Installing and Configuring the HMC

ESCALA

REFERENCE
86 A1 38EV 05

ESCALA

Installing and Configuring the HMC

Hardware

May 2009

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 38EV 05

Trademarks and Acknowledgements

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Contents

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

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

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

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

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

(C026)

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

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

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

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

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

The equipment is suitable for installation in the following:

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

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

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

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

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

Chapter 1. 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.

May 2009

The following updates have been made to the content:

- Added information about the USB memory device for Updating, upgrading, and migrating your HMC machine code.

Chapter 2. Installing and configuring the Hardware Management Console

Describes how to install the 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.

Road map for installing the Hardware Management Console

Follow the steps in this road map to perform a first-time HMC installation and configuration.

Use the information in this road map to guide you through the high-level tasks that you need to successfully set up the HMC for the first time. To install and configure the HMC, you must do the following:

1. Prepare for the installation and configuration
2. Install the HMC hardware
3. Configure the HMC software

Planning for HMC installation and configuration

This section describes the high-level planning tasks you must perform before you install and configure your HMC.

To plan for HMC installation and configuration, do the following:

1. Ensure that your HMC hardware meets the requirements to manage your server and obtain and install the latest HMC code.
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.
5. If you will use an open network to manage a Flexible Service Processor (FSP), you must manually set the FSP's address through the Advanced System Management Interface (ASMI) menus. A private, nonroutable 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 connect to use the call-home function. Call home options include 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 as which roles they will be given.
10. Document the following company contact information that will be needed when you configure call home:
    - Company name
    - Administrator contact
    - E-mail address
    - Telephone numbers

   - Fax numbers
   - The street address of the HMC's physical location

11. If you plan to use e-mail to notify operators or systems administrators when information is sent to IBM Service through call-home function, identify the Simple Mail Transfer Protocol (SMTP) server and the e-mail addresses you will use.
12. 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 you connect the first time to the managed server's FSP.
13. For detailed information about the planning tasks you should complete before performing a first-time installation, see Preparing for HMC configuration.

Install the HMC hardware. To Install the HMC into a rack, see "Installing your rack-mounted HMC." To install a desk-side HMC, see "Installing your stand-alone HMC" on page 5.

Installing your rack-mounted HMC

A procedure that describes how to install the Hardware Management Console into an existing rack enclosure.

To install the HMC into a rack, do the following:

1. Complete a parts inventory.
2. Locate the rack-mounting hardware kit and the system rail assemblies that were included with your system unit.
3. Determine where to install the HMC and monitor into the rack and mark the location.
4. Install the slide rails for the HMC and monitor into the rack.
5. Install the HMC and Monitor on the slide rails.
6. Install the cable-management arm.
7. Identify the location of the HMC connectors.
8. Attach the monitor cable to the monitor connector, tighten the screws, and connect the keyboard and mouse to Universal Serial Bus (USB) ports on the HMC.
9. Attach the power cord to the monitor.
10. Ensure that the voltage selection switch on the HMC is set to the voltage used in your world region.
11. Plug the power cord into the HMC.
12. Connect the optional modem.
13. Connect the Ethernet cable to the HMC in eth0 port.
14. Connect the Ethernet port on the HMC to the Ethernet port that is labeled **HMC1** on the managed system. If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **HMC2** on the managed system.
15. If you use an external modem, plug the modem power supply cord into the HMC modem.
16. 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, uninstalled managed system, do not connect the managed system to a power source at this time.
17. For detailed rack-mounted HMC installation procedures, go to: Installing the HMC into a rack (http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/iphai/hmccr4iphbf.htm).

Configure the HMC. For more information, see “Configuring the HMC for the first time.”

Installing your stand-alone HMC

Use high-level tasks to install the stand-alone (or deskside) HMC. Describes how to physically install a deskside, or stand-alone, HMC.

To cable your stand-alone HMC, do the following:

1. Position the HMC in the correct location.
2. Identify the location of the HMC connectors.
3. Attach the monitor cable to the monitor connector, tighten the screws, and connect the keyboard and mouse to Universal Serial Bus (USB) ports on the HMC.
4. Attach the power cord to the monitor.
5. Ensure that the voltage selection switch on the HMC is set to the voltage used in your world region.
6. Plug the power cord into the HMC.
7. Connect the optional modem.
8. Connect the Ethernet cable to the HMC on the eth0 port.
9. Connect the Ethernet port on the HMC to the Ethernet port that is labeled **HMC1** on the managed system. If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **HMC2** on the managed system.
10. If you use an external modem, plug the modem power supply cord into the HMC modem.
11. 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, uninstalled managed system, do not connect the managed system to a power source at this time.
12. For detailed stand-alone HMC cabling procedures, see Cabling your stand-alone HMC (http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/iphai/desksideinstall.htm).

Configure the HMC. For more information, see “Configuring the HMC for the first time.”

Configuring the HMC for the first time

Learn more about how to configure the HMC for the first time.

You can configure the HMC by using several different methods. The following procedure describes the most common way to configure the HMC.

To configure the HMC, do the following steps:

1. Turn on the HMC by pressing the power button.
2. Wait for the HMC to automatically select the default language and locale preference.
3. Accept the HMC license agreements. If you decline the HMC 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:
    - ID: `hscroot`
    - Password: `abc123`

    The Guided Setup wizard opens.
6. Click **OK** on the Guided Setup entry window.
7. Complete the steps in the Guided Setup wizard. 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 have not connected the Ethernet crossover cable to your managed system, do so now and power on the managed server.
10. In the HMC navigation area, click **Service Management**.
11. In the contents area, click **Authorize User**. The Authorize User window opens.
12. Enter your IBM ID in the field and click **OK**.

For more information about other ways to configure the HMC, see Configuring the HMC (http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/iphai/configure.htm).

Installation and configuration scenarios

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

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 scenario that best matches the task you want to perform.

Note: If you are managing POWER6 systems, you must be using HMC Version 7 or later. For more information, see "Determining your HMC machine code version and release" on page 61.

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 24 "Preparing for HMC configuration" on page 22
2. Unpack the hardware.	
3. Cable the HMC hardware.	"Cabling your stand-alone HMC" on page 30 "Cabling your rack-mounted HMC" on page 40
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 using the fast path through the Guided Setup wizard" on page 42 "Configuring the HMC using the HMC menus" on page 43
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 64
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	

Migrating HMC Version 6 code to HMC Version 7 code

Learn more about the high-level tasks you must perform when you migrate from an HMC Version 6 to an HMC Version 7.

If you have an existing HMC and want to migrate from Version 6 to Version 7, you must complete the following high-level tasks:

Table 3. Tasks you need to perform when migrating an HMC Version 6 to an HMC Version 7

Task	Where to find related information
1. Ensure your HMC hardware supports HMC Version 7 code.	
2. Ensure that your HMC code level is 6.12 or higher. If not, you must upgrade your existing HMC code.	“Determining your HMC machine code version and release” on page 61 “Upgrading your HMC software” on page 64
3. Upgrade your HMC to Version 7.	“Upgrading your HMC software” on page 64
4. Optional: upgrade your managed system’s firmware level to the highest available level.	2
5. If you have a second HMC, perform steps 1-4 for that HMC.	

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 4. 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 24
3. Unpack the hardware.	

Table 4. Tasks you need to perform when adding a second HMC to an existing installation (continued)

Task	Where to find related information
4. Cable the HMC hardware.	“Cabling your stand-alone HMC” on page 30 “Cabling your rack-mounted HMC” on page 40
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 61 “Upgrading your HMC software” on page 64
8. Access the Guided setup wizard or use the HMC menus to configure the HMC.	“Configuring the HMC using the HMC menus” on page 43
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 53
10. Attach the server to 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 41. 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 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 running in the logical partitions, as well as 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 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, 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 could access HMCs and other managed units 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.

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 scenario, 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.

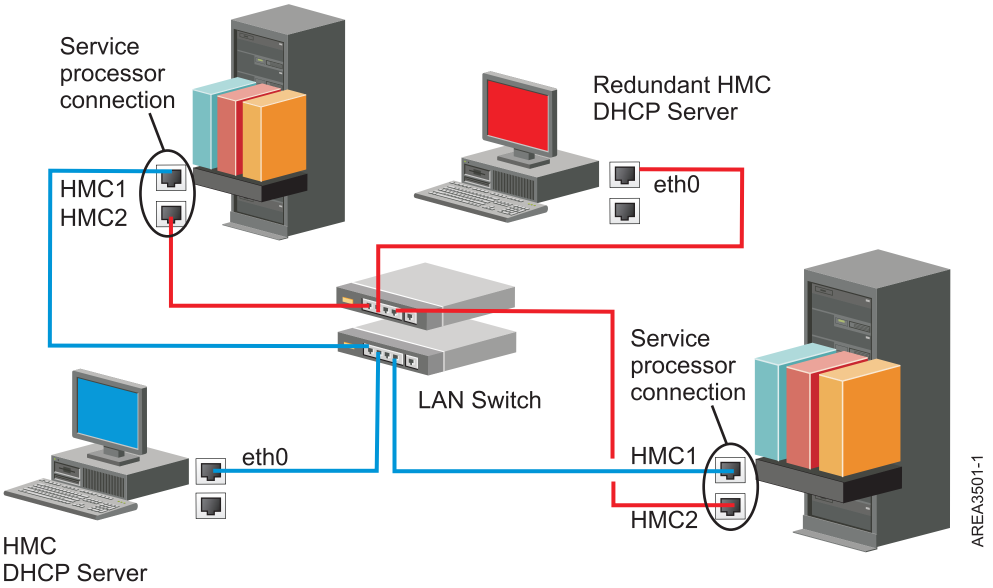
The HMC itself provides its own firewall on each of its network interfaces. A basic firewall is automatically configured when you run the HMC Guided Setup wizard, but you customize your firewall settings after the initial HMC installation and configuration.

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 49.

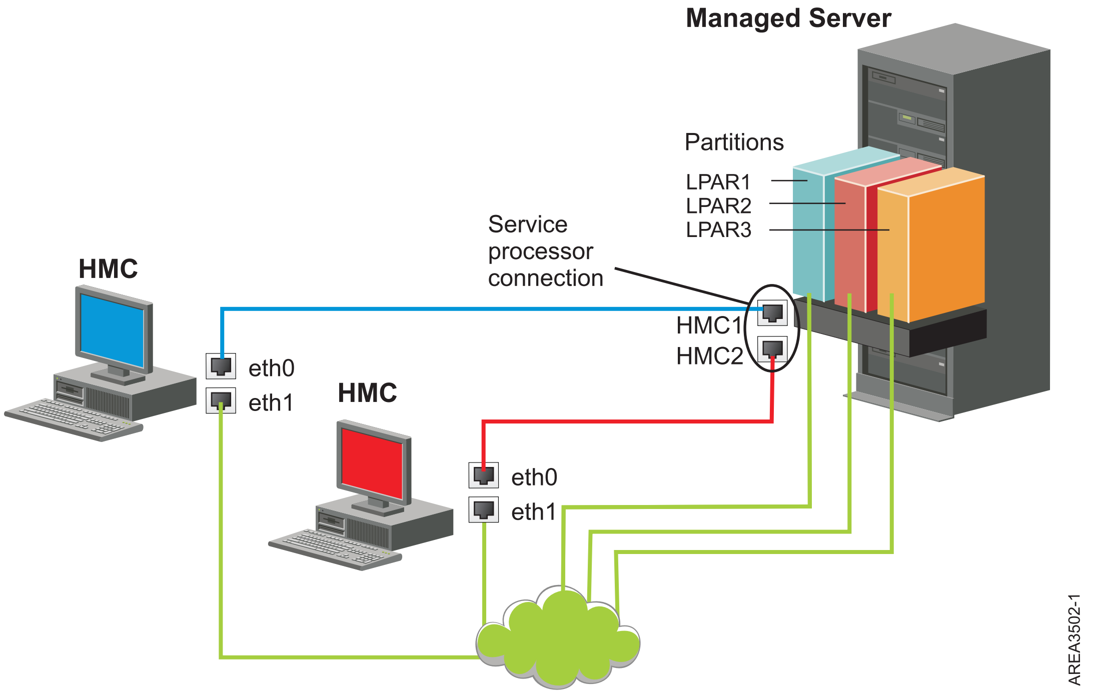

Service processor connection
HMC1
HMC2
Redundant HMC DHCP Server
eth0
LAN Switch
Service processor connection
HMC1
HMC2
eth0
HMC DHCP Server
AREA3501-1

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 49.

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.

You have two communication choices when configuring 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 used, see “Choosing an internet protocol” on page 13.

The advantages to using an Internet connection can include:

- Significantly 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.

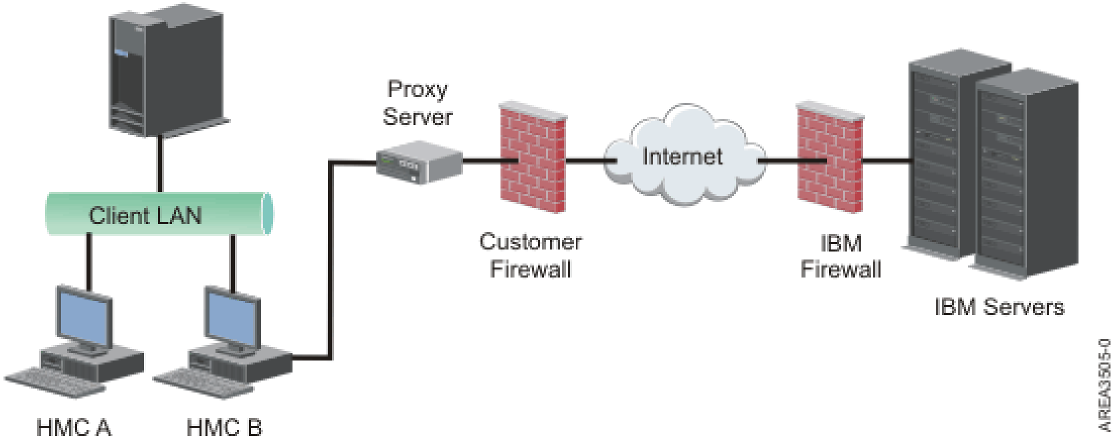
- All data transferred between the HMC and the IBM Service Support System are encrypted using a high-grade encryption. Depending upon the connectivity method chosen, it is encrypted using either SSL or IPSec Encapsulating Security Payload (ESP).
- When initializing the encrypted connection the HMC authenticates 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 may be able to connect indirectly to the Internet 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 may support logging and audit facilities.

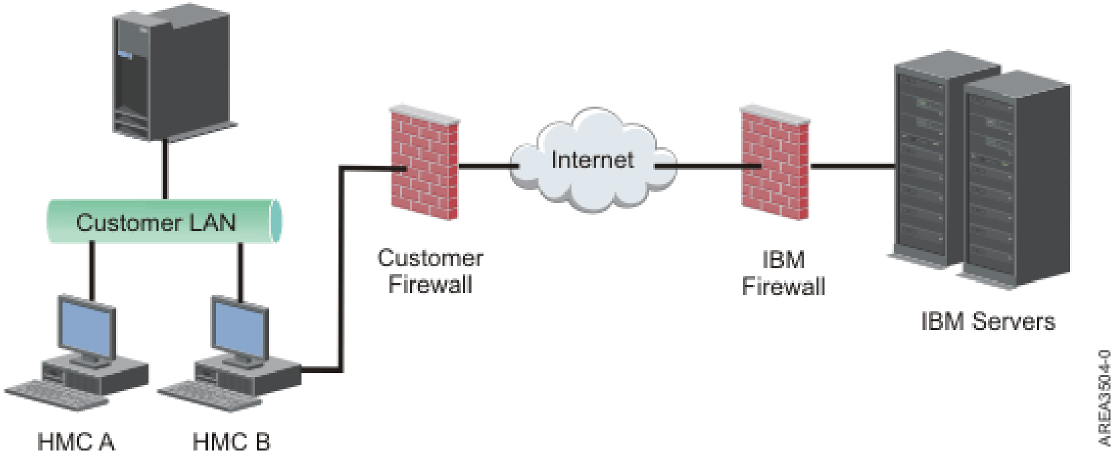
To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616) and the CONNECT method. Optionally, basic proxy authentication (RFC 2617) may be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.



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 13 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 13, 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”) 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 50 and “Setting the IPv6 address” on page 50.

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 the Americas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

The following IPv4 addresses are for countries and regions other than the Americas:

- 129.42.160.48
- 129.42.160.50
- 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.

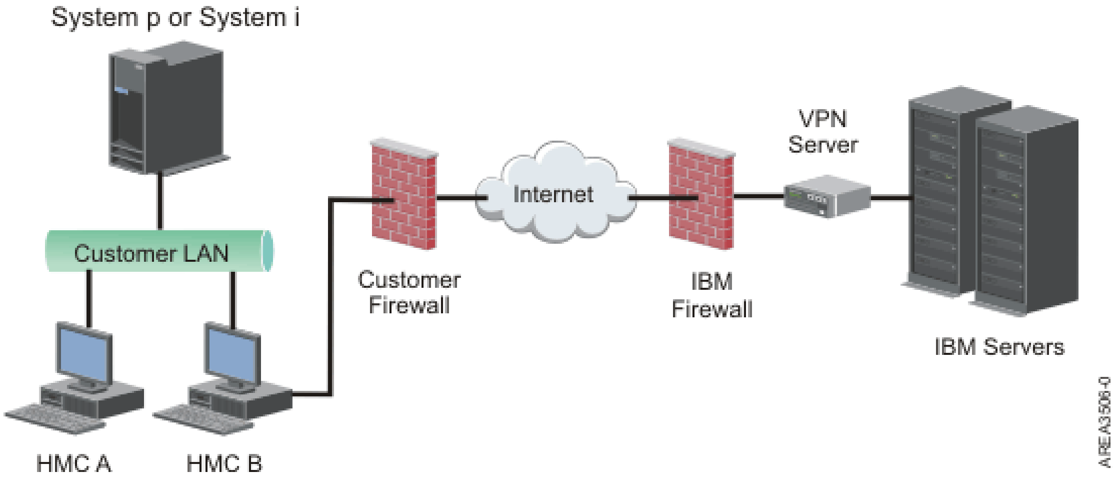
The HMC uses the following IPv6 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity:

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

Using a virtual private network to connect to remote support

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

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 may 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 using a LAN-based VPN, see "Configuring the HMC network types" on page 45.

VPN Server Address List

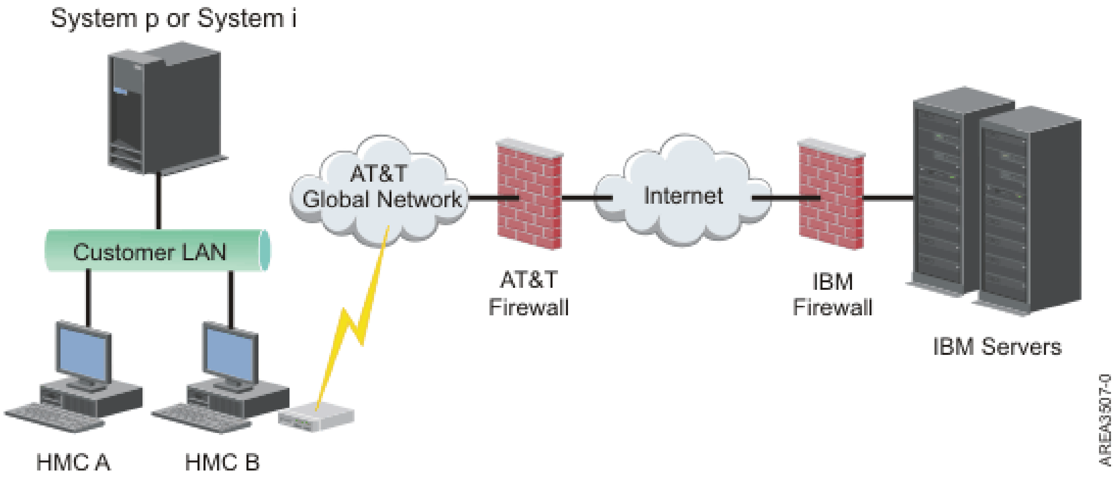
Lists the servers used by an HMC when the HMC is configured to use Internet VPN connectivity.

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 #1
- 207.25.252.196 IBM VPN Server #2

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.



For more information about connecting to remote support using the telephone and modems, see "Configuring the HMC network types" on page 45.

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

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 41. 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 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 running in the logical partitions, as well as 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 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, 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 could access HMCs and other managed units 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.

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 scenario, 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.

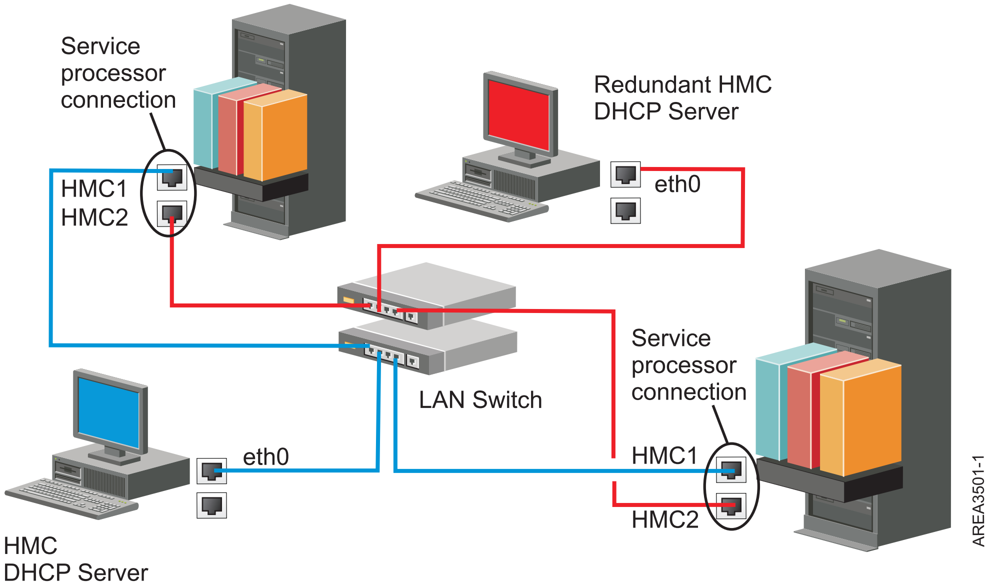
The HMC itself provides its own firewall on each of its network interfaces. A basic firewall is automatically configured when you run the HMC Guided Setup wizard, but you customize your firewall settings after the initial HMC installation and configuration.

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 49.

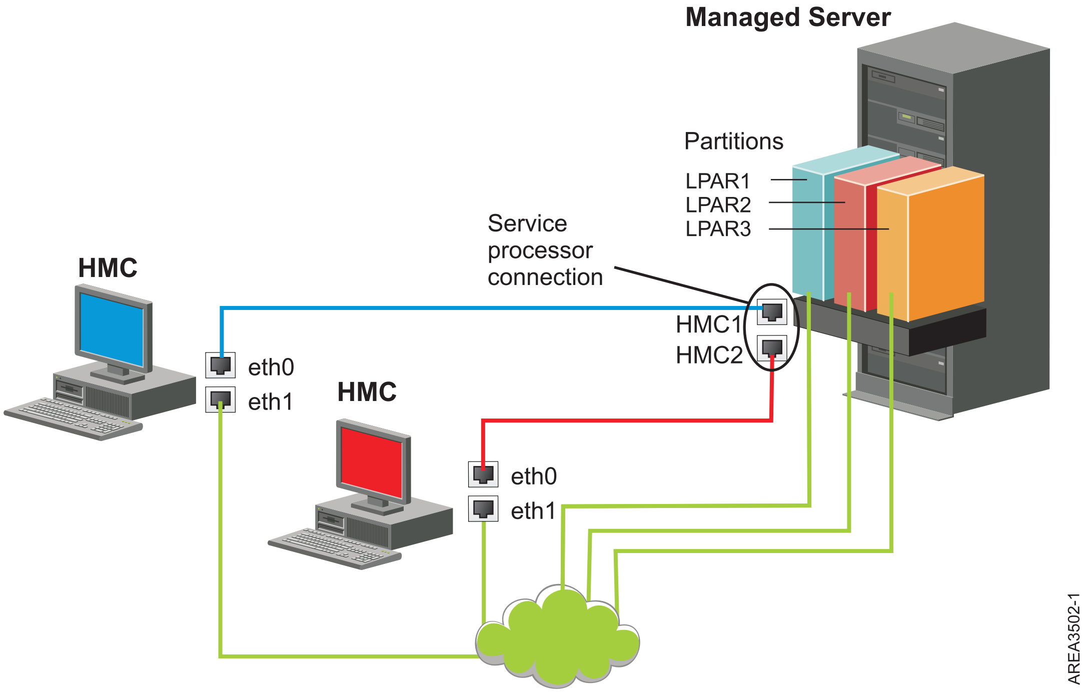


This figure shows a redundant HMC environment with two managed systems. The first HMC is connected to the first port on each FSP, and the redundant HMC is connected to the second port on each HMC. Each HMC is configured as a DHCP server, using a different range of IP addresses. The connections are on 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 49.

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.

You have two communication choices when configuring 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 used, see "Choosing an internet protocol" on page 13.

The advantages to using an Internet connection can include:

- Significantly 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:

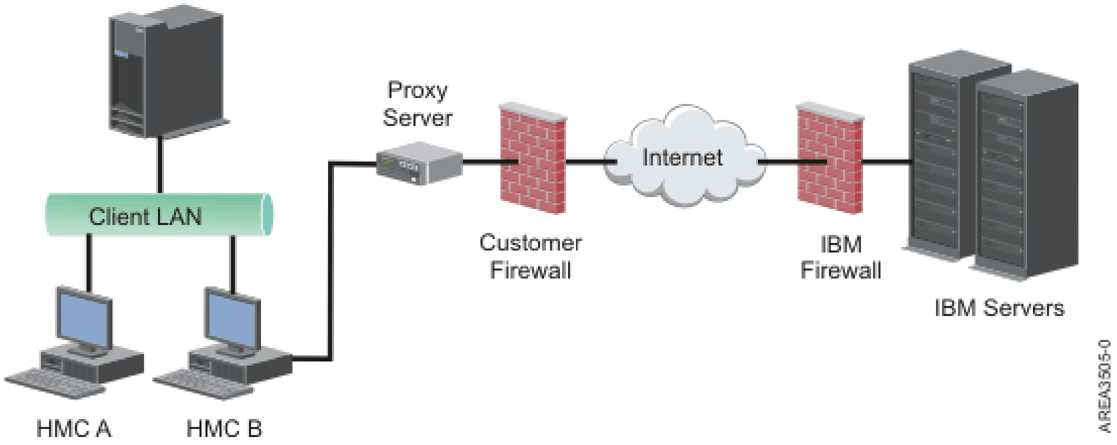
- Remote Support Facility requests are always initiated from the HMC to IBM. An inbound connection is never initiated from the IBM Service Support System.
- All data transferred between the HMC and the IBM Service Support System are encrypted using a high-grade encryption. Depending upon the connectivity method chosen, it is encrypted using either SSL or IPSec Encapsulating Security Payload (ESP).
- When initializing 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 may be able to connect indirectly to the Internet 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 may support logging and audit facilities.

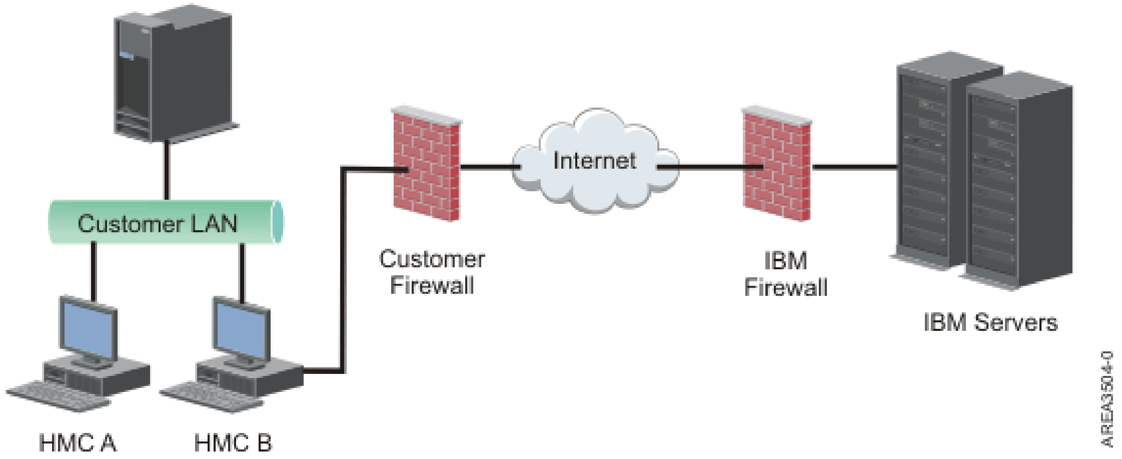
To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616) and the CONNECT method. Optionally, basic proxy authentication (RFC 2617) may be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.



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 13 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 13, 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 13) 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 50 and "Setting the IPv6 address" on page 50.

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 the Americas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

The following IPv4 addresses are for countries and regions other than the Americas:

- 129.42.160.48
- 129.42.160.50
- 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.

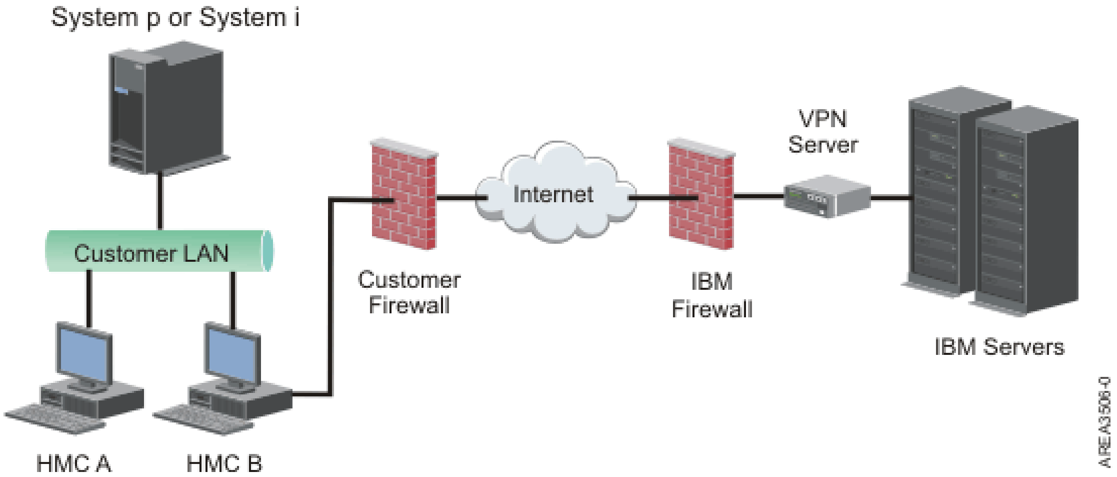
The HMC uses the following IPv6 addresses to contact IBM service and support when it is configured to use Internet SSL connectivity:

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

Using a virtual private network to connect to remote support

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

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 may 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 14 for a list of addresses you can use.

For more information about how to connect to the Internet using a LAN-based VPN, see “Configuring the HMC network types” on page 45.

VPN Server Address List

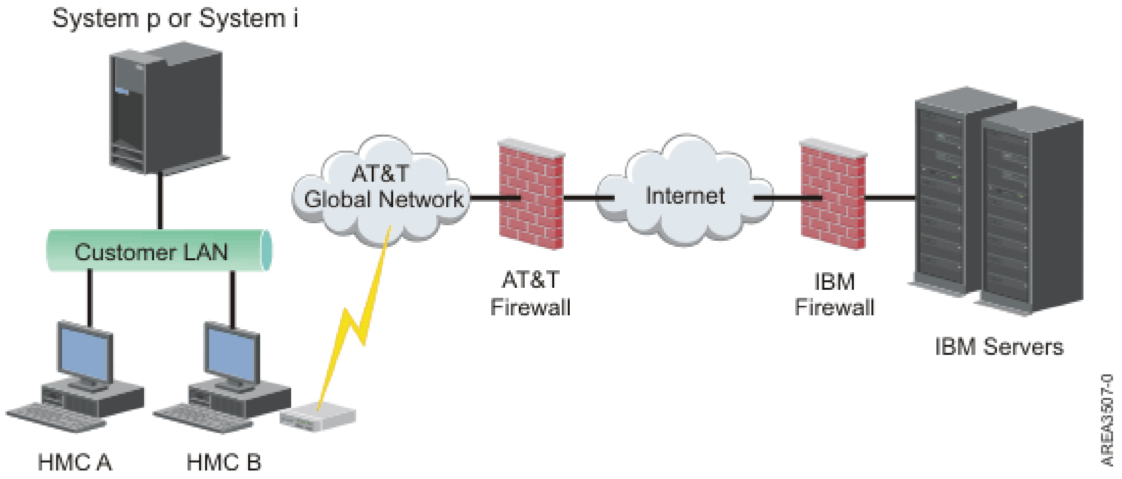
Lists the servers used by an HMC when the HMC is configured to use Internet VPN connectivity.

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 #1
- 207.25.252.196 IBM VPN Server #2

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.



For more information about connecting to remote support using the telephone and modems, see "Configuring the HMC network types" on page 45.

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 ″HMC Connectivity Security for IBM POWER5™ and POWER6™ Processor-Based Systems″ at the following Web link: http://w3-03.ibm.com/sales/support/ShowDoc.wss?docid=PSW03007USEN&infotype=SA &infosubtype=WH&node=&ftext=hardware%20management&sort=title&showDetails=true&hitsize=50 &campaign=&offset=2950

To prepare for HMC configuration, do the following:

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 9.
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."

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 8 for more information. Connectivity from the HMC can either be on a private or open network.

Note: Additional connectivity and security information is available. For more information, see ″HMC Connectivity Security for IBM POWER5 and POWER6 Processor-Based Systems″ at the following Web link: http://w3-03.ibm.com/sales/support/ShowDoc.wss?docid=PSW03007USEN&infotype=SA &infosubtype=WH&node=&ftext=hardware%20management&sort=title&showDetails=true&hitsize=50 &campaign=&offset=2950

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 auto detection unless you have a requirement to specify a fixed media speed.

	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 9.

	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:

	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		

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 13.

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:

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

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

	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 50. For more information about using only IPv6 addresses, see “Using only IPv6 addresses” on page 50.

Using IPv4

Complete the following tables for Ethernet adapters specified as open networks 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:				

	eth0	eth1	eth2	eth3

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:

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.

Email Address(es):	
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

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 11.

_____ 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. Check **Use SSL Proxy** if you want to configure the use of encrypted SSL using an indirect connection using an SSL Proxy.

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 13.

___ 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.

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 15.

___ This HMC

___ Another HMC

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

Table 5. 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

List your IBM ID __________________________

List any additional IBM IDs ________________________

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 Web site 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 Web site. 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.

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.

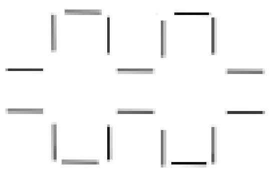
1. Ensure that you position the HMC in the correct location.
2. Attach the monitor cable to the monitor connector, and tighten the screws.
3. Attach the power cord to the monitor.
4. Ensure that the voltage selection switch on the HMC is set to the voltage used in your world region. The voltage selection 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. For more information, see “Deciding which connectivity method to use for the call-home server” on page 11.

   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:



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. For more information, see "Deciding which connectivity method to use for the call-home server" on page 11.

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 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 8.
10. If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled **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.

    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 41.

Installing the HMC into a rack

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

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

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

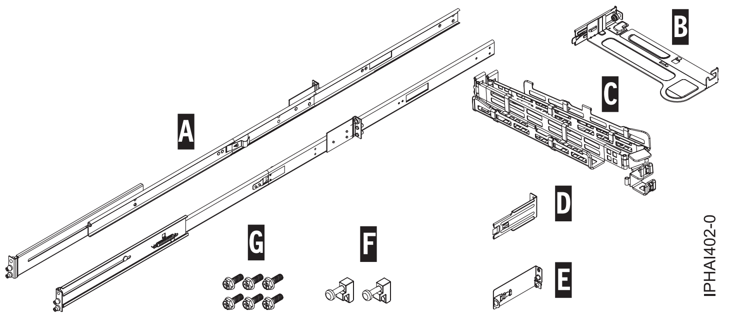


Figure 1. Rail Kit

Table 6. 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.

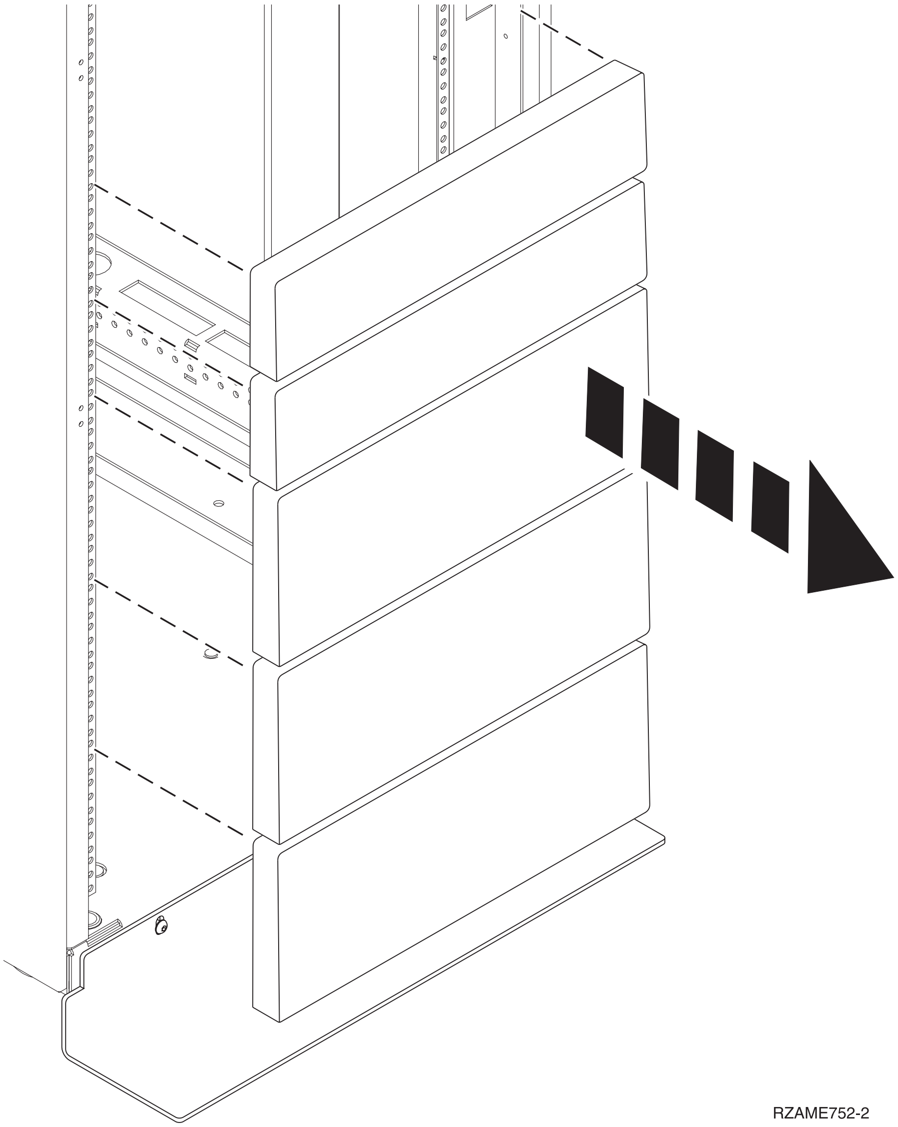


Figure 2. Removing the filler panels.

3. Remove the front and back 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 a rack-mounting template:

If you need to mark the location without a template, use the procedure in this section to perform this task.

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 where in the rack to place the system. 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 the 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 33 for the corresponding holes located on the left side of the rack.
5. Go to the back 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 slide rails into the rack

To install slide rails into the rack, use this procedure.

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

1. Insert the right slide rail **A**, marked *right*, into the back-right rack mounting flange **B** locations. The two rail pins will protrude through the bottom and middle holes **B** on the EIA unit.

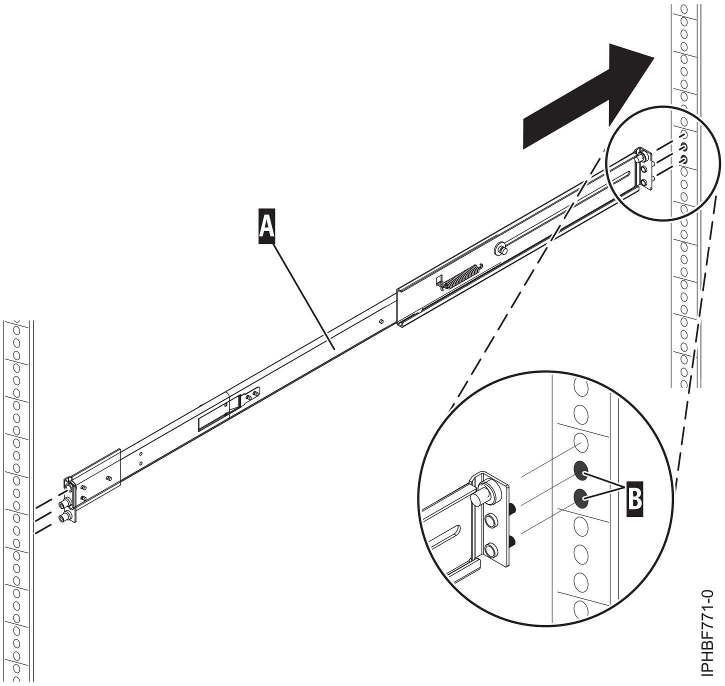


Figure 3. Installing the right slide rail into the back of the rack

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

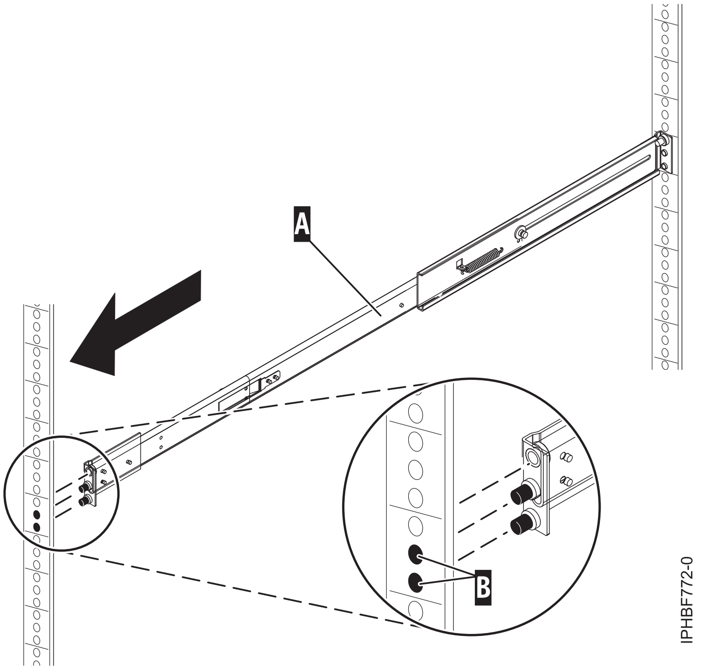


Figure 4. Installing the right slide rail into the front of the rack

3. Repeat these steps to install the left slide rail, 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**.

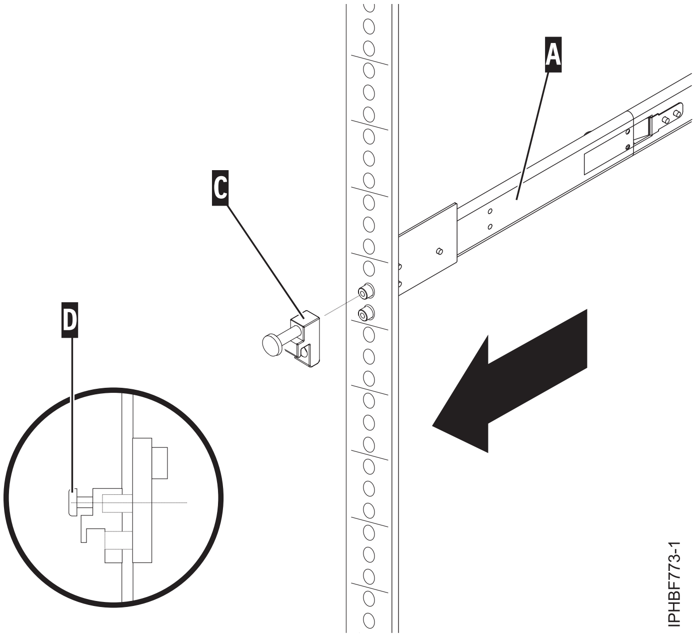


Figure 5. Installing the latch strike to the front of the rails

5. Repeat the previous step to install the latch strike on the front of the left slide rail.

6. Move to the back of the rack. Screw **F** to attach the cable-management arm mounting bracket **E** to the back of the left rail **G**. Finger-tighten the screw.

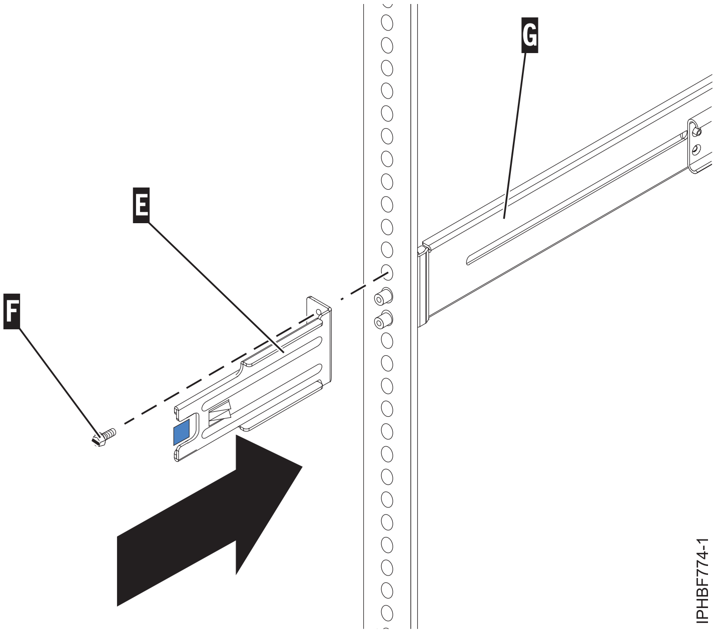


Figure 6. Attaching the cable-management bracket to the back-left rail

7. If you do not plan to transport this system, continue with “Installing the HMC on the slide rails” on page 37. If you plan to transport this system, insert screw **I** to attach the cable-management arm support bracket **H** to the back-right rail **A**.

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

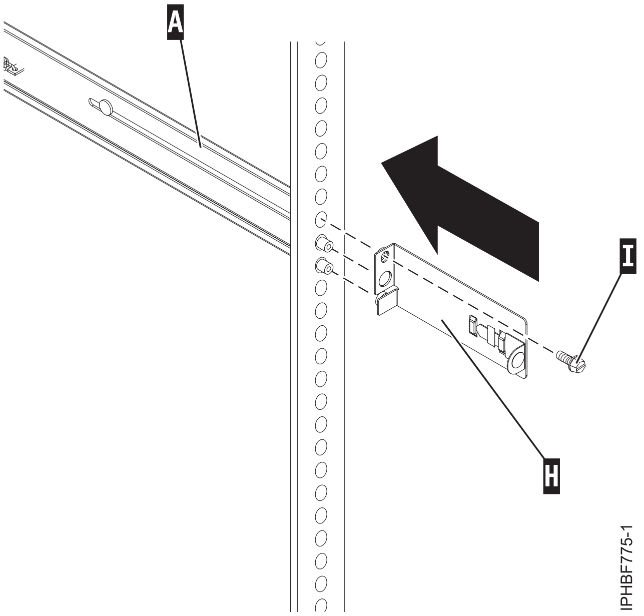


Figure 7. Attaching the cable-management support bracket to the back-right rail.

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.

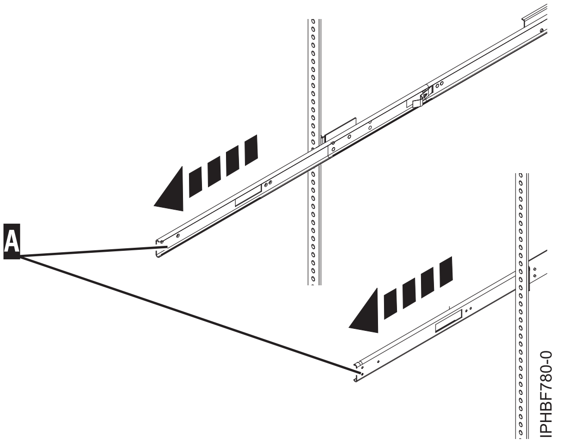


Figure 8. Extending the slide rails.

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 back of the HMC, between the rail guides.

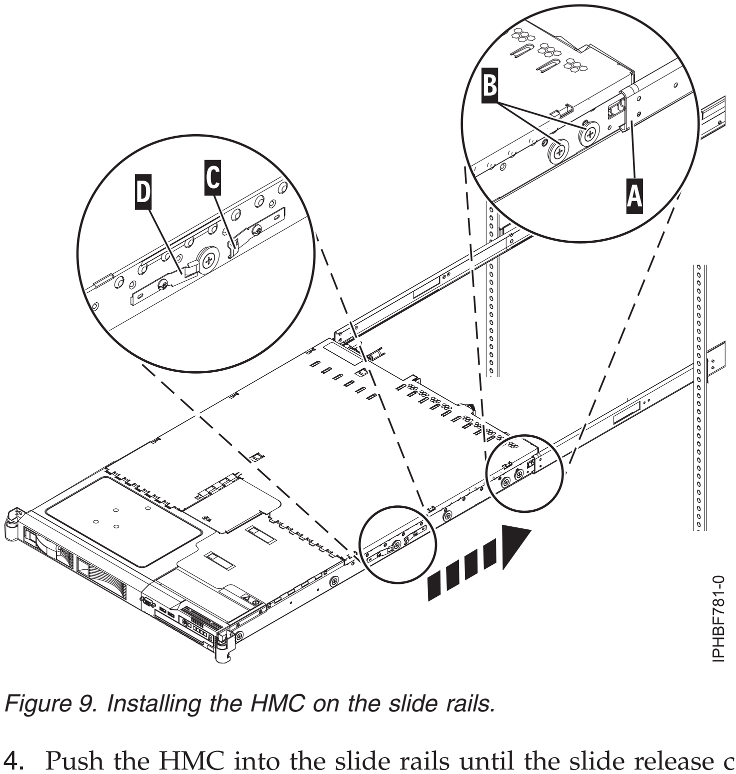


Figure 9. Installing the HMC on the slide rails.

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.

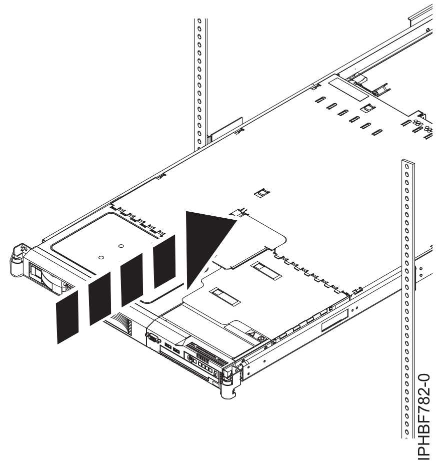


Figure 10. Slide the HMC into the rack.

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.

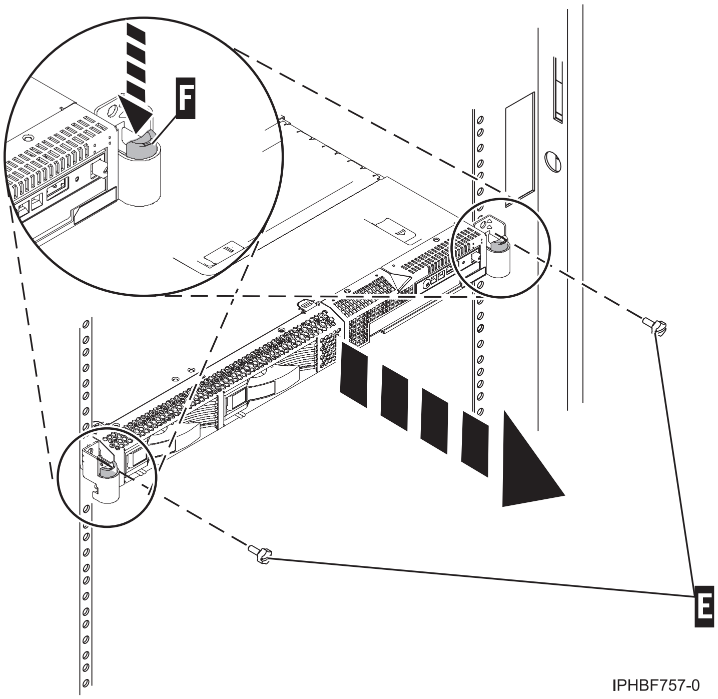


Figure 11. Rack latches and screws.

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 back of the rack, locate the cable-management arm flange **A** located on the fixed back portion of the left system rail assembly (viewing from the back 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.

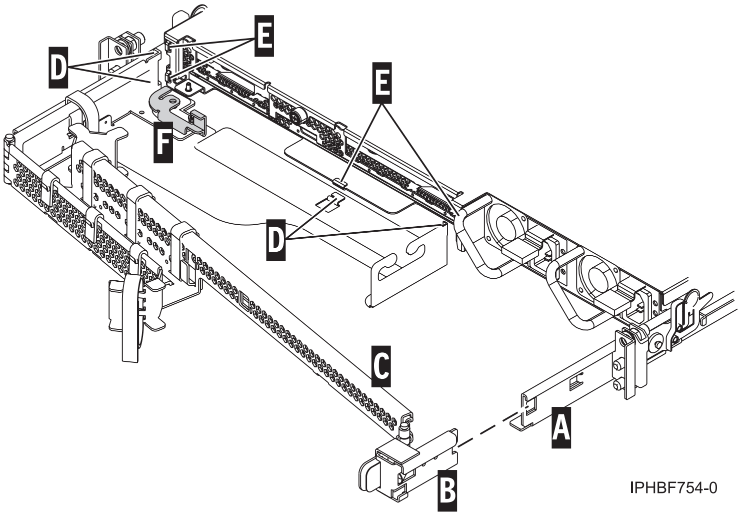


Figure 12. Cable-management arm and system unit.

3. Attach the other end of the cable-management arm **C** to the back of the HMC. Align the tabs **D** on the cable-management arm with the slots **E** on the back 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

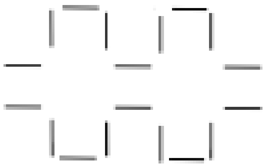
Learn how to physically install your rack-mounted HMC.

1. Ensure that you position the HMC in the correct location.
2. Install the HMC into a rack. For more information, see “Installing the HMC into a rack” on page 31. 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 11.

   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 11.

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 8.

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."

Configuring the HMC

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 will need to complete the steps successfully. See "Preparing for HMC configuration" on page 22 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 24 and then return to this section.

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

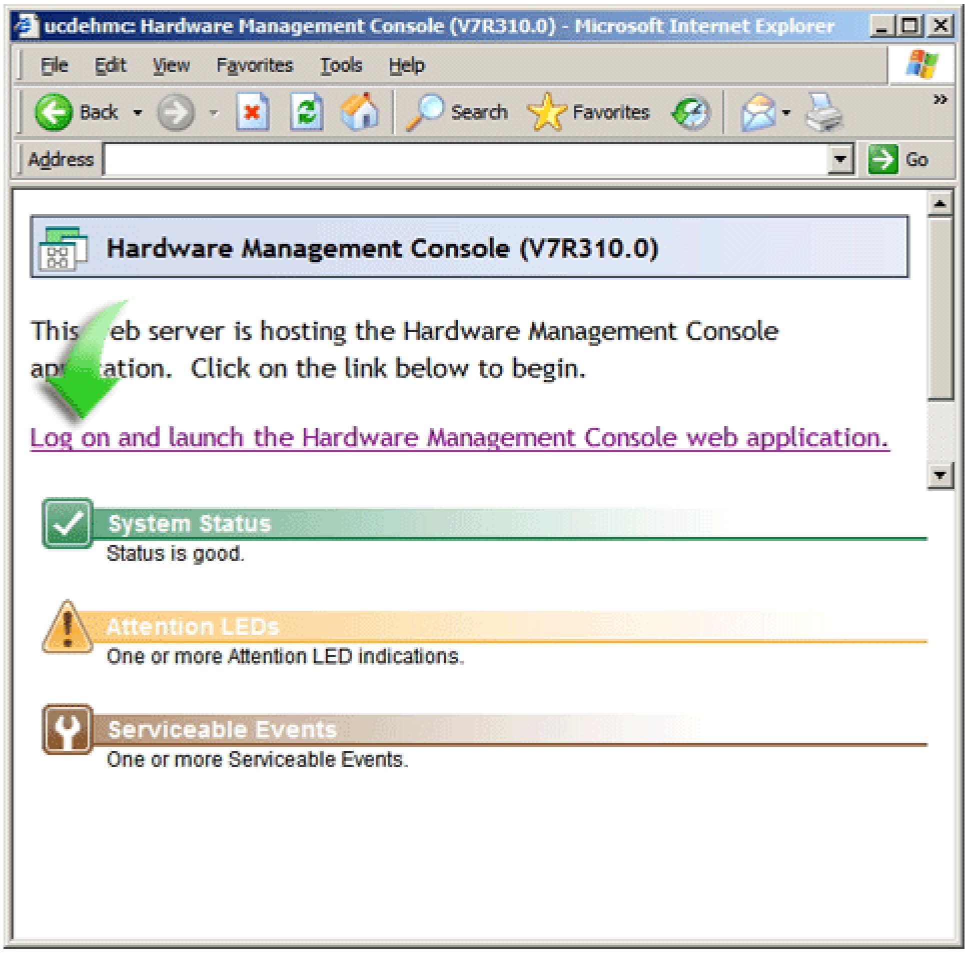
In most cases, the HMC can be set up to operate effectively using many of the default settings. Use this fast path checklist to prepare the HMC for service. When you have completed these steps, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected)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


ucdehmc: Hardware Management Console (V7R310.0) - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go

Hardware Management Console (V7R310.0)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

System Status
Status is good.

Attention LEDs
One or more Attention LED indications.

Serviceable Events
One or more Serviceable Events.

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 **Service Management**.
11. In the contents area, click **Authorize User**. The Authorize User window opens.
12. Enter your IBM ID in the field and click **OK**.

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 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 22.

Table 7. 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 44
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 45
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 51
8. If you are using an open network and a fixed IP address, configure domain name services.	"Configuring domain name services" on page 52

Table 7. Manual HMC configuration tasks and where to find related information (continued)

Task	**Where to find related information**
9. If you are using a fixed IP address and have DNS enabled, configure domain suffixes.	"Configuring domain suffixes" on page 52
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 53
11. Connect the managed system to a power source.	
12. Set passwords for the managed system, and each of the ASMI passwords (general and admin)	"Set passwords for the managed system" on page 58
13. Access ASMI to set the date and time on the managed system.	
14. Start the managed system and return to this checklist when you have completed this step.	
15. Ensure that you have one logical partition on the managed system.	
16. Optional: add another managed system and return to this checklist when you have completed this step.	
17. Optional: If you are installing a new server with your HMC, configure the logical partitions and install the operating system.	
18. If you are not installing a new server at this time, perform optional postconfiguration tasks to further customize your configuration.	"Postconfiguration steps" on page 59

Starting the HMC

You can long 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:

1. Turn on the HMC by pressing the power button.
2. If English is your language preference, continue with step 5.

   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 using the following default user ID and password:

   ID: `hscroot`

   Password: `abc123`
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 contents 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 8. 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 24
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 47
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	“Setting the media speed” on page 48
b. Select the open network type.	“Selecting a private or open network” on page 49
c. Set static addresses.	“Setting the IPv4 address” on page 50
d. Set the firewall.	“Changing HMC firewall settings” on page 50
e. Configure the default gateway.	“Configuring a routing entry as the default gateway” on page 51
f. Configure DNS.	“Configuring domain name services” on page 52
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 58

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 9. 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 24
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 47
3. Configure the HMC as a DHCP server.	“Configuring the HMC as a DHCP server” on page 49
4. Test the connection between the managed server and the HMC.	“Testing the connection between the HMC and the managed system” on page 58

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 10. 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 24
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 47
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	“Setting the media speed” on page 48
b. Select the open network type.	“Selecting a private or open network” on page 49
c. Set static addresses.	“Setting the IPv4 address” on page 50
d. Set the firewall.	“Changing HMC firewall settings” on page 50
e. Configure the default gateway.	“Configuring a routing entry as the default gateway” on page 51
f. Configure DNS.	“Configuring domain name services” on page 52
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 58

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 11. 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 24
2. Identify the Ethernet ports for your HMC.	“Identifying the Ethernet port defined as eth0” on page 47
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	“Setting the media speed” on page 48

Table 11. Configuring HMC settings to use an open network to connect to remote users (continued)

Task	Where to find related information
b. Select the open network type.	"Selecting a private or open network" on page 49
c. Set static addresses.	"Setting the IPv4 address" on page 50
d. Set the firewall.	"Changing HMC firewall settings" on page 50
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 51
f. Configure DNS.	"Configuring domain name services" on page 52
g. Configure suffixes.	"Configuring domain suffixes" on page 52
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 12. 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 24
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 54 "Choosing existing call-home servers to connect to service and support for this HMC" on page 56
3. Verify that your call-home configuration is working	"Verifying that your connection to service and support is working" on page 57
4. Authorize users to view collected system data	"Authorizing users to view collected system data" on page 57
5. Schedule transmission of system data	"Transmitting service information" on page 57

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 13. 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. • 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	The definitions depend upon the type of Ethernet adapter you have installed: • 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 and duplex mode of the Ethernet adapter.

The default for the adapter settings is **Autodetection**. If this adapter is connected to a LAN switch, you must configure the required settings manually. To set the media speed, 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. Click the **Lan Adapter** tab.
6. In the Local area network information section, select the media speed.
7. 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. 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 DHCP Server section, check **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, the you do not have the option to check the **Enable DHCP** box.
7. Enter the address range of the DHCP server.
8. 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 9.

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. Click **OK**.
4. Click **Remote Operation**.
5. Select **Enabled** 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 Command Execution**.
3. Click **OK**.
4. Click **Remote Operation**.
5. Select **Enabled** 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. Check **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 45.

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

1. In the Navigation area, click **HMC Management**.
2. In the Contents area, click **LDAP Configuration**. 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 45.

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 contents 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 contents 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 contents 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 22.
- 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 15.
- 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 contents 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 using LAN connectivity, the phone or modems, or VPN.

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 22.
- 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 9.
- 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** tab.
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** tab, 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.

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 22.
- 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, check **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, select the **Local Modem** tab.
7. In the Local Modem tab, check the **Allow local modem dial for service** box.
8. In the Local Modem tab, check the **Modem Configuration** box.
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, check the **Wait for dial tone** box. Fill in any dial prefix string that is required to obtain an outside line.
10. Click **OK**.
11. In the Local Modem tab, 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.

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 22.
- 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 15.
- 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, check **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, click the **Internet VPN** tab.
7. In the Internet VPN tab, check the **Allow A VPN and an existing internet connections for service** box.
8. In the Internet VPN tab, click **Test**.
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 contents area, click **Manage Outbound Connectivity**. The Call-Home Server Consoles window opens.
3. Click the **Use discovered call-home server consoles** box. 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. Check **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. Check 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 24.

To authorize users to view collected system data, do the following:
1. In the navigation area, select **Service Management**.
2. In the contents area, 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 Web site 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." 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 **Service Management**.
2. In the contents area, click **Transmit Service Information.**
3. Complete the tasks in the Transmit Service Information window, and click **OK**.

Set 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.

Update 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**.

Update your Advanced System Management (ASM) general password:

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**.

Reset the Advanced System Management (ASM) administrator password:

You can reset the administrator password by either of the following methods:

- Contact an authorized service provider
- Use the reset toggle jumpers on the service processor

To reset the toggle jumper on the service processor, move both service processor reset toggle switches from their current position to the opposite position.

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. To view the PDF file of Logical partitioning, approximately 1 MB in size, see

http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/iphat/iphat.pdf .

To understand how the HMC can be used in a network, see "HMC network connections" on page 8.

For more information about configuring the HMC to connect to a network, see "Configuring the HMC using the HMC menus" on page 43.

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, DVD, via FTP, or over the network.

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:

- DVD media
- 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 drive to a remote system

You can use your HMC to back up the entire hard disk 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 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 (i.e. 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 47.
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 Web site 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 59. 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. Check 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 through 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://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html.
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 Web site, 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 Web site at http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html
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 Web site at http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html
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 59
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 through 9.

Note: If you are upgrading from HMC with Version 6 with HMC Version 7, refer to "Migrating the machine code on an HMC from Version 6 to Version 7" on page 67.

Step 1. Obtain the upgrade

You can order the HMC machine code upgrade through the Fix Central Web site.

To obtain the upgrade through the Fix Central Web site, do the following:

1. From a computer or server with an Internet connection, go to the Hardware Management Console Web site at http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html.
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 Pane, 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 contents 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" on page 67.

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 contents 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.

Migrating the machine code on an HMC from Version 6 to Version 7

Learn how to move the machine code on an HMC from Version 6 to Version 7 while maintaining your HMC configuration data.

To migrate machine code on an HMC from Version 6 to Version 7, perform Steps 1 through 9.

Important: To migrate to Version 7 Release 0, you must be at a minimum of HMC machine code Version 6 Release 1.2.

Ensure you have met the minimum requirements

To migrate the machine code on an HMC from Version 6 to Version 7, you must first ensure that you have met the following minimum requirements:

- Your HMC is at level 6.12 or higher. For more information about checking your HMC code level and release, see "Determining your HMC machine code version and release" on page 61.
- Your system firmware is at its latest level.
- You have performed the network integrity check

- Your HMC hardware supports this upgrade.

Step 1. Obtain the upgrade

To obtain the upgrade, do the following:

You can order the HMC machine code upgrade through the Fix Central Web site, by contacting service and support, or by downloading it to an FTP server.

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. Navigate to the HMC version you want.
6. Locate the download and ordering section.

   Note: If you do not have access to the Internet, contact service and support to order the upgrade on DVD.
7. Follow the prompts to submit your order.
8. 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 **Licensed Internal Code Maintenance** folder.
2. Select **HMC Code Update**.
3. In the Status area, look for the version and release of your HMC machine code.
4. Record the current version and release.

   Important: To upgrade from HMC machine code 6.1.3 to 7.3.4.0, you must first apply a fix. For more information, see http://www.ibm.com/eserver/support/fixes.
5. 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 Contents area, select the managed system.
2. From the menu, click **Selected > Profile Data > Backup**.
3. Type a backup file name and record this information.
4. Click **OK**.
5. Repeat steps 1 through 4 for each managed system.

Step 4. Back up critical console information

Back up critical console information 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: If you choose to back up the console data to removable media, you must have that media available.

To back up critical console information, do the following:

1. Choose from the following options:
   - If you do *not* plan to back up to DVD-RAM, continue with the next step.
   - If you plan to back up to DVD-RAM, perform the following steps:
     a. Insert the DVD-RAM into the drive.
     b. In the navigation area, click **Licensed Internal Code Maintenance**.
     c. Select **HMC Code Update**.
     d. Select **Format Removable Media**.
     e. Select **Format DVD-RAM**.
     f. Click **OK**.
     g. Continue with the next step.
2. Select **Back up Critical Console Data**.
3. Select an archive option. You can back up to a DVD in the HMC, 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 DVD, choose **Back up to DVD on local system** and follow the instructions.
   - To back up to a mounted remote system, choose **Backup to mounted remote system** and follow the instructions.
   - To back up to a remote FTP site, choose **Send backup critical data to remote site** and follow the instructions.
4. 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 HMC configuration information, follow these steps:

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" on page 70.

Step 6. Record remote command status

1. In the navigation area, select **HMC Management**.
2. Select **HMC Configuration**.
3. In the tasks list, click **Enable/Disable Remote Command Execution**.
4. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
5. Click **Cancel**.
6. 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. 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.

The upgrade data will be restored automatically during the installation procedure.

Note: Only one level of backup data is allowed. Each time you save upgrade data, the previous level is overwritten.

1. In the navigation area, open the **Licensed Internal Code** folder.
2. Select **HMC Code Update**.
3. Select **Save Upgrade Data**.
4. Select **DVD** and click **Continue**.
5. Insert the DVD media into the drive.
6. Click **Continue** to start the task.
7. 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.
8. Click **OK**.
9. Click **Cancel**.
10. Continue with "Step 8. Upgrade the HMC software from Version 6 to Version 7."

Step 8. Upgrade the HMC software from Version 6 to Version 7

Important: To upgrade from HMC machine code 6.1.3 to 7.3.4.0, you must first apply a ptf. For more information, see http://www.ibm.com/eserver/support/fixes.

To upgrade the HMC software, restart the system with the DVD-RAM in the DVD drive.

1. Insert the HMC Product Installation media.
2. Perform the following steps:
   a. From the HMC menu bar, select **Console** → **Exit**.
   b. Click **Exit now**.
   c. From the logout list, select **Reboot Console** and click **OK**. The HMC restarts and system information scrolls on the window.
3. Select **Upgrade** and click **Next**.
4. When the warning is displayed, 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.
5. Select **Upgrade from media** and click **Next**.

6. Confirm the settings and click **Finish**.
7. 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.
8. When prompted, remove the first media and then insert the second media.
9. Select **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC will display status messages as it installs the packages.
10. Click **Log on and launch the Hardware Management Console web application**.
11. Log in to the HMC interface.
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

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.

Step 10. Obtain an update package

You can order the HMC update packages through the Fix Central Web site, by contacting service and support, or by downloading it to an FTP server.

1. From a computer or server with an Internet connection, go to http://www.ibm.com/eserver/support/fixeshttp://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. Navigate to the HMC version you want.
6. Locate the download and ordering section.

   Note: If you do not have access to the Internet, contact service and support to order the upgrade on DVD.
7. Follow the prompts to download the update package to removable media or submit your order.

Step 11. Reschedule operations for this HMC

When you upgrade the HMC, you must manually reschedule the operations you scheduled using the previous HMC version.

1. In the Navigation area, click **HMC Management**.
2. In the Work area, click **Schedule Operations**.

Appendix. Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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

Electronic emission notices

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER6 processor.

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

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC 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.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@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.

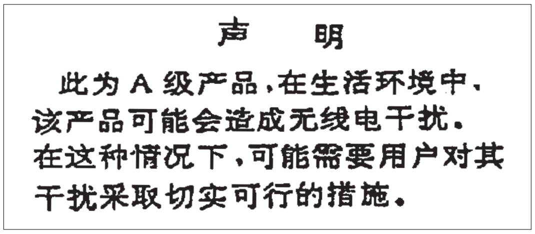
VCCI Statement - Japan

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス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。

The following is a summary of the VCCI Japanese statement in the box above.

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Electromagnetic Interference (EMI) Statement - People's Republic of China

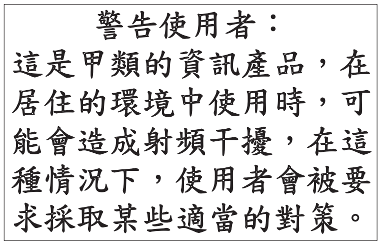


声　明

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。

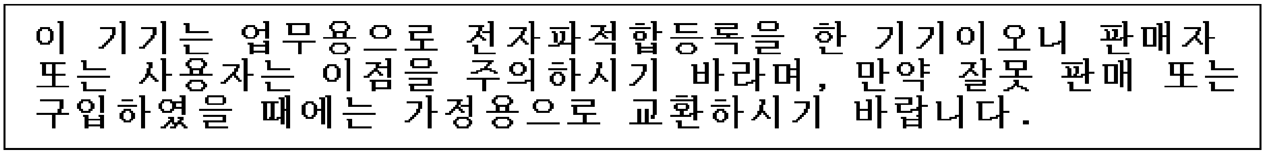
The following is a summary of the EMI Taiwan statement above.

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 업무용으로 전자파적합등록을 한 기기이오니 판매자
또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는
구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

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 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A.

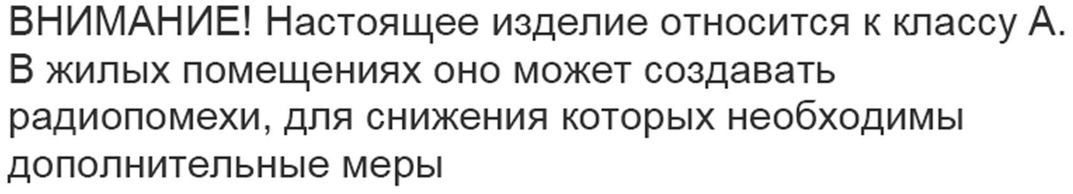
Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 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

Terms and conditions

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

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

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

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

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

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

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

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 38EV 05