roles in HMC, see HMC tasks, user roles, IDs, and associated commands.

Note: Ensure that you assign only the required resources and roles for users that are created on the HMC. You can also create custom roles, if necessary.

7. Enable user data replication between Hardware Management Consoles. The user data replication can be done in Master-slave mode or Peer-Peer mode. For more information on user data replication, see Manage Data Replication .
8. Import a certificate signed by the Certificate Authority.

Level 3 security (Optional)

If you have multiple Hardware Management Consoles and system administrators, complete the following steps to enhance the security:

9. Use centralized authentication such as LDAP or Kerberos. For more information about how to configure LDAP, see *How to Configure LDAP on HMC*.
10. Enable user data replication between Hardware Management Consoles.
11. Ensure that HMC is in NIST SP 800-131A mode so that the HMC uses only strong ciphers.
12. Block ports that are not required in the firewall. For HMC ports that can be used, see the following table:

Table 59. Port used by the user for interaction with HMC

Port	Description	Type	Protocol version (Default mode)	Protocol Version (NIST Mode)
22	Open SSH	TCP	SSH v2.0	SSH v2.0
123	NTP	UDP	NTP	NTP
161	SNMP Agent	UDP	SNMP v3	SNMP v3
162	SNMP Trap	UDP	SNMP v3	SNMP v3
427	SLP	UDP	NA	NA
443	HMC GUI and REST API	TCP	https (TLS 1.2, 1.1)	https (TLS 1.2)
657	RMC	TCP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)
2300	5250 Terminal for IBM i	TCP	Plain text	Plain text
2301	5250 Secure terminal for IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (legacy, removed)	TCP	Non-functional	Non-functional
9900	FCS: HMC-HMC discovery	UDP	FCS	FCS
9920	FCS: HMC-HMC communication	TCP	https (TLS 1.2)	https (TLS 1.2)
9960	VTerm applet in GUI	TCP	https (TLS 1.2, 1.1)	https (TLS 1.2)
12443	HMC REST API (legacy port)	TCP	https (TLS 1.2, 1.1, 1.0 for HMC Version 8.6.0, and before)	https (TLS 1.2)
12347	RSCT Peer Domain	UDP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)
12348	RSCT Peer Domain	UDP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)

Note: You must use only ssh (port 22), https (port 443 and port 12443), and VTerm (port 9960) that are exposed to an intranet. Remaining ports must be used in private or isolated network. You can use a separate Ethernet port and VLAN for the Resource Monitoring and Control (RMC) (port 657), FCS (port 9900 and port 9920), and RSCT Peer Domain (port 12347 and port 12348).

Solving common problems while securing HMC

This section describes the solutions to some problems that you might encounter when you secure HMC.

How to secure the Hardware Management Console (HMC) connection to the system?

HMC connects to the system through the Flexible Service processor (FSP). A proprietary binary protocol called NETC is used for managing both FSP and Power hypervisor. The following table lists ports that are used by the HMC:

Table 60. Ports on FSP that are used for interaction with the HMC

Port on FSP	Description	Protocol version (Default mode)	Protocol Version (NIST Mode)
443	Advanced System Management Interface	https (TLS 1.2)	https (TLS 1.2)
30000	NETC	NETC (TLS 1.2) . Falls back to SSLv3 for support of older firmware.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2) . Falls back to SSLv3 for support of older firmware.	NETC (TLS 1.2)

How to lock the HMC?

If you want to have an extra layer of security for your infrastructure, you can use an IBM Prerequisite Scanner Device or add all Hardware Management Consoles and Power servers behind a firewall. If you don't use the HMC remotely or want to lock the HMC down, you can disable network services on the HMC. To disable network services on the HMC, complete the following steps:

- Disable remote command execution by using the ssh port.
- Disable remote virtual terminal (VTerm port).
- Disable remote web access (HMC graphical user interface and REST API).
- Block ports in firewall by using HMC network settings for each configured Ethernet port.

How to set HMC in NIST SP 800-131A compliance mode?

With HMC Version 8.1.0, or later, when you set HMC in the compliance mode, only strong ciphers listed by NIST SP 800-131A are supported. You might not be able to connect to older Power servers such as, Power 5 that do not support Transport Layer Security (TLS 1.2). For more details about changing the security mode, see HMC V8R8 NIST mode.

How to view and change ciphers that are used by the HMC?

With HMC Version 8.1.0, or later, HMC introduces support for the more secure cipher sets defined in NIST 800-131A. Ciphers used in default mode are strong. If your corporate standards requires the use of a different set of ciphers, run the **chhmcencr** command to modify the encryption ciphers. To know details about the encryption ciphers that are used by the HMC, run the following **lshmcencr** commands.

List the encryption ciphers that are used by HMC to encrypt user password:

```
lshmcencr -c passwd -t c
```

List the encryption ciphers that can currently be used by the HMC Web user interface and REST API:

```
lshmcencr -c webui -t c
```

List the encryption ciphers and MAC algorithm that can currently be used by the HMC SSH interface:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

How to check the strength of the certificate on the HMC?

The self-signed certificates on HMC use SHA256 with 2048-bit RSA encryption, which is strong. If you are using CA signed certificates, ensure that you are not using the 1024-bit encryption, which is weak. The following are the two different certificates on HMC:

- For HMC graphical user interface and REST API (port 443 and port12443): The certificate can be replaced by a CA signed certificate.
- For HMC to HMC communication (port 9920): The port 9920 is used for communication between Hardware Management Consoles. You can't replace this certificate with your own certificate.

How to choose between a self-signed certificate (default) or a CA signed certificate?

HMC auto-generates a certificate during installation. However, you can generate a CSR (Certificate Signing Request) from HMC and get a new certificate issued by a certificate authority. You can import this certificate into HMC. Ensure that you also obtain a domain name for the HMC. For more details about managing the certificates in HMC, see Manage Certificates.

How to audit an HMC?

The audit on Hardware Management Consoles focuses on configured ciphers and the usage activity of various HMC users.

Table 61. Ciphers that are used by HMC

Purpose	Command
Password Encryption (global setting)	<code>lshmcencr -c passwd -t c</code>
Password Encryption for each user	<code>lshmcusr -Fname:password_encryption</code>
SSH Ciphers	<code>lshmcencr -c ssh -t c</code>
SSH MAC	<code>lshmcencr -c sshmac -t c</code>
Cipher used for HMC graphical user interface and REST API	<code>lshmcencr -c webui -t c</code>

Use the following commands to monitor various user logon information and operations:

Table 62. Commands to view the logged on users and console or serviceable events information in HMC

Information	Command
GUI users	<code>lslogon -r webui -u</code>
GUI tasks	<code>lslogon -r webui -t</code>
CLI users	<code>lslogon -r ssh -u</code>
CLI tasks	<code>lslogon -r ssh -t</code>
Operations on HMC	<code>lssvcevents -t console -d <number of days></code>
Operations on System	<code>lssvcevents -t hardware -m <managed system> -d <number of days></code>

Centralized monitoring of Events: If you have many Hardware Management Consoles, set the `rsyslog` file to collect all the usage data.

How to find the version of OpenSSH running on the HMC

Use KALI Linux tool that can be used for the penetration testing of the servers. As a best practice, use KALI Linux 64 bit. To detect the version of an open source software on HMC, complete the following procedure:

- Start Metasploit framework that is available in KALI and run the following commands:

```
use auxiliary/scanner/ssh/ssh_version
set RHOSTS <HMC IP / DNS Name>
run
```

Output: “SSH server version: SSH-2.0-OpenSSH-6.6.1 (service.version=6.6.1 ...)”

To run KALI Linux on multiple Hardware Management Consoles in a subnet, complete the following procedure:

- Start Metasploit framework that is available in KALI and run the following commands:

```
use auxiliary/scanner/ssh/ssh_version
set RHOSTS <Range of IPs in CIDR format> For example, set RHOSTS 10.0.1.0/24
set THREADS 100
run
```

How does IBM fix HMC security vulnerabilities?

IBM has a security incidence response process named PSIRT. Open Source and IBM components that are included with HMC are actively monitored and analyzed and fixes are provided by IBM. All supported releases of HMC get regular security fixes.

How to track new fixes on the HMC?

The security bulletin contains information about the vulnerability and fixes for supported HMC versions. To track fixes on HMC, you can:

- Search security bulletins at IBM Security Bulletin.
- Follow @IBMPowereSupp on Twitter for notifications.
- Subscribe to email notifications at IBM Support.

Security profiles: Global Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI-DSS)

Learn more on how Hardware Management Console (HMC) handles the privacy rights of the customers.

The Hardware Management Console (HMC) is a closed appliance that does not have any cardholder data. Hence, only a subset of requirements and security assessment procedures of IT security that are defined by PCI DSS are applicable for the HMC. Only trusted code that are distributed by IBM can be installed on HMC. As soon as any vulnerability is known through the IBM PSIRT process, a fix is published. The requirements and recommendations include the following items:

GDPR queries

Table 63. GDPR queries. The table provides information on the questions related to GDPR.

Questions	Answers
What kind of data are stored by the HMC?	The HMC stores Power hardware, PowerVM virtualization configuration, and performance metrics information.
Does the HMC process any personal data?	You can provide contact information for call home function. Providing contact information for call home function is optional.

Table 63. *GDPR queries (continued)*. The table provides information on the questions related to GDPR.

Questions	Answers
Which predefined accounts are used for system administration of the HMC?	The system administrator user uses the <i>hscroot</i> username.
Do any of the accounts in the HMC relates to a specific person?	No.
Is it mandatory to provide personal data in the HMC?	No. You do not need to provide personal data information. However, providing the information is optional.
Does the HMC log file have any personal data information?	No.
Is it possible to delete personal data completely and permanently?	Yes. Unconfigure call home.

PCI-DSS queries

Table 64. *PCI-DSS queries*. The table provides information on the questions related to PCI-DSS

Questions	Answers
How to install and maintain a firewall configuration to protect the data of the cardholder?	The HMC does not store or access any cardholder data. However, the HMC has a firewall configuration and you can control and enable specific ports.
Can I use vendor-supplied default value for system passwords and other security parameters?	Before you install a system on the network, change all the predefined passwords of the <i>hscroot</i> user.
How does the HMC protect the stored data of the cardholder?	The HMC does not store or access any cardholder data.
How does the HMC encrypt the data of the cardholder when the data is transmitted across open public networks?	The HMC does not store or access any cardholder data.
How to use and regularly update anti-virus software programs?	The HMC is a closed appliance, so malware cannot infect the HMC.
How to develop and maintain secure systems and applications?	You must install the required patches to your system manually from the IBM fix central site. Only trusted code that are distributed by IBM can be installed on the HMC.
Does the HMC restrict access to the cardholder data?	The HMC does not store or access any cardholder data.
How to assign a unique ID to each person who has access to the computer?	You can implement this requirement by ensuring that there are no shared IDs and you follow the password policies.
How to restrict the physical access to the data of the cardholder?	The HMC does not store or access any cardholder data.
How to track and monitor the access to network resources and to the cardholder data?	The HMC does not store or access any cardholder data.
How does the HMC test the security of the system and processes?	The scan tools are used to run security scans on all released version of the HMC. The scan tools include: <i>Qualys</i> , <i>Nessus</i> , <i>testssl</i> , <i>ssllscan</i> and <i>ASoC</i> .
How to maintain a security policy that includes information security for employees and contractors?	System administrator disables the remote user login, activates the user login on a need basis, and deactivates the user login when the access is no longer required.

HMC port locations

You can find part locations by using location codes. Use the HMC port location illustrations to map a location code to the HMC port position on the server.

Model 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

Use this diagram and table to map the HMC ports on the 8247-21L, 8247-22L, 8284-21A, or 8284-22A.

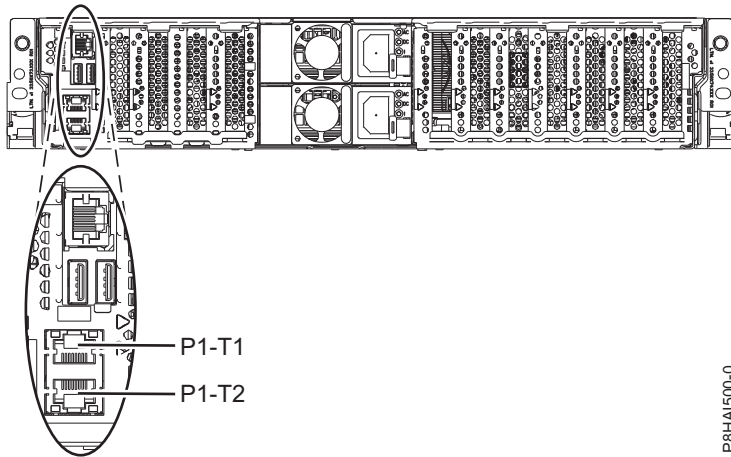


Figure 81. 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

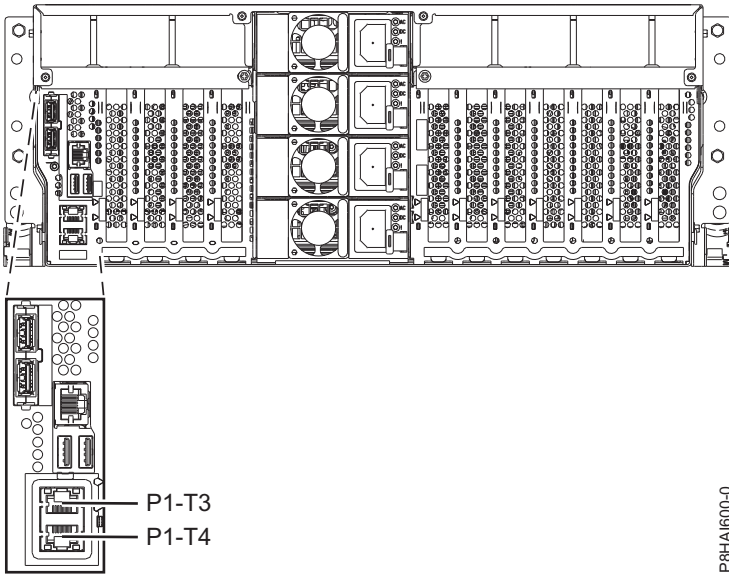
Table 65. 8247-21L, 8247-22L, 8284-21A, or 8284-22A HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-T1	No
HMC port 2	Un-P1-T2	No

For more information on HMC port locations about the 8247-21L, 8247-22L, 8284-21A, or 8284-22A, see Part location and location codes for 8247-21L, 8247-22L, or 8284-22A.

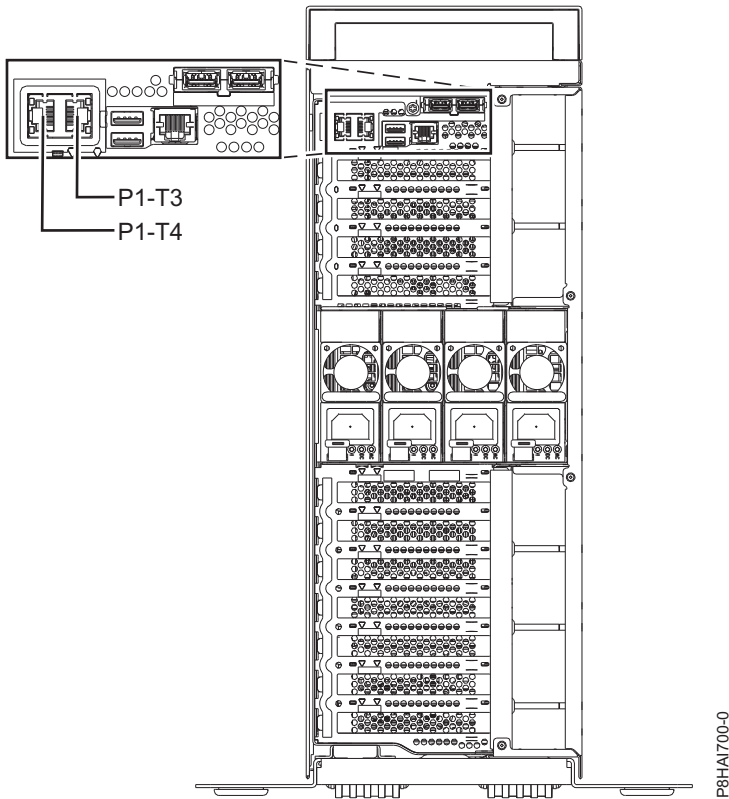
Model 8247-42L, 8286-41A, or 8286-42A HMC port locations

Use this diagram and table to map the HMC ports on the 8247-42L, 8286-41A, or 8286-42A.



P8HA1600-0

Figure 82. Rack view - 8247-42L, 8286-41A, or 8286-42A HMC port locations



P8HA1700-0

Figure 83. Tower view - 8286-41A HMC port locations

Table 66. 8247-42L, 8286-41A, or 8286-42A HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-T3	No
HMC port 2	Un-P1-T4	No

Table 66. 8247-42L, 8286-41A, or 8286-42A HMC port locations (continued)

Port	Physical location code	Identify LED
For more information about HMC port locations on the 8247-42L, 8286-41A, or 8286-42A, see Part location and location codes for 8247-42L, 8286-41A, or 8286-42A.		

Model 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Use this diagram and table to map the HMC ports on the 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME.

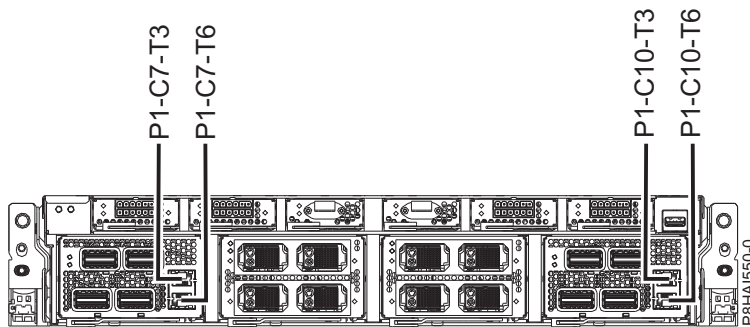


Figure 84. 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Table 67. 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC port locations

Port	Physical location code	Identify LED
Service processor card 1 - HMC port 1	Un-P1-C7-T3	No
Service processor card 1 - HMC port 2	Un-P1-C7-T6	No
Service processor card 2 - HMC port 1	Un-P1-C10-T3	No
Service processor card 2 - HMC port 2	Un-P1-C10-T6	No
For more information about HMC port locations on the 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME, see Part location and location codes for 9080-MHE, 9080-MME, 9119-MHE, or 9119-MME locations.		

Model 8408-44E and 8408-E8E HMC port locations

Use this diagram and table to map the HMC ports on the 8408-44E and 8408-E8E.

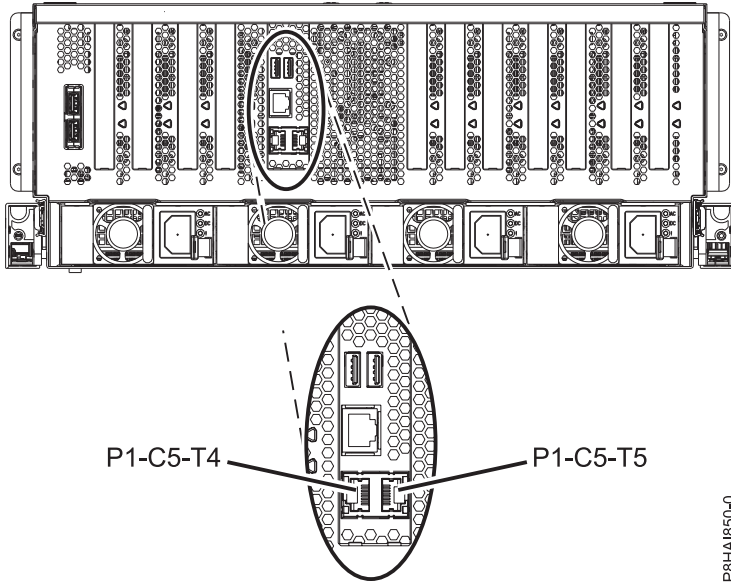


Figure 85. 8408-44E and 8408-E8E HMC port locations

Table 68. 8408-44E and 8408-E8E HMC port locations

Port	Physical location code	Identify LED
HMC port 1	Un-P1-C5-T4	No
HMC port 2	Un-P1-C5-T5	No

For more information about HMC port locations on the 8408-44E and 8408-E8E, see Part location and location codes for 8404-44E and 8408-E8E locations.

Notices

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

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

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

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

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

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

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

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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

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

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 IBM.

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

IBM'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 IBM's support websites for updated information and fixes applicable to the system and related software.

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Accessibility features for IBM Power Systems servers

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

Overview

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

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

The IBM Power Systems servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power Systems servers.

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

Keyboard navigation

This product uses standard navigation keys.

Interface information

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

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

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

Vendor software

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

Related accessibility information

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

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

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

Privacy policy considerations

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

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

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other

Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER8 processor and its features unless designated as electromagnetic compatibility (EMC) Class B in the feature information.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

CAN ICES-3 (A)/NMB-3(A)

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

The following is a summary of the VCCI Japanese statement in the box above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値： Knowledge Centerの各製品の
仕様ページ参照

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、PFC回路付)
- 換算係数 : 0

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

Electromagnetic Interference (EMI) Statement - People's Republic of China

声 明

此为 A 级产品,在生活环境中,该产品可能会造成无线电干扰。在这种情况下,可能需要用户对其干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 / EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road

Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC) Class B in the feature installation information.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

CAN ICES-3 (B)/NMB-3(B)

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
email: halloibm@de.ibm.com

VCCI Statement - Japan

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値 : Knowledge Centerの各製品の
仕様ページ参照

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、PFC回路付)
- 換算係数 : 0

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

IBM Taiwan Contact Information

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022/ EN 55032 Klasse B.

Terms and conditions

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

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

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

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

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

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

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

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



Printed in USA