Power Systems

Installing and configuring the Hardware Management Console

IBM

Note

Before using this information and the product it supports, read the information in "Safety notices" on page v, "Notices" on page 89, the *IBM Systems Safety Notices* manual, G229-9054, and the *IBM Environmental Notices and User Guide*, Z125–5823.

This edition applies to IBM® Hardware Management Console Version 10 Release 2 Maintenance Level 1030 and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2021, 2024.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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

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

German safety information

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

Laser safety information

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

Laser compliance

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

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

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard: If IBM supplied the power cord(s), connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product. Do not open or service any power supply assembly. Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. For AC power, disconnect all power cords from their AC power source. For racks with a DC power distribution panel (PDP), disconnect the customer's DC power source to the PDP.
- When connecting power to the product ensure all power cables are properly connected. For racks with AC power, connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate. For racks with a DC power distribution panel (PDP), connect the customer's DC power source to the PDP. Ensure that the proper polarity is used when attaching the DC power and DC power return wiring.
- Connect any equipment that will be attached to this product to properly wired outlets.

© Copyright IBM Corp. 2021, 2024

- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Do not attempt to switch on power to the machine until all possible unsafe conditions are corrected.
- When performing a machine inspection: Assume that an electrical safety hazard is present. Perform all continuity, grounding, and power checks specified during the subsystem installation procedures to ensure that the machine meets safety requirements. Do not attempt to switch power to the machine until all possible unsafe conditions are corrected. Before you open the device covers, unless instructed otherwise in the installation and configuration procedures: Disconnect the attached AC power cords, turn off the applicable circuit breakers located in the rack power distribution panel (PDP), and disconnect any telecommunications systems, networks, and modems.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

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

  To Connect: 1) Turn off everything (unless instructed otherwise). 2) Attach all cables to the devices. 3) Attach the signal cables to the connectors. 4) For AC power, attach the power cords to the outlets. 5) For racks with a DC power distribution panel (PDP), restore the power from the Customer's DC power source and turn on the circuit breakers located in the PDP. 6) Turn on the devices.
- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)

(R001 part 1 of 2):

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

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

- Stability hazard:
  - The rack may tip over causing serious personal injury.
  - Before extending the rack to the installation position, read the installation instructions.
  - Do not put any load on the slide-rail mounted equipment mounted in the installation position.
  - Do not leave the slide-rail mounted equipment in the installation position.
- Each rack cabinet might have more than one power cord.
  - For AC powered racks, be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.

  - For racks with a DC power distribution panel (PDP), turn off the circuit breaker that controls the power to the system unit(s), or disconnect the customer’s DC power source, when directed to disconnect power during servicing.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (R001 part 1 of 2)

(R001 part 2 of 2):

CAUTION:

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

- *(For fixed drawers.)* This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack. (R001 part 2 of 2)

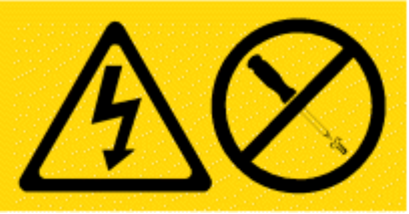
CAUTION: Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building.

- Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must observe the following precautions:
  - Remove all devices in the 32U position (compliance ID RACK-001 or 22U (compliance ID RR001) and above.
  - Ensure that the heaviest devices are installed in the bottom of the rack cabinet.

  - Ensure that there are little-to-no empty U-levels between devices installed in the rack cabinet below the 32U (compliance ID RACK-001 or 22U (compliance ID RR001) level, unless the received configuration specifically allowed it.
- If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.
- If the rack cabinet you are relocating was supplied with removable outriggers they must be reinstalled before the cabinet is relocated.
- Inspect the route that you plan to take to eliminate potential hazards.
- Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.
- Verify that all door openings are at least 760 x 2083 mm (30 x 82 in.).
- Ensure that all devices, shelves, drawers, doors, and cables are secure.
- Ensure that the four leveling pads are raised to their highest position.
- Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.
- Do not use a ramp inclined at more than 10 degrees.
- When the rack cabinet is in the new location, complete the following steps:
  - Lower the four leveling pads.
  - Install stabilizer brackets on the rack cabinet or in an earthquake environment bolt the rack to the floor.
  - If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.
- If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.

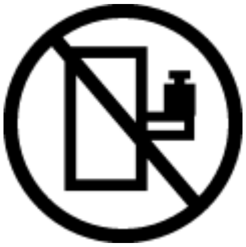
(R002)

(L001)



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

(L002)



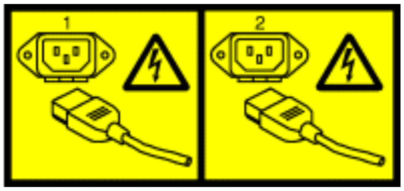
⚠ **DANGER:** Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices. In addition, do not lean on rack-mounted devices and do not use them to stabilize your body position (for example, when working from a ladder). Stability hazard:

- The rack may tip over causing serious personal injury.

- Before extending the rack to the installation position, read the installation instructions.
- Do not put any load on the slide-rail mounted equipment mounted in the installation position.
- Do not leave the slide-rail mounted equipment in the installation position.

(L002)

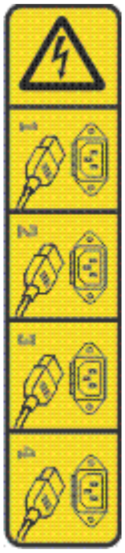
(L003)



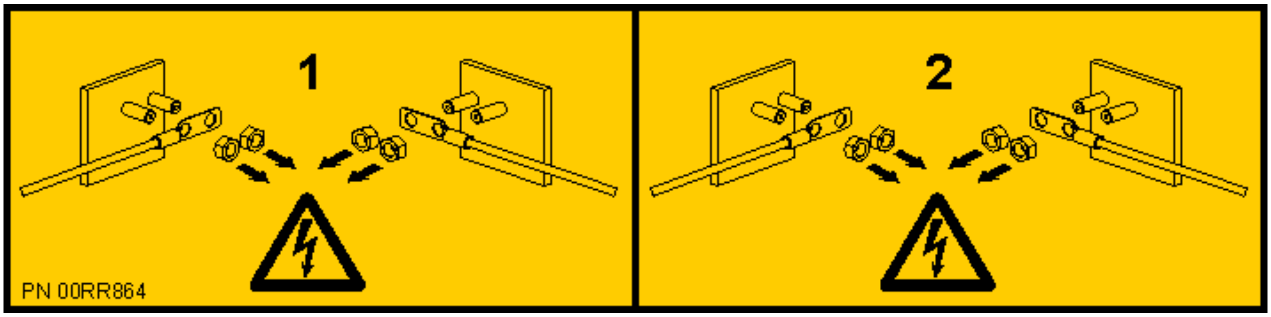
or

or

or



or



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

(L007)

CAUTION: A hot surface nearby. (L007)

(L008)

CAUTION: Hazardous moving parts nearby. (L008)

(L018)

or

CAUTION: High levels of acoustical noise are (or could be under certain circumstances) present. Use approved hearing protection and/ or provide mitigation or limit exposure. (L018)

(L031)

⚠ **CAUTION:**

Enclosure Integrity.

- Access covers are intended only for occasional removal.
- Follow documented procedures when opening during live or temporary service.
- When service is complete, promptly reinstall all covers, lids, and/or doors for correct operation. (L031)

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

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

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

(C026)

⚠ **CAUTION:** Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. Although shining light into one end and looking into the other end of a disconnected optical fiber to verify the continuity of optic fibers may not injure the eye, this procedure is potentially dangerous. Therefore, verifying the continuity of optical fibers by shining light into one end and looking at the other end is not recommended. To verify continuity of a fiber optic cable, use an optical light source and power meter. (C027)

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

⚠ **CAUTION:** Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information:

- Laser radiation when open.
- Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

(C030)

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

Do Not:

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

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

⚠ **CAUTION:** Regarding IBM provided VENDOR LIFT TOOL:

- Operation of LIFT TOOL by authorized personnel only.
- LIFT TOOL intended for use to assist, lift, install, remove units (load) up into rack elevations. It is not to be used loaded transporting over major ramps nor as a replacement for such designated tools like pallet jacks, walkies, fork trucks and such related relocation practices. When this is not practicable, specially trained persons or services must be used (for instance, riggers or movers).
- Read and completely understand the contents of LIFT TOOL operator's manual before using. Failure to read, understand, obey safety rules, and follow instructions may result in property damage and/or personal injury. If there are questions, contact the vendor's service and support. Local paper manual must remain with machine in provided storage sleeve area. Latest revision manual available on vendor's web site.
- Test verify stabilizer brake function before each use. Do not over-force moving or rolling the LIFT TOOL with stabilizer brake engaged.
- Do not raise, lower or slide platform load shelf unless stabilizer (brake pedal jack) is fully engaged. Keep stabilizer brake engaged when not in use or motion.
- Do not move LIFT TOOL while platform is raised, except for minor positioning.
- Do not exceed rated load capacity. See LOAD CAPACITY CHART regarding maximum loads at center versus edge of extended platform.
- Only raise load if properly centered on platform. Do not place more than 200 lb (91 kg) on edge of sliding platform shelf also considering the load's center of mass/gravity (CoG).
- Do not corner load the platforms, tilt riser, angled unit install wedge or other such accessory options. Secure such platforms -- riser tilt, wedge, etc options to main lift shelf or forks in all four (4x or all other provisioned mounting) locations with provided hardware only, prior to use. Load objects are designed to slide on/off smooth platforms without appreciable force, so take care not to push or lean. Keep riser tilt [adjustable angling platform] option flat at all times except for final minor angle adjustment when needed.
- Do not stand under overhanging load.
- Do not use on uneven surface, incline or decline (major ramps).
- Do not stack loads.
- Do not operate while under the influence of drugs or alcohol.
- Do not support ladder against LIFT TOOL (unless the specific allowance is provided for one following qualified procedures for working at elevations with this TOOL).
- Tipping hazard. Do not push or lean against load with raised platform.
- Do not use as a personnel lifting platform or step. No riders.
- Do not stand on any part of lift. Not a step.
- Do not climb on mast.
- Do not operate a damaged or malfunctioning LIFT TOOL machine.
- Crush and pinch point hazard below platform. Only lower load in areas clear of personnel and obstructions. Keep hands and feet clear during operation.
- No Forks. Never lift or move bare LIFT TOOL MACHINE with pallet truck, jack or fork lift.
- Mast extends higher than platform. Be aware of ceiling height, cable trays, sprinklers, lights, and other overhead objects.
- Do not leave LIFT TOOL machine unattended with an elevated load.
- Watch and keep hands, fingers, and clothing clear when equipment is in motion.

- Turn Winch with hand power only. If winch handle cannot be cranked easily with one hand, it is probably over-loaded. Do not continue to turn winch past top or bottom of platform travel. Excessive unwinding will detach handle and damage cable. Always hold handle when lowering, unwinding. Always assure self that winch is holding load before releasing winch handle.
- A winch accident could cause serious injury. Not for moving humans. Make certain clicking sound is heard as the equipment is being raised. Be sure winch is locked in position before releasing handle. Read instruction page before operating this winch. Never allow winch to unwind freely. Freewheeling will cause uneven cable wrapping around winch drum, damage cable, and may cause serious injury.
- This TOOL must be maintained correctly for IBM Service personnel to use it. IBM shall inspect condition and verify maintenance history before operation. Personnel reserve the right not to use TOOL if inadequate. (C048)

⚠ **CAUTION:** This equipment is not suitable for use in locations where children are likely to be present. (C052)

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 intra-building ports of this equipment are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building 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.

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

Installing the HMC virtual appliance

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

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

- Kernel-based Virtual Machine (KVM) on Ubuntu 18.04 LTS or Red Hat® Enterprise Linux® 8.0 or 9.0
- Xen on SUSE Linux Enterprise Server 12
- VMware ESXi 6.5, 7.0 or 7.0.2

The HMC virtual appliance supports the following POWER virtualization hypervisors:

- PowerVM®

Minimum requirements for running the HMC virtual appliance:

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

  Note:

  PowerVM virtualization hypervisor requires 160 GB of disk space. 500 GB of memory is recommended.

  The minimum PowerVM processor requirement is 1.0 processing units and four shared virtual processors in capped sharing mode. Using dedicated processor is not recommended. 16 GB of memory is recommended.

Notes:

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

Performance and scale requirements:

- When the HMC is at V9.2.950.0, or later, a single HMC can manage up to 48 systems and 2000 partitions across the systems that are managed by the HMC with the following requirements:
  - 16 GB memory for 1 - 500 partitions
  - 32 GB memory for 500 - 2000 partitions
- You can refer to the corresponding product documentation to find the maximum number of systems and partitions that an HMC can manage, when the HMC is used in combination with Cloud Management Console (CMC), PowerVC, VM High Availability/Disaster Recovery (HA/DR).

Related information

HMC V8 network installation images and installation instructions

© Copyright IBM Corp. 2021, 2024

Installing the HMC virtual appliance on x86

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

Installing the HMC virtual appliance by using the KVM hypervisor

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

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

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

1. Verify that virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) versions 8.0 or 9.0 and Ubuntu versions 18.04 or 20.04.
2. Download the `<KVM vHMC installation filename>.tar.gz` file to the host system.
3. Run the following command: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Run the following command: `cd /var/lib/libvirt/images/vHMC`.
5. To extract the virtual disk images, run the following command:

   ```
   tar -zxvf <KVM vHMC installation filename>.tgz
   ```

   Note: In this command, specify the full path of your HMC virtual appliance .tar file.
6. A **domain.xml** file is provided in the `<KVM vHMC installation filename>.tar.gz` file. Complete the following steps:
   a. Edit the **domain.xml** file and verify that the path to your disks is correct. This file contains the string **DISK_PATH**.
   b. Make sure `virtio` is used in the bus value for your disk device.
   c. You can choose to have a different name for your VM. The default name in the **domain.xml** file is **vHMC**.
   d. For Ubuntu based KVM, change the Emulator value to `/usr/bin/qemu-system-x86_64`.
   e. Verify that the media access control (MAC) address is set in the **domain.xml** file. This file contains the string **MAC_ADDRESS**.

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

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

Installing the HMC virtual appliance by using the Xen hypervisor

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

The HMC virtual appliance supports Xen version 4.2 or later.

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

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

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

   Note: In this command, specify the full path of your HMC virtual appliance .tar file.
6. A **vhmc.cfg** file is provided in the `<XEN vHMC installation filename>.tar.gz` file. Open the **vhmc.cfg** file in a text editor and edit the following values:

   a. Change the name of the virtual HMC (optional): Edit the **vhmc.cfg** file and verify that the path to your disks is correct. This file contains the string **DISK_PATH**.

   b. Replace **DISK_PATH** with the path for `disk1.img`:

   ```
   disk = [ 'file:DISKPATH,hda,w' ]
   ```

   c. Replace **ethernet adapter** and add MAC address (optional):

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

   Optional MAC Address:

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

   Note: When the Virtual HMC is rebooted, the Xen hypervisor automatically regenerates a MAC address. Adding the optional MAC Address solves this issue.

   d. Replace **FLOPPYPATH** (if you are using the Activation Engine):

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

Installing the HMC virtual appliance by using VMware ESXi

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

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

Note: You can install the HMC virtual appliance on VMware ESXi versions: 6.5, 7.0 or 7.0.2.

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

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

1. Obtain the Tar archive file: `<VMware vHMC installation file name>.tgz`.
2. Use the `tar` command to extract the OVA file from the Tar archive file.
3. Start the vSphere client and log in to the ESXi host.
4. From the **File** menu, select **Deploy OVF template**.
5. Click **Browse** and select the OVA file.
6. Click **Next**.
7. After the deployment is completed, click **Close** and select the HMC virtual appliance icon to power the HMC virtual appliance on.

Installing the HMC virtual appliance enabled with secure boot by using KVM hypervisor on Ubuntu

Learn how to install the Hardware Management Console (HMC) virtual appliance that is enabled with secure boot by using the kernel-based Virtual Machine (KVM) hypervisor on Ubuntu.

About this task

To install the virtual HMC enabled with secure boot by using KVM hypervisor on Ubuntu, complete the following steps:

Note: The following setup uses the command line interface (CLI) and requires root user authority. The command syntax might vary depending on the operating system.

Initial setup

Procedure

1. Verify that virtualization packages are installed on systems with Ubuntu 20.04.
2. Create a folder to store virtual HMC components.
3. Download the <KVM vHMC installation filename> .tar.gz file to the host system.
4. To create a vHMC directory, run the following command:
   ```
   mkdir -p /var/lib/libvirt/images/vHMC
   ```
5. To navigate to the vHMC directory, run the following command:
   ```
   cd /var/lib/libvirt/images/vHMC
   ```
6. To extract virtual disk images, run the following command. Specify the full path of the .tar file where the HMC virtual appliance is present.
   ```
   tar -zxvf <KVM vHMC installation filename>.tgz
   ```

   The following files and folders are displayed:

   - `data`
   - `Readme.html`
   - `user_data`
   - `disk1.img`
   - `checksum`
   - `domain.xml`
   - `vHMC_VARS.fd`
   - `db.der`
   - `pk.der`

Configuring `domain.xml` file

A `domain.xml` file is provided in the `<KVM vHMC installation file name>_efi.tar.gz` file. Open the file with a text editor and edit the following values:

Procedure

1. Replace the name of the bundled nvram file, according to the name of the virtual machine (optional), to **mv vHMC_VARS.fd {VM_NAME}_VARS.fd**.
2. Copy the `vHMC_VARS.fd` file to the **/var/lib/libvirt/qemu/nvram/** location by running the following command:

   ```
   cp {VM_NAME}_VARS.fd /var/lib/libvirt/qemu/nvram/{VM_NAME}_VARS.fd
   ```
3. Optional: Change the name of the virtual HMC.

   Note: This step is mandatory if the VM name is same as the nvram file name.
4. Change **OVMF_CODE_PATH** to `/usr/share/OVMF/OVMF_CODE_4M.fd`.
5. Change **NVRAM_VARS_TEMPLATE_PATH** to `/usr/share/OVMF/OVMF_VARS.fd`.
6. Change **NVRAM_PATH** to `/var/lib/libvirt/qemu/nvram/{VM_NAME}_VARS.fd`.
7. Change the emulator value to `/usr/bin/qemu-system-x86_64`.
8. Replace **DISK_PATH** with the path for `disk1.mg`.
9. Replace **MAC_ADDRESS** with a media access control (MAC) address of the Ethernet adapter.

   Note: Remove the *<mac address='MAC_ADDRESS'/>* tag if you want a MAC address to be generated automatically.
10. If you are using the Activation Engine (AE), replace **AEDISK** with the name of the Activation Engine virtual disk image. Otherwise, remove the disk element.

Deploying virtual HMC

Procedure

1. To define the virtual HMC by using the edited `domain.xml` file, run the following command:

   ```
   virsh define <domain>.xml
   ```
2. To verify that the vHMC was added to the list of defined VMs, run the following command:

   ```
   virsh list --all
   ```
3. To start the defined vHMC, run the following command:

   ```
   virsh start <name>
   ```

   Note: Use the <name>NAME<name> tag format.

Enabling secure boot on HMC by using KVM hypervisor on Ubuntu

After the vHMC is powered on, press the Escape (Esc) key and complete the following steps:

Procedure

1. Navigate to the secure boot menu, **Boot Menu** > **Device Manager** > **Secure Boot Configuration**.
2. Check whether the **Current Secure Boot State** option is enabled.

   Note: If the **Current Secure Boot State** option is disabled, then register both PK and DB keys. Otherwise, register only the DB key.
3. To register the PK key, select **PK Options**, enroll the PK key, which is bundled with an image under the EFI partition (**EFI** > **base** > **pk.der**) and click **Commit Changes and Exit**.

   This action enables the secure boot.

4. To register the DB key, select **DB Options**, enroll the DB key, which is bundled with an image under the EFI partition (**EFI** > **base** > **db.der**) and click **Commit Changes and Exit**.

   This action enables kernel signature verification.
5. Press Esc to navigate to the secure boot configuration menu.
6. To save your changes, press F10+Y.
7. Press Esc to return to the secure boot menu.
8. Select **Reset** to apply all changes.

   After this action, the VM reboots and launches the virtual HMC by enabling secure boot.

   Note: The status of the secure boot capability on the HMC can be verified through CLI (`lshmc --boot`) and the graphical user interface (GUI) page.

Installing the HMC virtual appliance enabled with secure boot by using KVM hypervisor on RHEL

Learn how to install the Hardware Management Console (HMC) virtual appliance that is enabled with secure boot by using the Kernel-based Virtual Machine (KVM) hypervisor on Red Hat Enterprise Linux® (RHEL) platform.

About this task

To install the virtual HMC enabled with secure boot by using KVM hypervisor on RHEL, complete the following steps:

Note: The following setup uses the command-line interface (CLI) and requires root user authority. The command syntax might vary depending on the operating system.

Procedure

1. Verify that the virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) version 8.0 or 9.0.
2. Create a folder to store virtual HMC components.
3. Download the <KVM vHMC installation filename> .tar.gz file to the host system.
4. To create a vHMC directory, run the following command:

   ```
   mkdir -p /var/lib/libvirt/images/vHMC
   ```
5. To navigate to the vHMC directory, run the following command:

   ```
   cd /var/lib/libvirt/images/vHMC
   ```
6. To extract virtual disk images, run the following command. Specify the full path of the .tar file where the HMC virtual appliance is present.

   ```
   tar -zxvf <KVM vHMC installation filename>.tgz
   ```

   The following files and folders are displayed:

   - `data`
   - `Readme.html`
   - `user_data`
   - `disk1.img`
   - `checksum`
   - `domain.xml`
   - `vHMC_VARS.fd`
   - `db.der`
   - `pk.der`

Configuring `domain.xml` file

A `domain.xml` file is present in the `<KVM vHMC installation filename>_efi.tar.gz` file. To configure the domain.xml file, open the file in a text editor and edit the following values:

Procedure

1. Optional: Change the name of the virtual HMC.
2. Change **OVMF_CODE_PATH** to `/usr/share/OVMF/OVMF_CODE.secboot.fd`.
3. Change **NVRAM_VARS_TEMPLATE_PATH** to `/usr/share/OVMF/OVMF_VARS.secboot.fd`.
4. Change **NVRAM_PATH** to `/var/lib/libvirt/qemu/nvram/{VM_NAME}_VARS.fd`.
5. Replace **DISK_PATH** with the path for `disk1.mg`.
6. Replace **MAC_ADDRESS** with a media access control (MAC) address of the Ethernet adapter.

   Note: Remove the *<mac address='MAC_ADDRESS'/>* tag if you want a MAC address to be generated automatically.
7. If you are using the Activation Engine (AE), replace **AEDISK** with the name of the Activation Engine virtual disk image. Otherwise, remove the disk element.

Deploying virtual HMC

Procedure

1. To define the virtual HMC by using the edited `domain.xml` file, run the following command:
   ```
   virsh define <domain>.xml
   ```
2. To verify that the vHMC was added to the list of defined VMs, run the following command:
   ```
   virsh list --all
   ```
3. To start the defined vHMC, run the following command:
   ```
   virsh start <name>
   ```
   Note: Use the *<name>NAME<name>* format.

Enabling secure boot on HMC by using KVM hypervisor on RHEL

After the vHMC is powered on, press the Escape (Esc) key and complete the following steps:

Procedure

1. Navigate to the secure boot menu, **Boot Menu** > **Device Manager** > **Secure Boot Configuration**.
2. Check whether the **Current Secure Boot State** option is enabled.

   Note: If the **Current Secure Boot State** option is disabled, register both PK and DB keys. Otherwise, register only the DB key.
3. To register the PK key, select **PK Options**, enroll the PK key, which is bundled with an image under the EFI partition (click **EFI** > **base** > **pk.der**) and click **Commit Changes and Exit**.

   This action enables the secure boot.
4. To register the DB key, select **DB Options**, enroll the DB key, which is bundled with an image under the EFI partition (**EFI** > **base** > **db.der**) and click **Commit Changes and Exit**.

   This action enables kernel signature verification.
5. Press **Esc** to navigate to the secure boot configuration menu.
6. To save your changes, press F10+Y.
7. Press **Esc** to return to the secure boot menu.
8. a) To boot the signed binaries, add a boot option. Click **Boot Menu** > **Add Boot Option** > **Boot Menu EFI** > **base** > **BOOTX64.EFI** > **Input description (basehmc)** > **Commit Changes and Exit**.

   b) For the boot loader to recognize the proper boot entry, change the boot order. Click **Change Boot Order** > **(Bring basehmc to first boot option)** > **Commit Changes and Exit**.

9. Select **Reset** to apply all changes.

   After this action, the virtual machine reboots and launches the virtual HMC by enabling secure boot.

   Note: The status of the secure boot capability on the HMC can be verified through CLI (`lshmc --boot`) and the graphical user interface (GUI).

Installing the HMC virtual appliance enabled with secure boot by using VMware ESXi

Learn how to install the Hardware Management Console (HMC) virtual appliance that is enabled with secure boot by using VMware ESXi.

About this task

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

Note:

- You can install the HMC virtual appliance on VMware ESXi version 7.0 or 7.0.2.
- The command syntax might vary depending on the operating system.

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

Initial setup

Procedure

1. Obtain the Tar archive file, `<VMware vHMC installation file name>_UEFI.ESX7_0.tgz`.
2. To extract virtual disk images, run the following command:

   ```
   tar -zxvf <KVM vHMC installation filename>.tgz
   ```

   The following files and folders are displayed:

   - `data`
   - `Readme.html`
   - `user_data`
   - `disk1.img`
   - `vHMC_nvram`
   - `vHMC_vmx`
   - `vHMC_ova`
   - `db.der`
   - `pk.der`
3. Start the VMware ESXi web client and log in to the ESXi host.

Deploying virtual HMC

Procedure

1. Click **File** and select **Deploy a virtual machine from an OVF or OVA file** as the creation type. Then, click **Next**.
2. Select the `vHMC.ova` file.
3. Enter a name for the virtual machine and click **Next**.

Note: The names of virtual machine can contain up to 80 characters and must be unique within each ESXi instance.

4. In the **Standard** tab, select a datastore for configuration files and virtual disks of the virtual machine.
5. Click **Next**.
6. Select **VM Network** from the network mapping list.
7. Choose **Thin** or **Thick** as the disk provisioning type.
8. Disable the **Power on automatically** checkbox and click **Next**.
9. Review and verify your deployment settings and click **Finish**.
10. Select the deployed virtual machine from the displayed list.
11. Click **Edit** from the menu to edit the following settings:

    - **CPU settings**
    - **Memory settings**
    - **Configure network adapters**
    - **Configure floppy/ CD interfaces**
    - **I/O settings**

    Note: Click **VM Options** > **Boot Options** tab > and select **EFI** as the firmware to be used to boot the virtual machine in secure mode.

Enabling secure boot on HMC by using VMware ESXi

Procedure

1. Navigate to the datastore location of the virtual machine (`/vmfs/volumes/datastore1/{VM_NAME}/`) and upload `db.der` and `vHMC.nvram` files.

   Note: Change the name of the .nvram file according to the name of the virtual machine by using the **Move** operation.
2. Check and add the following entries at the end of the `vmx` (`/vmfs/volumes/datastore1/{VM_NAME}/{VM_NAME}.vmx`) file of the virtual machine through the command line interface (CLI):

   - `uefi.secureBoot.enabled = "TRUE"`
   - `uefi.allowAuthBypass = "TRUE"`
   - `uefi.secureBoot.dbDefault.file0 = "db.der"`
3. Refresh the settings and boot the virtual machine (VM).

   After this action, the VM reboots and launches the virtual HMC by enabling secure boot.

   Note: The status of the secure boot capability on the HMC can be verified through CLI (`lshmc --boot`) and the graphical user interface (GUI).

Installing the HMC virtual appliance on POWER

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

Installing the HMC virtual appliance on PowerVM (logical partition)

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

The HMC virtual appliance supports POWER9 servers on firmware level FW910 or later. For more information, see Supported Linux distributions for POWER8 and POWER9 Linux on Power® systems (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm).

Notes:

1. You cannot manage the server that hosts the HMC virtual appliance.
2. You cannot manage the server that hosts another HMC virtual appliance which is managing the server that hosts this HMC virtual appliance.

   For example, HMC virtual appliance A is running on server A and HMC virtual appliance B is running on server B. HMC virtual appliance A cannot manage server B and HMC virtual appliance B cannot manage server A at the same time. One of the HMC virtual appliance can manage the other server, but both HMC virtual appliance cannot manage each other at the same time.
3. For HMC virtual appliances that are created on PowerVM, enable **`LargeSend`** on the `NetworkBridge` of the corresponding virtual network for better network bandwidth to the HMC virtual appliance.

.

Create automated HMC installation image (optional)

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

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

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

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

Note: For more information about setting up the Activation Engine and the configuration file, see "Using the Activation Engine for the HMC virtual appliance" on page 13.

Logical volume setup

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

1. Select a managed system.
2. From the menu pod, select **System Actions** > **Power VM** > **Virtual Storage**.
3. Select **Manage System VIOS** > **Action** > **Manage Virtual Storage**.
4. Select the **Virtual Disks** tab.
5. Click **Create virtual disk** and enter the following information:
   - **Virtual disk name**: The name of the virtual disk.

- **Storage pool name**: The name of the storage pool.
- **Virtual disk size**: The size of the virtual disk.
- **Assigned partition**: The name of the logical partition.

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

Installation media setup - create media library

To create a media library, complete the following steps:

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

Installation media setup - upload media to VIOS

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

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

Installation media setup - link media to media library

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

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

Logical partition setup

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

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

   Note: A minimum of four virtual processors and 8 GB of memory is required.
6. From the menu pod, select **Partition Actions** > **Virtual I/O** > **Virtual Networks**.
7. Click **Attach Virtual Network** and select the **Show and attach new virtual ethernet adapters** check box. From the table, select the virtual network adapters that you want to attach to the logical partition.

   Note: A maximum of four virtual network adapters is allowed.
8. From the menu pod, select **Partition Actions** > **Virtual I/O** > **Virtual Storage**.
9. From the **Virtual Optical Device** tab, click **Add Virtual Optical Device**.
10. Enter the **Device Name** (for example, `HMCInstall` or `AEDrive`) and select the wanted Virtual I/O Server from the table.

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

Starting the HMC virtual appliance

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

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

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

15. Follow the onscreen instructions from the **HMC Install** wizard.

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

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

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

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

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

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

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

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

19. Restart the system.

Using the Activation Engine for the HMC virtual appliance

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

Activation Engine is a framework that allows various components within a virtual machine to be configured during system startup. To use the Activation Engine, you need to set up an XML configuration profile to allow the HMC virtual appliance to be in a ready-to-manage state on first start. For more information about configuring the XML configuration profile, see "Setting up the configuration profile for the Activation Engine" on page 14. The configuration file can be used to configure the following options:

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

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

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

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

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

1. Create a directory:

   ```
   mkdir -p config-drive/openstack/latest
   ```

2. Copy the edited **user_data** file into the directory:

   ```
   cp user_data config-drive/openstack/latest
   ```

3. Create a virtual disk image with the Activation Engine configuration:

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

Setting up the configuration profile for the Activation Engine

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

Configuration file

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

```
<vHMC-Configuration>
   <ConfigurationVersion>2.0</ConfigurationVersion>
   <LicenseAgreement></LicenseAgreement>
   <AcceptLicense>Yes</AcceptLicense>
   <Locale>en_US.UTF-8</Locale>
   <SetupWizard>No</SetupWizard>
   <SetupCallHomeWizard>No</SetupCallHomeWizard>
   <SetupKeyboard>No</SetupKeyboard>
   <SetupDisplay>No</SetupDisplay>
   <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
      <Hostname></Hostname>
      <Domain></Domain>
      <DNSServers></DNSServers>
      <IPV4Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Netmask></Netmask>
         <Gateway></Gateway>
      </IPV4Config>
      <IPV6Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Gateway></Gateway>
      <IPV6Config>
      <Firewall>
         <PEGASUS>Enabled</PEGASUS>
         <RPD>Enabled</RPD>
         <FCS>Enabled</FCS>
         <I5250>Enabled</I5250>
         <PING>Enabled</PING>
         <L2TP>Disabled</L2TP>
         <SLP>Enabled</SLP>
         <RSCT>Enabled</RSCT>
         <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
```

```
          <SSH>Enabled</SSH>
          <NTP>Disabled</NTP>
          <SNMPTraps>Disabled</SNMPTraps>
          <SNMPAgents>Disabled</SNMPAgents>
       </Firewall>
    </Ethernet>
    <NTPServers>
       <ntpparam ntpserver="" ntpversion=""/>
    </NTPServers>
</vHMC-Configuration>
```

XML tags for the configuration file

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

Table 1. XML tags

Tags	Description	Acceptable values	Notes
ConfigurationVersion	Required element that defines the configuration version to use.	**2.0**	
LicenseAgreement	Required element that displays the HMC virtual appliance license agreement.		
AcceptLicense	Required element to accept the HMC virtual appliance license agreement.	• **Yes**: Accepts the HMC license agreement. • **No**: Prompts User to Accept HMC License Agreement	If an invalid value is entered, the Activation Engine uses the default setting of **No**.
Locale	Required element to define locale settings.	**en_US.UTF-8**	If an invalid value is entered, the Activation Engine uses the default setting of **US**.
SetupWizard	Required element to enable or disable the **HMC Setup** wizard.	• **Yes**: Displays the **HMC Setup** wizard. • **No**: Disables the **HMC Setup** wizard display.	If an invalid value is entered, the Activation Engine uses the default setting of **Yes**.
SetupCallHomeWizard	Required element to enable or disable the **HMC Call Home** wizard.	• **Yes**: Displays the **HMC Call Home** wizard. • **No**: Disables the **HMC Call Home** wizard display.	If an invalid value is entered, the Activation Engine uses the default setting of **Yes**.
SetupKeyboard	Required element to define the keyboard configuration.	• **Yes**: Prompts the user for keyboard configuration. • **No**: Accepts default keyboard configuration (US).	If an invalid value is entered, the Activation Engine uses the default setting of **Yes**.
SetupDisplay	Required element to enable or disable the display configuration.	• **Yes**: Prompts the user for display configuration. • **No**: Accepts default display configuration.	If an invalid value is entered, the Activation Engine uses the default setting of **Yes**.

Table 1. XML tags (continued)

Tags	Description	Acceptable values	Notes
Ethernet	Required element that holds values for Ethernet adapter configurations. A maximum of four Ethernet adapters can be configured.	**Enable**: - **Yes**: Configure this adapter. - **No**: Do not configure this adapter. **DefaultGatewayDevice**: - **Yes**: Configure this adapter as the main network adapter. - **No**: Do not configure this adapter as the main network adapter. **PrivateInterface**: - **Yes**: Configure this adapter as a private interface. **Yes** is required to configure interface as an IPv4 DHCP Server. - **No**: Do not configure this adapter as a private interface. **No** is required to configure interface as IPv4 static type.	The Activation Engine runs the default configuration if any invalid values are entered within the Ethernet adapter section or if multiple **Default Gateway Devices** are defined. Optional elements can be omitted from the configuration. At least one IPV4 or IPV6 configuration is required. If you do not specify an IP configuration, the Activation Engine uses the default configuration.
HostName	Optional element to define the network host name.	Any valid host name string.	If the element is not defined, the Activation Engine uses the default local host **HostName** value.
Domain	Optional element to define the network domain.	Any valid domain value (for example, **example.us.com**).	If the element is not defined, the Activation Engine uses the default empty **Domain** value.
DNSServers	Optional element to define the network DNS servers.	It is acceptable to have one DNS Server value or up to three valid IPv4 or IPv6 addresses that are separated by a comma. - Example 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 - Example 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 - Example 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201	If the element is not defined, the Activation Engine uses the default empty **DNSServers** value.

Table 1. XML tags (continued)

Tags	Description	Acceptable values	Notes
IP4Config	Optional element to define IPv4 configuration settings.	**IPType**: Required element to define IPv4 configuration type. • **Static**: Configure this adapter by using static configuration. • **DHCP**: Configure this adapter by using DHCP configuration. • **DHCPServer**: Configure this adapter to be IPv4 DHCP server (requires **PrivateInterface** to be set to **Yes**). **IPAddress**: Optional element that is required only if **Static** or **DHCPServer** configuration is selected. • **Static Configuration**: Any valid IPv4 address value. • **DHCPServer Configuration**: Any DHCP server IP within the IP range. **Netmask**: Optional element that is required only if **Static** configuration is selected. • Any valid IPv4 netmask value. **Gateway**: Optional element that is required only if **Static** configuration is selected. • Any valid IPv4 netmask value.	
IP6Config	Optional element to define IPv6 configuration settings.	**IPType**: Required element to define IPv6 configuration type. • **Static**: Configure this adapter by using static configuration. • **DHCP**: Configure this adapter by using DHCP configuration. **IPAddress**: It is acceptable to have long or short form IPv6 format and long or short form IPv6 prefix. • Example 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • Example 2: IPv6: 2001:4860:4860::8888 • Example 3: IPv6: 2001:4860:4860::8888/128 If no prefix is specified, the Activation Engine uses the default setting of /64 prefix. **Gateway**: • Any valid IPv6 address value.	

Table 1. XML tags (continued)

Tags	Description	Acceptable values	Notes
Firewall	Optional element to define firewall settings.	**PEGASUS**: • **Enabled**: Allows the PEGASUS ports to be open. • **Disabled**: Disables PEGASUS ports. **RPD**: • **Enabled**: Allows the RMC ports to be open. • **Disabled**: Disables RMC ports. **FCS**: • **Enabled**: Allows the FCS ports to be open. • **Disabled**: Disables FCS ports. **I5250**: • **Enabled**: Allows the 5250 ports to be open. • **Disabled**: Disables 5250 ports. **PING**: • **Enabled**: Allows the Ping port to be open. • **Disabled**: Disables Ping port. **L2TP**: • **Enabled**: Allows the L2TP ports to be open. • **Disabled**: Disables L2TP ports. **SLP**: • **Enabled**: Allows the SLP ports to be open. • **Disabled**: Disables SLP ports. **RSCT**: • **Enabled**: Allows the RSCT ports to be open. • **Disabled**: Disables RSCT ports. **SECUREREMOTEACCESS**: • **Enabled**: Allows the secure remote access ports to be open. • **Disabled**: Disables secure remote access ports. **SSH**: • **Enabled**: Allows the SSH port to be open. • **Disabled**: Disables SSH port.	

Table 1. XML tags (continued)

Tags	Description	Acceptable values	Notes
Firewall	Optional element to define firewall settings.	**NTP**: • **Enabled**: Allows the NTP ports to be open. • **Disabled**: Disables NTP ports. **SMNPTraps**: • **Enabled**: Allows the SMNP traps ports to be open. • **Disabled**: Disables SMNP traps ports. **SMNPAgents**: • **Enabled**: Allows the SMNP agents ports to be open. • **Disabled**: Disables SMNP agents ports.	

NTPServers	The **NTPServers** tag is needed if you want to configure up to five NTP servers within a HMC virtual appliance.	**NTPServers**: Accepts `<ntpparam ntpserver="server" ntpversion="version"/>`
		ntpparam:
		• **ntpserver**: Accepts any valid IPv4 or IPv6 values and valid host names.
		• **ntpversion**: Accepts 1-4 numeric value
		Example:
		`<NTPServers>`
		`  <ntpparam ntpserver=`
		`   "test.austin.ibm.com"`
		`   ntpversion="2"/>`
		`  <ntpparam`
		`ntpserver="192.168.34.1"`
		`   ntpversion="4"/>`
		`  <ntpparam`
		`ntpserver="::ffff:903:201"`
		``   ntpversion="3"/>` ``
		`</NTPServers>`	

Configuring the HMC

Learn how to set up your network connections, configure your HMC, complete postconfiguration steps, and upgrade and update your HMC.

Choosing network settings on the HMC

Learn about the network settings that you can use on the Hardware Management Console (HMC).

HMC network connections

Learn how the Hardware Management Console HMC can be used in a network.

You can use different types of network connections to connect your HMC to managed systems. For more information about using the HMC on a network, see the following information:

Types of HMC network connections

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

The HMC supports the following types of logical communications:

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

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

HMC to BMC

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

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

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

- By using the web browser to access all the HMC GUI functions remotely.
- By using Secure Socket Shell (SSH) to access the HMC command line functions remotely.
- By using a virtual terminal server for remote access to virtual logical partition consoles.

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

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

- One network interface can be used exclusively for HMC-to-managed system communications, which means that only the HMC and service processors of the managed systems would be on that network. One or more network interfaces can be used exclusively for HMC-to-managed system communications,

© Copyright IBM Corp. 2021, 2024

which means that only the HMC and service processors of the managed systems are on that network. Even though the network interfaces into the service processors are encrypted for the Secure Sockets Layer (SSL) Protocol and password-protected, having a separate dedicated network can provide a higher level of security for these interfaces.

- An open network interface would typically be used for the network connection between the HMC and the logical partitions on the managed systems, for the HMC-to-logical partition communications. You can also use this open network interface to manage the HMC remotely.
- Optionally, you can use a third interface to connect to logical partitions and manage the HMC remotely. This interface can also be used as a separate HMC connection to different groups of logical partitions. For example, you might want to have an administrative LAN that is separate from the LAN on which all the usual business transactions are running. Remote administrators can access the HMC and other managed units by using this method. Sometimes the logical partitions are in different Network security domains, perhaps behind a firewall, and you might want to have different HMC network connections into each of those two domains.

Web browser requirements for HMC

The Hardware Management Console (HMC) version 9.1.0 is supported by Google Chrome version 57, Microsoft Internet Explorer (IE) version 11.0, Mozilla Firefox versions 45 and 52 Extended Support Release (ESR), and Safari version 10.1.

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

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

Enabling session cookies in Internet Explorer.

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

Enabling session cookies in Firefox.

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

Private and open networks in the HMC environment

The Hardware Management Console (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 Flexible Service Processor (FSP).

On most systems, the FSP provides two Ethernet ports that are labeled **HMC1** and **HMC2**. You to connect up to two HMCs.

Some systems have a dual-FSP option. In this situation, the second FSP acts as a redundant backup. The basic setup requirements for a system with two FSPs are essentially the same as a system without a second FSP. The HMC must be connected to each FSP, so more network hardware is required (for example, a LAN switch or hub) when there is more than one FSP or 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 any hardware errors 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 Hardware Management Console (HMC) as a Dynamic Host Configuration Protocol (DHCP) server.

If you want to configure the first network interface as a private network, you can select from a range of IP addresses for the DHCP server to assign to its clients. The selectable address ranges include segments from the standard nonroutable IP address ranges.

In addition to these standard ranges, a special range of IP addresses is reserved for IP addresses. This special range can be used to avoid conflicts in cases where the HMC attached open networks are using one of the nonroutable address ranges. Based on the range that is selected, the HMC network interface on the private network is automatically assigned the first IP address of that range. The service processors are then assigned addresses from the rest of the range.

The DHCP server in the HMC uses automatic allocation, which means that each unique service processor Ethernet interface is reassigned the same IP address each time it is started. Each Ethernet interface has a unique identifier that is based on a built-in Media Access Control (MAC) address, which allows the DHCP server to reassign the same IP parameters. You can configure both **eth0** and **eth1** HMC ports to serve DHCP addresses.

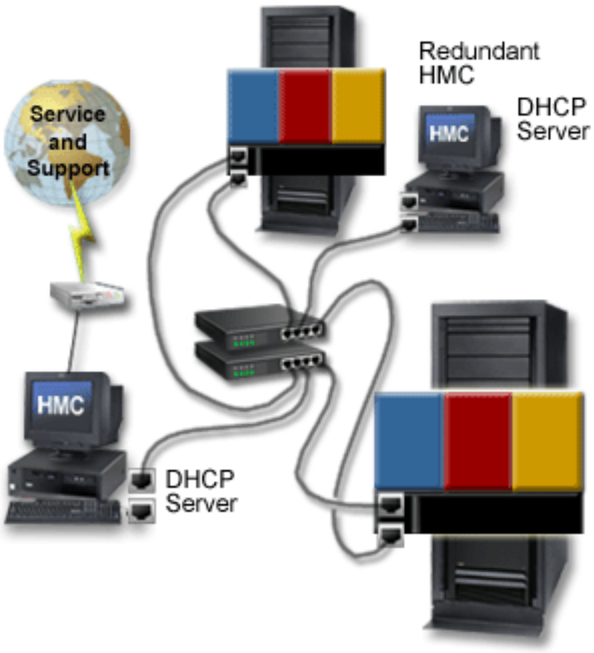
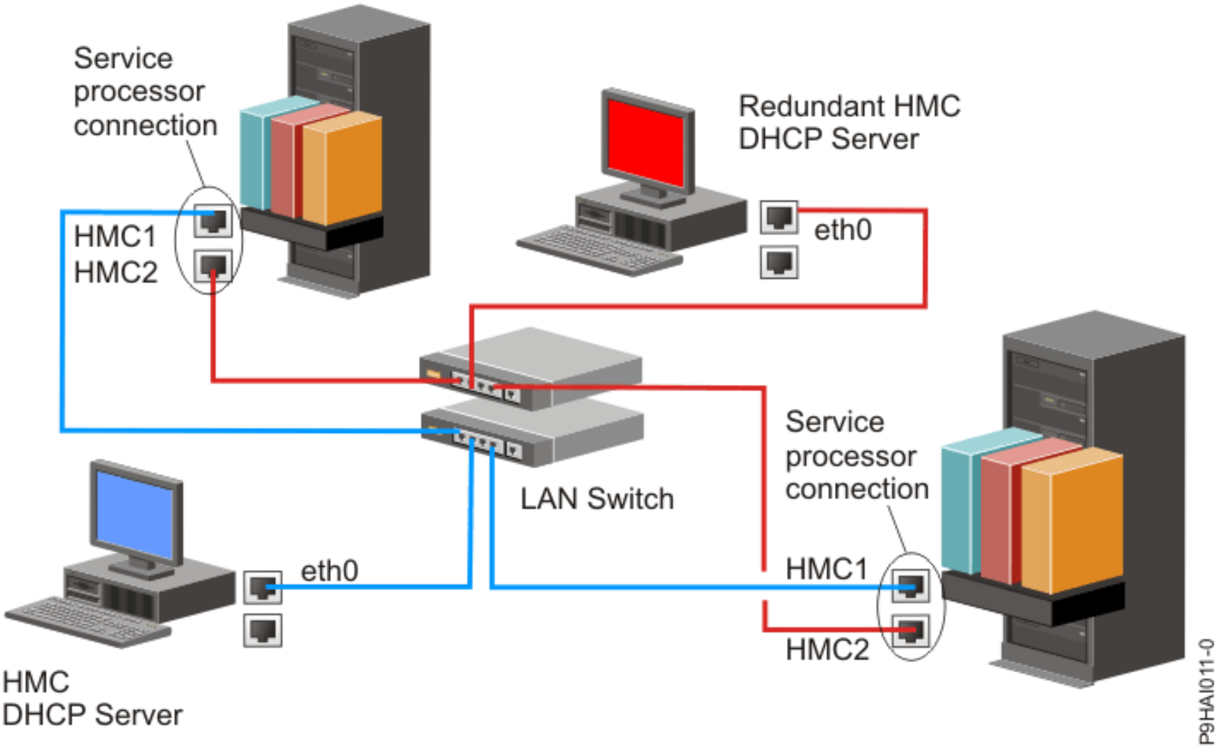


Figure 1. Private network with one HMC as a DHCP server

Note: If you are using IPv6, the discovery process must be done manually. For IPv6, automatic discovery is not available.

For more information about how to configure the HMC as a DHCP server, see "Configuring the HMC as a DHCP server" on page 45.

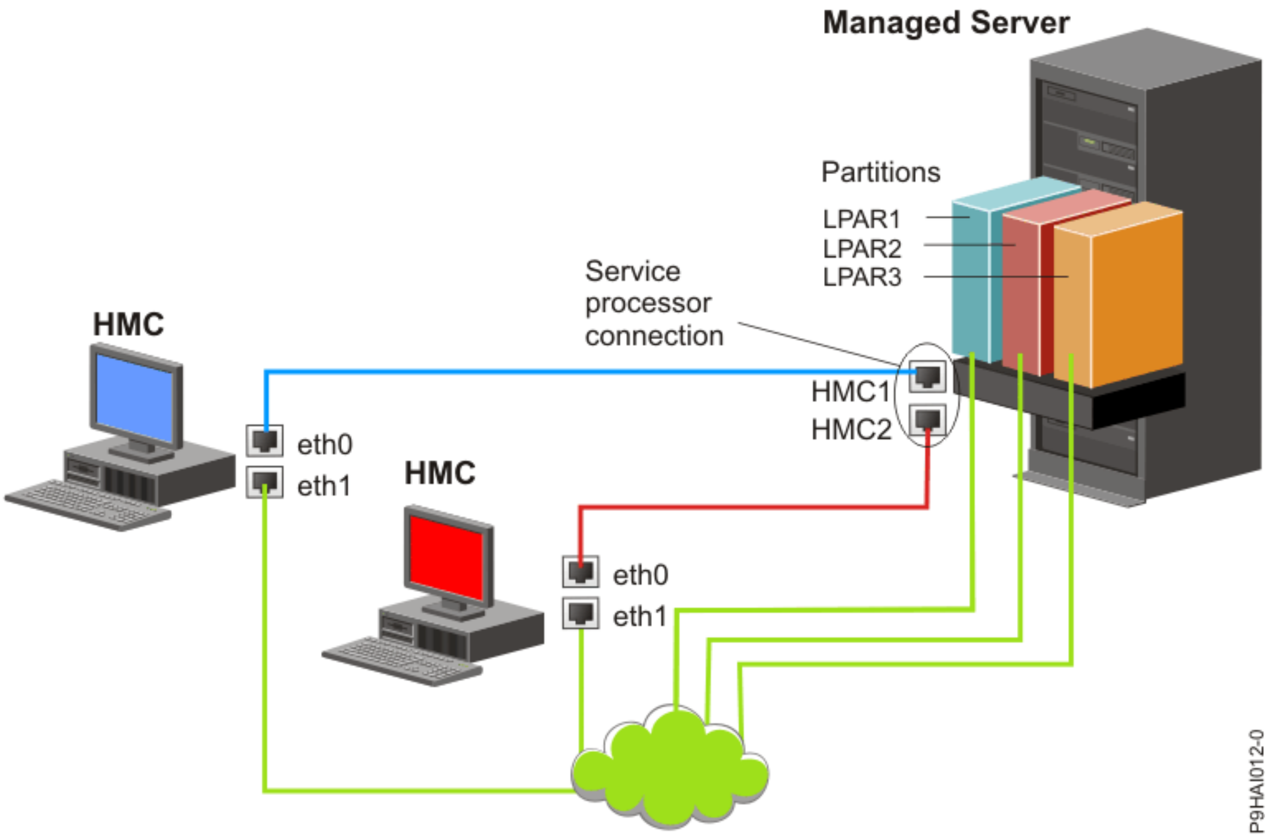

Service processor connection
HMC1
HMC2
Redundant HMC DHCP Server
eth0
LAN Switch
Service processor connection
HMC1
HMC2
eth0
HMC DHCP Server
P9HAI011-0

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, by 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 without 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 extra 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.

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 Hardware Management Console (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 you configure the LAN-based internet connection. The first choice is to use standard Secure Sockets Layer (SSL). The SSL communication can be enabled to connect to the internet through your proxy server. SSL connectivity is more likely to be compliant with corporate security guidelines.

Note: If your open network interface connection uses only Internet Protocol Version 6 (IPv6), you cannot use internet VPN to connect to support. For more information about the protocols that are used, see "Choosing an Internet Protocol" on page 27.

The advantages to using an internet connection can include:

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

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

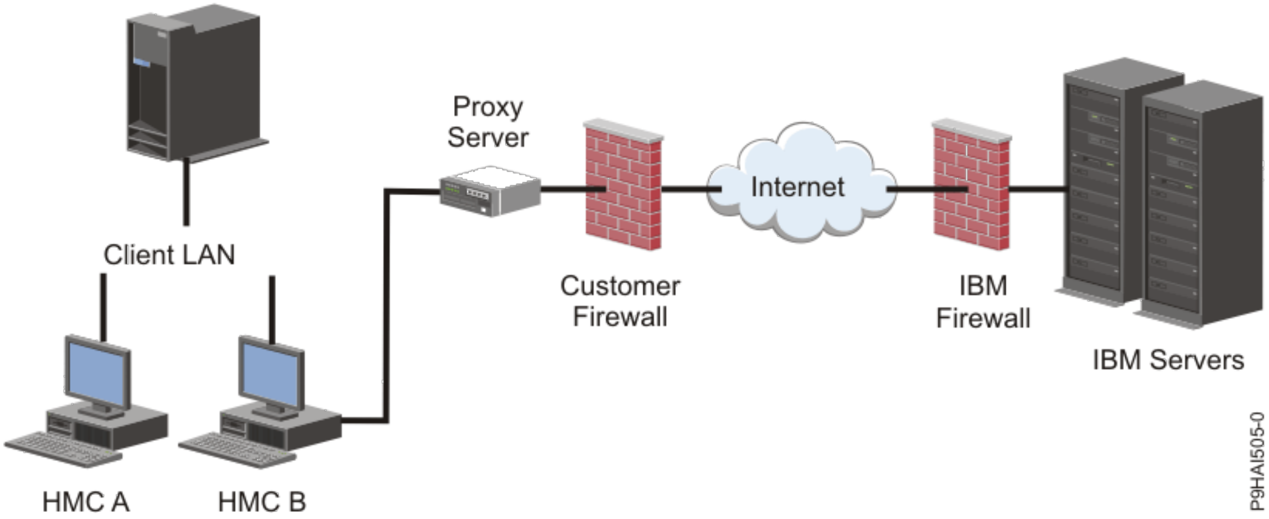
- Remote Support Facility requests are always initiated from the HMC to IBM. An inbound connection is never initiated from the IBM Service Support System.
- All data that is transferred between the HMC and the IBM Service Support System are encrypted by using a high-grade encryption. Depending upon the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

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

Using an indirect internet connection with a proxy server

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

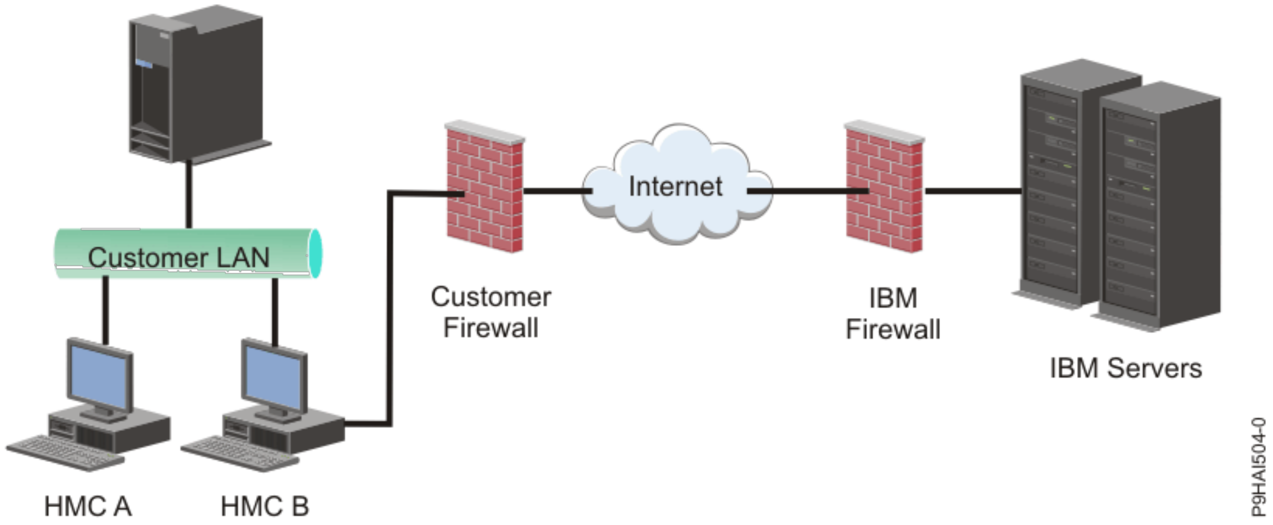
To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616) and the CONNECT method. Optionally, basic proxy authentication (RFC 2617) can be configured so that the HMC authenticates before you attempt to forward sockets through the proxy server.



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 27 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 27, you can use a direct internet connection.



Using internet SSL to connect to remote support

All the communications are handled through TCP sockets that are initiated by the Hardware Management Console (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 27) 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 that is provided by the customer. The decision about which approach is 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 that is used when the Hardware Management Console (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 that represents the 4 bytes of the IPv4 address, which is 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 46 and "Setting the IPv6 address" on page 47.

Internet SSL address lists

Learn about the addresses that the Hardware Management Console (HMC) uses when the HMC is using internet SSL connectivity.

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

The following IPv4 addresses are for all locations:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216

- 129.42.60.216
- 170.225.15.41

The following IPv4 addresses are for the Americas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

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

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

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

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

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

Using multiple call-home servers

Learn about 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 Hardware Management Console (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 by using the other available call-home servers until one is successful or all servers are tried.

The connected HMC that is identified by the problem analysis to be the primary analyzing console for a given managed system that reports the problem. This primary console also replicates 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 extra 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 is manually added to the list of call-home server consoles available for outbound connectivity.

Preparing for HMC configuration

Learn about the 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.

Learn about the information that you need to connect your HMC to the following locations:

- Service processors in your managed systems
- Logical partitions on those managed systems

- Remote workstations
- IBM Service to implement “call-home” functions

To prepare for HMC configuration, complete the following steps:

1. Obtain and install the latest level of the HMC code version you want to install.
2. Determine the physical location of the HMC in relation to the servers it manages. 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 manages.
4. Determine whether you 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 “Selecting a private or open network” on page 44.
5. If you 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 needs be physically closer to the system, and must be the HMC that is configured to call home.
7. Determine the network settings that you need to connect the HMC to remote workstations, logical partitions, and network devices.
8. Define how the HMC calls 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 create and their passwords, as well which roles they are given. You must assign the **hscroot** and **hscpe** users a password.
10. Document the following company contact information that is needed when you configure 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 use.
12. You must define the following passwords:
    - The access password that is used to authenticate the HMC to the FSP.
    - The ASMI password that is used for the **admin** user.
    - The ASMI password that is 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.

When you complete these preparation steps, complete the “Preinstallation configuration worksheet for the HMC” on page 30.

Preinstallation configuration worksheet for the HMC

Use this worksheet to note the installation information that you can use for the HMC installation.

Note: You can download the preinstallation configuration worksheet to your local drive for viewing or printing. To save the file in Microsoft Word format to your local drive, click HMC_preinstallation_configuration_worksheet.docx.

Improved password policy for HMC

You must set a new password on the first use for newly manufactured systems with HMC version 9.940.0, or later, and after a factory reset of the system. This policy change helps to enforce that the HMC is not left in a state with a well-known password.

With HMC Version 9.940.0, and later, the `hscroot` password is expired and must be changed before you can access the functions of the HMC. For more information about how to change the password, see https://www.ibm.com/support/knowledgecenter/POWER10/p10eh6/p10eh6_useridsandpassword.htm. However, if you are upgrading from a previous HMC level or an operational installation, you do not need to change the password.

Network Settings

LAN Interface: Choose the available adapters (such as eth0, eth1) that is used by the HMC to connect to managed systems, logical partitions, service and support, and remote users. For more information, see "HMC network connections" on page 21. Connectivity from the HMC can either be on a private or open network.

Ethernet Adapter Speed and Duplex

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

Table 2. Ethernet Adapter Speed and Duplex

Characteristic	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 22.

Table 3. Private or Open network

Characteristic	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 enable the HMC as a DHCP server, the managed systems on the network are automatically configured and discovered by the HMC.

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

Table 4. DHCP server

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

If you are using the 7063-CR1 HMC, you must connect the Ethernet **IPMI** port to a network to access the baseboard management controller (BMC) on the HMC. For more information, see "Configure BMC connectivity (7063-CR1)" on page 45. Complete the following table for your BMC connection.

Table 5. BMC connection

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

For Ethernet adapters specified as *open* networks, complete the following tables. For more information about the different Internet Protocol versions, see "Configuring the HMC network types" on page 39.

Using IPv6

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

Table 6. IPv6 (static)

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

Table 7. IPv6 (DHCP server)

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

Table 8. IPv6 (IPv6 router)

Characteristic	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 47. For more information about using only IPv6 addresses, see “Using only IPv6 addresses” on page 47.

Using IPv4

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

Table 9. IPv4

Characteristics	**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 must be allowed through the firewall:				

TCP/IP information

A unique TCP/IP address is required for each node, both for Support Element (SE) and Hardware Management Console (HMC). The assigned network mask is used to generate a unique address, by default, for the local private LAN. If the nodes are connected into a larger network with an administered TCP/IP address, you can specify the TCP/IP address that you want to use. 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, so that you can control over which HMC network applications can be accessed on each network.

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

Table 10. Open network adapter

Local host information	
HMC host name:	
Domain name:	
Description of HMC:	
Gateway information	

Table 10. Open network adapter (continued)

Local host 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, complete the TCP/IP address that will 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 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 want to be notified by email when hardware problem events occur on your system.

Table 11. Email notification

Characteristics	**Entry field**
Email Addresses:	
SMTP server:	
Port:	
Errors to be notified:	
Only call-home problem events	

Table 11. Email notification (continued)

Characteristics	Entry field
All problem events	

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

SMTP is the protocol that is used to send email. When you use SMTP, a client sends a message and communicates with the SMTP server by 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 about 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 receive notification only when events occur that create a call-home function.
- Select **All problem events** to receive notification when any events occur.

Service contact information

Table 12. Service contact information

Characteristics	Entry field
Company name	
Administrator name	
Email address	
Phone number	
Alternative phone number	
Fax number	
Alternative phone 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 or locality	
State	

Table 12. Service contact information (continued)

Characteristics	Entry field
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 that include security characteristics and configuration requirements, see "Choosing existing call-home servers to connect to service and support for this HMC" on page 56.

Table 13. Service authorization and connectivity

Characteristics	Entry field
Secure Sockets Layer (SSL) through the internet	_____
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) by using the existing internet connection. Select **Use SSL Proxy** if you want to configure the use of encrypted SSL by using an indirect connection that uses an SSL Proxy.

Table 14. SSL

Characteristics	Entry field
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 "Configuring the HMC network types" on page 39.

___ IPv4

___ IPv6

___ IPv4 and IPv6

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) by using the existing internet connection.

Note: If you select Virtual Private Network (VPN) through the internet, you cannot 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 28.

___ This HMC

___ Another HMC

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

Table 15. Other HMCs that are configured as call-home servers

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

Extra Support Benefits

My Systems and Premium Search

Table 16. My Systems and Premium Search

Characteristics	**Entry field**
List your IBM ID	__________________________
List any additional IBM IDs	__________________________

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 that is collected by the IBM Electronic Service Agent application. To use these functions, you must first register on the IBM Registration website at http://www.ibm.com/account/profile.

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

Configuring the HMC

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

Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to ease the setup of the HMC. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the available settings that the wizard guides you through. You can also perform the configuration steps without the aid of the wizard by Configuring the HMC by using the HMC menus.

Before you start, gather the required configuration information that you need to complete the steps successfully. See "Preparing for HMC configuration" on page 28 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 30 and then return to this section.

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

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

Configuring the HMC by using the 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 document. You can access the information centerIBM Power systems hardware information on the HMC or on the Web. On the HMC, IBM Knowledge Center can be accessed from the upper-right corner of the task bar. On the web, IBM Knowledge Center can be accessed at https://www.ibm.com/support/knowledgecenter.

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 28.

Table 17. 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 38
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 39
6. For HMC model 7063-CR1, you must configure the baseboard management controller (BMC) IP address.	"Configure BMC connectivity (7063-CR1)" on page 45
7. If you are using an open network and a fixed IP address, set identification information.	
8. If you are using an open network and a fixed IP address, configure a routing entry as the default gateway.	"Configuring a routing entry as the default gateway" on page 50
9. If you are using an open network and a fixed IP address, configure domain name services.	"Configuring domain name services" on page 50
10. If you are using a fixed IP address and have DNS enabled, configure domain suffixes.	"Configuring domain suffixes" on page 51
11. Configure your server to connect to IBM service and support and return to this checklist when you have completed this step.	"Configuring the local console to report errors to service and support" on page 54
12. Configure the Events Manager for Call Home.	"Configuring the Events Manager for Call Home" on page 58

Table 17. Manual HMC configuration tasks and where to find related information (continued)

Task	Where to find related information
13. Connect the managed system to a power source.	
14. Set passwords for the managed system, and each of the ASMI passwords (general and admin)	"Setting passwords for the managed system" on page 59
15. Access ASMI to set the date and time on the managed system.	
16. Start the managed system and return to this checklist when you have completed this step.	
17. Ensure that you have one logical partition on the managed system.	
18. Optional: add another managed system and return to this checklist when you have completed this step.	
19. Optional: If you are installing a new server with your HMC, configure the logical partitions and install the operating system.	
20. If you are not installing a new server at this time, perform optional postconfiguration tasks to further customize your configuration.	"Postconfiguration steps" on page 61

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.

About this task

To start the HMC, do the following procedure:

Procedure

1. Turn on the HMC by pressing the power button.
2. If English is your language preference, continue with step 4.

   If your language preference is a language other than English, type the number **2** when you are prompted to change the locale.

   Note: This prompt times out in 30 seconds if you do not act.
3. Select the locale that you want to display from the list in the **Locale Selection** window, and click **OK**. The locale identifies the language that the HMC interface uses.
4. Click **Log on and launch the Hardware Management Console web application**.
5. Log in to the HMC with the following default user ID and password:

   ID: `hscroot`
   Password: `abc123`

   HMC Enhanced
   Displays the newer enhanced GUI with the enhanced PowerVM features.

   HMC Classic
   Displays the standard GUI without the enhanced PowerVM features.

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

6. Press Enter.

Changing the date and time

The battery-operated clock keeps the date and time for the Hardware Management Console (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.

About this task

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

If you are using HMC Version 10.1.1020, or earlier, to change the date and time for the HMC, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to change the date and time for the HMC, complete the following steps:

1. Ensure that you are a member of one of the following roles:
   - Super administrator
   - Service representative
   - Operator
   - Viewer
2. In the navigation area, click **HMC management**, and then select **HMC settings**.
3. In the content pane, change the date and time settings under the **Date and time** section.
4. If you select **UTC** in the **Clock** field, the time setting adjusts 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.

Before you begin

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

Table 18. 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 30
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port that is defined as eth0" on page 42
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 44
b. Select the open network type.	"Selecting a private or open network" on page 44
c. Set static addresses.	"Setting the IPv6 address" on page 47
d. Set the firewall.	"Changing HMC firewall settings" on page 48
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 50
f. Configure DNS.	"Configuring domain name services" on page 50
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 60

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.

Before you begin

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

Table 19. 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 30
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port that is defined as eth0" on page 42
3. Configure the HMC as a DHCP server.	"Configuring the HMC as a DHCP server" on page 45
4. Test the connection between the managed server and the HMC.	"Testing the connection between the HMC and the managed system" on page 60

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

Before you begin

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

Table 20. 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 30
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port that is defined as eth0" on page 42
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 44
b. Select the open network type.	"Selecting a private or open network" on page 44
c. Set static addresses.	"Setting the IPv6 address" on page 47
d. Set the firewall.	"Changing HMC firewall settings" on page 48
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 50
f. Configure DNS.	"Configuring domain name services" on page 50
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 60

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

Before you begin

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

Table 21. 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 30
2. Identify the Ethernet ports for your HMC.	"Identifying the Ethernet port that is defined as eth0" on page 42
3. Configure the Ethernet adapter by performing the following tasks:	
a. Set the media speed.	"Setting the media speed" on page 44
b. Select the open network type.	"Selecting a private or open network" on page 44
c. Set static addresses.	"Setting the IPv6 address" on page 47
d. Set the firewall.	"Changing HMC firewall settings" on page 48
e. Configure the default gateway.	"Configuring a routing entry as the default gateway" on page 50
f. Configure DNS.	"Configuring domain name services" on page 50
g. Configure suffixes.	"Configuring domain suffixes" on page 51
4. Configure additional adapters, if you have them.	

Configuring HMC call-home server settings

Before you begin

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

Table 22. 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 30
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 56
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 that is defined as eth0

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

If you did not install any additional Ethernet adapters in the PCI slots on your HMC, then 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 install extra Ethernet adapters in the PCI slots, then the port that is defined as eth0 depends on the location and type of Ethernet adapters that are installed.

Note: The following general rules might not apply for all configurations.

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

Table 23. 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 extra Ethernet adapter. • If an extra Ethernet adapter is installed, then 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 the port that is labeled Act/Link A is eth0. The port that is labeled Act/link B is 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, then the primary-integrated Ethernet port is defined as eth0.

Table 23. HMC types and associated rules for Ethernet placement (continued)

HMC type	Rules for Ethernet placement
Stand-alone models with a single integrated Ethernet port.	The definitions depend upon the type of Ethernet adapter that is installed: • If only one Ethernet adapter is installed, then that adapter is defined as `eth0`. • If the Ethernet adapter is a dual port Ethernet adapter, then the port that is labeled `Act/link A` is `eth0`. The port that is 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, then the integrated Ethernet port is defined as `eth0`. • If multiple Ethernet adapters are installed, see "Determining the interface name for an Ethernet adapter" on page 43.

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 that the HMC identifies as `eth0` and `eth1`.

About this task

If you are using HMC Version 10.1.1020, or earlier, to determine the name the HMC has assigned to an Ethernet adapter, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Settings**.
2. In the content pane, click **Change Network Settings**.
3. From the **Change Network Settings** window, click the **LAN adapters** tab. The following example entry shows that this Ethernet port is identified as `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>)`.
4. Record your results. If you need to view or change the LAN adapter settings, click **Details**.
5. Click **OK**.

If you are using HMC Version 10.2.1030, or later, to determine the name the HMC has assigned to an Ethernet adapter, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the menu pod, click **Network settings**.
3. From the **Change Network Settings** window, click the **LAN adapters** tab. The following example entry shows that this Ethernet port is identified as `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>)`.
4. Record your results. If you need to view or change the LAN adapter settings, click **Details**.
5. Click **OK**.

Setting the media speed

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

Before you begin

The default for the HMC adapter settings is **Autodetection**. If this adapter is connected to a LAN switch, you must match the switch port settings.

About this task

If you are using HMC Version 10.1.1020, or earlier, to set the media speed and duplex, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. In the local area network (LAN) information section, select **Autodetection** or the appropriate media speed and duplex combination.
6. Click **OK**.

If you are using HMC Version 10.2.1030, or later, to set the media speed and duplex, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. In the local area network (LAN) information section, select **Autodetection** or the appropriate media speed and duplex combination.
6. Click **OK**.

Selecting a private or open network

A *private service network* consists of the Hardware Management Console (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.

About this task

If you are using HMC Version 10.1.1020, or earlier, to select a private or public network, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to select a private or public network, complete the following steps:

1. In the navigation area, click **HMC management**.

2. In the content pane, click **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.

If you are using HMC Version 10.1.1020, or earlier, to configure the Hardware Management Console (HMC) as a DHCP server, complete the following steps:

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

   Note: You can configure the HMC to be a DHCP server only on a private network. If you use an open network, the option to select the **Enable DHCP** is not available.
6. Enter the address range of the DHCP server.
7. Click **OK**.

If you are using HMC Version 10.2.1030, or later, to configure the Hardware Management Console (HMC) as a DHCP server, complete the following steps:

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

   Note: You can configure the HMC to be a DHCP server only on a private network. If you use an open network, the option to select the **Enable DHCP** is not available.
6. Enter the address range of the DHCP server.
7. Click **OK**.

If you configured your HMC to be a DHCP server on a private network, you must verify that your HMC DHCP private network is configured correctly. For information about connecting your HMC to a private network, see "Selecting a private or open network" on page 44.

For more information, see " HMC as a DHCP server" on page 23.

Configure BMC connectivity (7063-CR1)

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

Note: This task applies only to the 7063-CR1. This connection is required to access the baseboard management controller (BMC) on the HMC.

If you are using HMC Version 10.1.1020, or earlier, to configure the BMC connection, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Settings**.
2. In the content pane, click **Change BMC/IPMI network settings**.
3. Select the connection mode (**DHCP** or **Static**).

If you select **Static** mode, complete the following addresses:

- **IP address**
- **Subnet mask**
- **Gateway**

4. Click **OK**.

If you are using HMC Version 10.2.1030, or later, to configure the BMC connection, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Change BMC/IPMI network settings**.
3. Select the connection mode (**DHCP** or **Static**).

   If you select **Static** mode, complete the following addresses:

   - **IP address**
   - **Subnet mask**
   - **Gateway**
4. Click **OK**.

You can also configure the BMC network connection by using the Petitboot bootloader interface. For more information, see Configuring the firmware IP address.

Setting the IPv4 address

Learn how to set your IPv4 address on the HMC.

About this task

If you are using HMC Version 10.1.1020, or earlier, to set the IPv4 address, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to set the IPv4 address, complete the following steps:

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

About this task

If you are using HMC Version 10.1.1020, or earlier, to set the IPv6 address, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to set the IPv6 address, complete the following steps:

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

About this task

If you are using using HMC Version 10.1.1020, or earlier, to configure the HMC so that it uses only IPv6 addresses, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to configure the HMC so that it uses only IPv6 addresses, complete the following steps:

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

What to do next

After you click **OK**, you must restart 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.

About this task

If you are using HMC Version 10.1.1020, or earlier, to configure a firewall, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Settings**.
2. In the content pane, click **Change network settings**.
3. Click the **LAN Adapters** tab.
4. Select the LAN adapter that you want to work with and click **Details**.
5. Click the **Firewall** tab.
6. Using one of the following methods, you can allow any IP address by using a particular application through the firewall, or you can specify one or more IP addresses:
   - Allow any IP address by 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 is 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**.

   Notes:

   - For more information about enabling remote restricted shell access, see "Enabling remote restricted shell access" on page 49.
   - For more information about enabling remote web access, see "Enabling remote web access" on page 49.

If you are using HMC Version 10.2.1030, or later, to configure a firewall, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **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 by using a particular application through the firewall, or you can specify one or more IP addresses:
   - Allow any IP address by 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 is 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**.

   Notes:

   - For more information about enabling remote restricted shell access, see "Enabling remote restricted shell access" on page 49.
   - For more information about enabling remote web access, see "Enabling remote web access" on page 49.

Enabling remote restricted shell access

You can enable remote restricted shell access when you configure a firewall.

About this task

If you are using HMC Version 10.1.1020, or earlier, to enable remote restricted shell access, complete the following steps:

1. In the navigation area, click **Users and Security** > **Systems and Console Security**.
2. Click **Enable Remote Command Execution**.
3. Select **Enable remote command execution using the ssh facility** and then click **OK**.

If you are using HMC Version 10.2.1030, or later, to enable remote restricted shell access, complete the following steps:

1. In the navigation area, click **User management** > **HMC settings**.
2. Select **Remote command execution through SSH**.

What to do next

Now remote restricted shell access is enabled.

Enabling remote web access

You can enable remote web access to your Hardware Management Console (HMC).

About this task

To enable remote web access, complete the following steps:

If you are using HMC Version 10.1.1020, or earlier, to enable remote web access, complete the following steps:

1. In the navigation area, click **Users and Security** > **Systems and Console Security**.
2. Click **Enable Remote Command Execution**.
3. Select **Enable** and then click **OK**.

If you are using HMC Version 10.2.1030, or later, to enable remote web access, complete the following steps:

1. In the navigation area, click **User management** > **HMC settings**.
2. Select **Remote web access**.

What to do next

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 when you are using an open network.

About this task

If you are using HMC Version 10.1.1020, or earlier, to configure a routing entry as the default gateway, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to configure a routing entry as the default gateway, complete the following steps:

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

About this task

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.

If you are using HMC Version 10.1.1020, or earlier, to configure domain name services, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to configure domain name services, complete the following steps:

1. In the navigation area, click **HMC management**.

2. In the content pane, click **Network settings**. The **Change Network Settings** window opens.
3. Click the **Name Services** tab.
4. Select **DNS enabled** to enable DNS.
5. Specify the DNS server and domain suffix search order and click **Add**.
6. Click **OK**.

Configuring domain suffixes

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

About this task

The domain suffix is a string that is 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 an attempt is made to resolve `myname.mloc.mycompany.com`.

If you are using HMC Version 10.1.1020, or earlier, to configure a domain suffix entry, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to configure a domain suffix entry, complete the following steps:

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

You can configure your Hardware Management Console (HMC) so that it uses LDAP (Lightweight Directory Access Protocol) remote user management.

Before you begin

When a user logs in to the HMC, the HMC can contact a remote LDAP server for user management with necessary authorization parameters on LDAP server. You must configure your HMC so that it uses LDAP remote user management.

Note: Before you configure the HMC so that it uses LDAP authentication, you must ensure that a working network connection exists between the HMC and the LDAP servers.

About this task

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

Procedure

1. In the navigation area, click **User management**, and then select **LDAP**. The LDAP Server Definition window opens.
2. Select **Enable LDAP**.
3. Define an LDAP server to use for authentication.
4. Define the LDAP attribute that is used to identify the user that is being authenticated. The default is **uid**, but you can use your own attributes.
5. Define the distinguished name tree, also known as the search base, for the LDAP server. You can use this field to specify the search criteria for the LDAP server that is used to locate the user record to authenticate the user. For example, **`dc=example, dc=com`**. Click **Add** to add more than one distinguished name tree to the LDAP server. All the distinguished name trees that are added by the user is displayed in a list. If you want to delete an entry in the list, select the distinguished name tree and click **Remove**.
6. Specify the search scope for limiting the search of the LDAP server for the user ID of the user being authenticated. The two options that are available are:

   - one
   - sub

   The default value is **one**.
7. Enable LDAP for Remote User Management by selecting **LDAP for Remote User Management** check box.
8. Configure the following properties under **LDAP for Remote User Management Configuration** section:

   - `LDAP Attribute to Retrieve User Properties`: The LDAP attribute that locates and retrieves the role and authorization properties of the user being authenticated.
   - `LDAP Group Login (Optional)`: The **LDAP Group Login** field is applicable only when Remote User Management is enabled. You can specify a value for the **LDAP Group Login** field when you configure the LDAP server so that you can retrieve the group login information for a specific user from the LDAP server when required.
   - `Attributes for Group Members (Optional)`: The **LDAP Group Member Login** field is applicable only when remote user management is enabled. You can specify a value for the **LDAP Group Member Login** field when you configure the LDAP server so that you can retrieve the member information for a specific user when required.
   - `Use Kerberos for User Authentication`: Select this option to specify that the remote user must be authenticated by Kerberos. This option applies only to remote user management.
   - `LDAP Attribute to Retrieve Remote User ID (optional)`: Select **Use Kerberos for User Authentication** to specify an LDAP attribute to locate and retrieve the remote authentication name from the LDAP server.
9. Click **OK**.

   Note: Ensure that a working network connection exists between the HMC and the LDAP servers.

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 verifies 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.

If you are using HMC Version 10.1.1020, or earlier, to configure the HMC so that it uses KDC servers for Kerberos remote authentication, complete the following steps:

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, complete the following steps:
   a. In the navigation area, click **Console Management**, and then select **Console Settings**.
   b. In the content pane, select **Change Date and Time**.
   c. Select the **NTP Configuration** tab.
   d. Select **Enable NTP service on this HMC**.
   e. Click **OK**.
2. Configure each remote HMC user's profile so that it uses Kerberos remote authentication instead of local authentication.
3. Optionally, 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, complete the following steps:
   a. In the navigation area, click **Users and Security**, and then select **Systems and Console Security**.
   b. In the content pane, select **Manage KDC**.
   c. Select **Actions > Import Service Key**. The Import Service Key window opens.
   d. Type the location of the service key file.
   e. Click **OK**.
4. Add a new KDC server to this HMC. To add a new KDC server to this HMC, complete the following steps:
   a. In the navigation area, click **Users and Security**, and then select **Systems and Console Security**.
   b. In the content pane, select **Manage KDC**.
   c. Select **Actions > Add KDC Server**. The Import Service Key window opens.
   d. Type the realm and the host name or IP address of the KDC server.
   e. Click **OK**.

If you are using HMC Version 10.2.1030, or later, to configure the HMC so that it uses KDC servers for Kerberos remote authentication, complete the following steps:

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, complete the following steps:
   a. In the navigation area, click **HMC management**, and then select **HMC settings**.
   b. In the content pane, select **Use network time protocol (NTP) server to manage date and time** under **Date and time** section.
2. Configure each remote HMC user's profile so that it uses Kerberos remote authentication instead of local authentication.
3. Optionally, 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, complete the following steps:
   a. In the navigation area, click **User management**, and then select **KDC**.
   b. Select **Actions > Import Service Key**. The **Import Service Key** window opens.
   c. Type the location of the service key file.
   d. Click **OK**.
4. Add a new KDC server to this HMC. To add a new KDC server to this HMC, complete the following steps:

a. In the navigation area, click **User management**, and then select **KDC**.

b. Select **Actions > Add KDC Server**. The **Import Service Key** window opens.

c. Type the realm and the host name or IP address of the KDC server.

d. Click **OK**.

Configuring the local console to report errors to service and support

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

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

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

Before you begin

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

Before you begin this task, ensure that:

- The network administrator verifies that connectivity is allowed.
- If you are configuring internet support through a proxy server, you must also have the following information:
  - The IP address and port of the proxy server
  - The proxy authentication information
- The adapter that is 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 21.
- An Ethernet cable physically connects the HMC to the LAN.

If you are using HMC Version 10.1.1020, or earlier, to configure the HMC so that it is a call-home server by using the call-home wizard, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to configure the HMC so that it is a call-home server by using the call-home wizard, complete the following steps:

1. In the navigation area, click **Call home** > **Setup electronic service agent**. The Connectivity and Call-Home Servers wizard opens. Follow the instructions in the wizard to configure call-home.

Configuring the local console to report errors to service and support

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

Configuring an HMC to contact service and support by using LAN-based internet and SSL

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

Before you begin

Before you begin this task, ensure that:

- The network administrator verifies that connectivity is allowed..
- Customer contact information is configured.
  - If you are using HMC Version 10.1.1020, or earlier, to verify the contact information, click **Serviceability** > **Service Management** > **Manage Customer Information**.

  - If you are using HMC Version 10.2.1030, or later, click **Call home** > **Customer information**.
- If you are configuring internet support through a proxy server, you must also have the following information:
  - 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 22.
- An Ethernet cable physically connects the HMC to the LAN.

About this task

If you are using HMC Version 10.1.1020, or earlier, to configure the HMC as a Call Home server by using LAN-based internet and SSL, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Service Management**.
2. In the Connectivity section, click **Manage Outbound Connectivity**. The Call-home Server Consoles window opens.
3. Click **Configure.**
4. In the **Outbound Connectivity Settings** window, check **Enable local system as call-home server**.
5. Accept the agreement.
6. In the Outbound Connectivity Settings window, select the **Internet** page.
7. Check the **Allow an existing internet connections for service** box.
8. If you are using an SSL proxy, check the **Use SSL proxy** box.
9. If you are using an SSL proxy, complete 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 user ID and password. Obtain the user ID and password from the network administrator.
11. Select the **Protocol to Internet** you want to use.
12. On the **Internet** page, click **Test**.
13. In the **Test internet** window, click **Start**.
14. Verify that the test completes successfully.
15. In the Test internet window, click **Cancel**.
16. In the Outbound Connectivity Settings window, click **OK**.

If you are using HMC Version 10.2.1030, or later, to configure the HMC as a Call Home server by using LAN-based internet and SSL, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Outbound connectivity**. The **Call-home Server Consoles** window opens.
2. Click **Configure.**
3. In the **Outbound Connectivity Settings** window, check **Enable local system as call-home server**.
4. Accept the agreement.
5. In the Outbound Connectivity Settings window, select the **Internet** page.
6. Check the **Allow an existing internet connections for service** box.
7. If you are using an SSL proxy, check the **Use SSL proxy** box.
8. If you are using an SSL proxy, complete the proxy's address and port. Obtain this information from the network administrator.

9. 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 user ID and password. Obtain the user ID and password from the network administrator.
10. Select the **Protocol to Internet** you want to use.
11. On the **Internet** page, click **Test**.
12. In the **Test internet** window, click **Start**.
13. Verify that the test completes successfully.
14. In the Test internet window, click **Cancel**.
15. In the Outbound Connectivity Settings window, click **OK**.

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

Choose existing Hardware Management Console (HMC) call-home servers that are recognized or discovered by the HMC to report errors.

Before you begin

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.

About this task

If you are using HMC Version 10.1.1020, or earlier, to choose a discovered HMC to call home when the HMC reports errors, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to choose a discovered HMC to call home when the HMC reports errors, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Outbound connectivity**. The **Call-Home Server Consoles** window opens.
2. Click **Use discovered call-home server consoles**. The HMC displays the IP address or host name of the HMCs configured for call-home.
3. Click **OK**.

Results

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** and 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.

About this task

If you are using HMC Version 10.1.1020, or earlier, to verify that your call-home configuration is working, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Service Management**.
2. In the content pane, click **Create Event**.
3. Select **Test Automatic problem Reporting** and type a comment.

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

If you are using HMC Version 10.2.1030, or later, to verify that your call-home configuration is working, complete the following steps:

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

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 30.

About this task

If you are using HMC Version 10.1.1020, or earlier, to authorize users to view collected system data, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to authorize users to view collected system data, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Service user authorization**.
2. Enter your IBM ID.
3. Click **OK**.

Transmitting service information

You can transmit information to your service provider immediately, or you can schedule the information to be sent regularly.

IBM provides personalized web functions that use information that is collected by IBM Electronic Service Agent. To use these functions, you must first register on the IBM Registration website at http://www.ibm.com/account/profile. To authorize users to use the Electronic Service Agent information to personalize the web functions, see "Authorizing users to view collected system data" on page 57. For more information about the benefits of registering an IBM ID with your systems, see http://www.ibm.com/support/electronic.

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

If you are using HMC Version 10.1.1020, or earlier, to transmit service information, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Service Management**.
2. In the content pane, click **Transmit Service Information.**
3. Complete the tasks in the **Transmit Service Information** window, and click **OK**.

If you are using HMC Version 10.2.1030, or later, to transmit service information, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Transmit service information**.
2. Complete the tasks in the **Transmit Service Information** window, and click **OK**.

Configuring the Events Manager for Call Home

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

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

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

```
chhmc -c emch

-s {enable | disable}

[--callhome {enable | disable}]

[--help]
```

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

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

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

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

The Events Manager for Call Home task can be run from any HMC or from multiple HMCs.

If you are using HMC Version 10.1.1020, or earlier, to register a management console with the Events Manager for Call Home task, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Events Manager for Call Home**.
2. From the **Events Manager for Call Home** pane, click **Manage Consoles**.
3. From the **Manage Registered Consoles** window, click **Add Console** to enter information to register a management console with the Events Manager for Call Home task.

4. Click **OK** to commit the changes to the list of registered management console.

If you are using HMC Version 10.2.1030, or later, to register a management console with the Events Manager for Call Home task, complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Events manager for call home**.
2. From the **Events Manager for Call Home** pane, click **Manage Consoles**.
3. From the **Manage Registered Consoles** window, click **Add Console** to enter information to register a management console with the Events Manager for Call Home task.
4. Click **OK** to commit the changes to the list of registered management console.

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

Setting passwords for the managed system

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

Before you begin

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

About this task

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

Updating your server password

Before you begin

If you are using HMC Version 10.1.1020, or earlier, to update your server password, complete the following steps:

1. In the navigation area, select the managed system and click **Users and Security**, and then select **Users and Roles**.
2. Click **Change Password**. The Update Password window opens.
3. Type the required information and click **OK**.

If you are using HMC Version 10.2.1030, or later, to update your server password, complete the following steps:

1. In the title bar, click the **User** icon, and then select **Change password**. The **Update Password** window opens.
2. Type the required information and click **OK**.

Updating your Advanced System Management Interface (ASMI) general password

Before you begin

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

Resetting the Advanced System Management (ASM) administrator password

Before you begin

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

About this task

If you are using HMC Version 10.1.1020, or earlier, to update your ASMI general password, complete the following steps:

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**.

If you are using HMC Version 10.2.1030, or later, to update your ASMI general password, complete the following steps:

1. In the navigation area of the HMC, select **System resources** > **Systems**.
2. Select the managed system, and click **Connections and operations** > **Launch advanced system management (ASMI)**. The **Launch ASM Interface** window opens.
3. Select a Service Processor IP Address and click **OK**. The ASM interface opens.
4. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
5. In the navigation area, expand **Login Profile**.
6. Select **Change Password**.
7. Specify the required information, and click **Continue**.

Testing the connection between the HMC and the managed system

Learn how to verify that you are properly connected to the network.

About this task

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

- Super administrator
- Service representative

If you are using HMC Version 10.1.1020, or earlier, to test the connection between the HMC and the managed system, complete the following steps:

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

If you are using HMC Version 10.2.1030, or later, to test the connection between the HMC and the managed system, complete the following steps:

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

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**.

Results

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

To understand how the HMC can be used in a network, see “HMC network connections” on page 21.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC by using the menus ” on page 37.

Postconfiguration steps

After you install and configure the HMC, back up HMC data as necessary.

Backing up management console data

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

Before you begin

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.

About this task

To back up the HMC hard disk drive to a remote system, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

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

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

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

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.

If you are using HMC Version 10.1.1020, or earlier, to back up the HMC hard drive to a remote system, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Backup Management Console Data**.
3. From the **Backup Management Console Data** window, select the archive option you want to perform.

4. Click **Next**, then follow the appropriate instructions depending on the option you chose.
5. Click **OK** to continue with the backup process.

If you are using the HMC Version 10.2.1030, or later, to back up the HMC hard drive to a remote system, complete the following steps:

1. In the navigation area, click **HMC management** > **HMC actions** > **Backup HMC data**.
2. From the **Backup HMC Data** window, select the archive option you want to perform.
3. Click **Next**, then follow the appropriate instructions depending on the option you chose.
4. Click **OK** to continue with the backup process.

Updating, upgrading, and migrating your HMC machine code

Updates and upgrades are periodically released for the HMC to add new functionality and to improve existing features. Learn more about the differences between updating, upgrading, and migrating your HMC machine code. Also learn how to perform an HMC machine code update, upgrade, or migration.

When you are finished with each of these tasks, the HMC reboots but the partitions do not.

Updating HMC code

Applies maintenance to an existing HMC level

Does not require that you perform the **Save upgrade data** task

Upgrading HMC code

Replaces HMC software with a new release or fix level of the same program

Requires that you boot from recovery media

Migrating HMC code

Moves HMC data from one HMC version to another

A migration is a type of upgrade.

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

Determining your HMC machine code version and release

Find out how to view the HMC machine code version and release.

About this task

The level of machine code on the HMC determines the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

If you are using HMC Version 10.1.1020, or earlier, to view the HMC machine code version and release, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the **Current HMC Driver Information** heading, including: the HMC version, release, maintenance level, build level, and base versions.

If you are using HMC Version 10.2.1030, or later, to view the HMC machine code version and release, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the **Current HMC Driver Information** heading, including: the HMC version, release, maintenance level, build level, and base versions.

Obtaining and applying machine code updates for the HMC with an internet connection

Learn how to obtain machine code updates for the HMC when the HMC has an internet connection.

About this task

To obtain machine code updates for the HMC, complete all steps.

Step 1. Ensure that you have an Internet connection

About this task

To download updates from the service and support system or website to your HMC or server, you must have one of the following connections:

- SSL connectivity with or without a SSL proxy
- Internet VPN

If you are using HMC Version 10.1.1020, or earlier, to ensure that you have an internet connection,complete the following steps:

1. In the navigation area, click **Serviceability**, and then select **Service Management**.
2. In the content pane, **Manage Outbound Connectivity**.
3. Select the tab for the type of outbound connectivity that you chose for your HMC (Internet VPN or SSL connectivity).

   Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see Setting up your server to connect to IBM service and support.
4. Click **Test**.
5. Verify that the test completes successfully.

   Note: If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on DVD.

   Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.
6. Continue with "Step 2. View the existing HMC machine code level" on page 64.

If you are using HMC Version 10.2.1030, or later, to ensure that you have an internet connection, complete the following steps:

1. In the navigation area, click **Call home**, and then select **Outbound connectivity** to view the **Manage Outbound Connectivity** page.
2. 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.
3. Click **Test**.
4. Verify that the test completes successfully.

   Note: If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on DVD.

   Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.
5. Continue with "Step 2. View the existing HMC machine code level" on page 64.

Step 2. View the existing HMC machine code level

About this task

If you are using HMC Version 10.1.1020, or earlier, to view the existing HMC machine code level, complete the following steps:

1. In the navigation area, click the **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 3. View the available HMC machine code levels" on page 64.

If you are using HMC Version 10.2.1030, or later, to view the existing HMC machine code level, complete the following steps:

1. In the navigation area, click the **HMC Management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 3. View the available HMC machine code levels" on page 64.

Step 3. View the available HMC machine code levels

About this task

To find out if there are new HMC machine code updates available, contact service and support.

If you are using HMC Version 10.1.1020, or earlier, to view the available HMC machine code levels, complete the following steps:

1. In the navigation area, click the **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.

If you are using HMC Version 10.2.1030, or later, to view the available HMC machine code levels, complete the following steps:

1. In the navigation area, click the **HMC Management**.
2. In the content pane, click **Update HMC**.
3. Select the **IBM Website** option to view the available updates.
4. Continue with "Step 4. Apply the HMC machine code update" on page 64.

Step 4. Apply the HMC machine code update

About this task

If you are using HMC Version 10.1.1020, or earlier, to apply the HMC machine code update, complete the following steps:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see "Backing up management console data" on page 61. Then continue with the next step.
2. In the navigation area, click **Console Management**, and then select **Console Management**.
3. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.

4. Follow the instructions in the Wizard to install the update.
5. Shut down and then restart the HMC for the update to take effect.
6. Click **Log on and launch the Hardware Management Console web application**.
7. Log in to the HMC interface.

If you are using HMC Version 10.2.1030, or later, to apply the HMC machine code update, complete the following steps:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see "Backing up management console data" on page 61. Then continue with the next step.
2. In the navigation area, click **HMC Management**.
3. In the content pane, click **Update HMC**. The Install Corrective Service Wizard opens.
4. Select the **IBM Website** option as the service repository.
5. Follow the instructions in the Wizard to install the update.
6. Shut down and then restart the HMC for the update to take effect.
7. Click **Log on and launch the Hardware Management Console web application**.
8. Log in to the HMC interface.

Step 5. Verify that the HMC machine code update installed successfully

About this task

If you are using HMC Version 10.1.1020, or earlier, to verify that the HMC machine code update installed correctly, complete the following steps:

1. In the navigation area, click the **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code displayed is not the level that you installed, perform the following steps:
   a. Select the network connection on the HMC.
   b. Retry the firmware update using a different repository.
   c. If the problem persists, contact your next level of support.

If you are using HMC Version 10.2.1030, or later, to verify that the HMC machine code update installed correctly, complete the following steps:

1. In the navigation area, click the **HMC Management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code displayed is not the level that you installed, perform the following steps:
   a. Select the network connection on the HMC.
   b. Retry the firmware update using a different repository.
   c. If the problem persists, contact your next level of support.

Obtaining and applying machine code updates for the HMC by using removable media or remote server

Learn how to obtain machine code updates for the Hardware Management Console (HMC) by using removable media or remote server.

About this task

To obtain HMC machine code updates, complete all steps.

Note: For HMC model 7063-CR1, you can connect an external USB DVD drive.

Step 1. View the existing HMC machine code level

Before you begin

If you are using HMC Version 10.1.1020, or earlier, to view the existing HMC machine code level, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 2. View the available HMC machine code levels" on page 66.

If you are using HMC Version 10.2.1030, or later, to view the existing HMC machine code level, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 2. View the available HMC machine code levels" on page 66.

Step 2. View the available HMC machine code levels

Before you begin

To find out whether new HMC machine code updates are available, contact IBM service and support.

To view the available HMC machine code levels, complete the following steps:

About this task

Procedure

1. From a computer or server with an internet connection, go to the Fix Central website.
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" on page 67.

Step 3. Obtain the HMC machine code update

Before you begin

To obtain the HMC machine code update, complete the following steps:

About this task

To order the HMC machine code update on removable media, contact service and support.

You can order the HMC machine code update through the Fix Central website, contact service and support, or download it to an FTP server.

Ordering the HMC machine code update through the Fix Central website

1. From a computer or server with an Internet connection, go to the Fix Central website.
2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File names / Package area and locate the update that 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 Fix Central website.
2. Under Supported HMC products, select the latest HMC level.
3. Scroll down to the File names / Package area and locate the update that you want to download.
4. Click the update that you want to download.
5. Accept the license agreement, and save the update to your removable media.

What to do next

When you are finished, continue with “Step 4. Apply the HMC machine code update” on page 67.

Step 4. Apply the HMC machine code update

Before you begin

If you are using HMC Version 10.1.1020, or earlier, to apply the HMC machine code update, complete the following steps:

1. Before you install updates to the HMC machine code, back up HMC data. For more information, see “Backing up management console data” on page 61.
2. If you obtained or created the update on DVD-RAM, insert it into the DVD drive on the HMC. If you obtained or created the update on a USB memory device, insert the memory device.
3. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see “Backing up management console data” on page 61. Then continue with the next step.
4. In the navigation area, click **Console Management**, and then select **Console Management**.
5. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.
6. Follow the instructions in the Wizard to install the update.
7. Shut down, restart, and log back in to the HMC for the update to take effect.
8. Continue with “Step 5. Verify that the HMC machine code update installed successfully” on page 68.

If you are using HMC Version 10.2.1030, or later, to apply the HMC machine code update, complete the following steps:

1. Before you install updates to the HMC machine code, back up HMC data. For more information, see "Backing up management console data" on page 61.
2. If you obtained or created the update on DVD-RAM, insert it into the DVD drive on the HMC. If you obtained or created the update on a USB memory device, insert the memory device.
3. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see "Backing up management console data" on page 61. Then continue with the next step.
4. In the navigation area, click **HMC Management**.
5. In the content pane, click **Update HMC**. The Install Corrective Service Wizard opens.
6. Follow the instructions in the Wizard to install the update.
7. Shut down, restart, and log back in to the HMC for the update to take effect.
8. Continue with "Step 5. Verify that the HMC machine code update installed successfully" on page 68.

Step 5. Verify that the HMC machine code update installed successfully

Before you begin

If you are using HMC Version 10.1.1020, or earlier, to verify that the HMC machine code update installed successfully, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code that is displayed is not the level that you installed, 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.

If you are using HMC Version 10.2.1030, or later, to verify that the HMC machine code update installed successfully, complete the following steps :

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code that is displayed is not the level that you installed, perform the following steps:
   a. Retry the machine code update. If you created a DVD for this procedure, use a new media.
   b. If the problem persists, contact your next level of support.

Upgrading your HMC software

Learn how to upgrade the software on an HMC from one release to the next while you maintain your HMC configuration data.

About this task

To upgrade the machine code on an HMC, complete all steps.

Note: For HMC models 7063-CR1 and 7063-CR2, you can connect an external USB DVD drive.

Step 1. Obtain the upgrade

About this task

To order the HMC machine code upgrade on DVD-RAM, contact service and support.

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

To obtain the upgrade through the Fix Central website, complete the following steps:

1. From a computer or server with an internet connection, go to the Hardware Management Console website at http://www-933.ibm.com/support/fixcentral/.
2. Click **Continue**The Hardware Management Console site is displayed..
3. Navigate to the HMC version you want to upgrade to.
4. Locate the download and ordering section.

   Note: If you do not have access to the internet, contact IBM service and support to order the upgrade on DVD.
5. Follow the on-screen prompts to submit your order.
6. After you have the upgrade, continue with “Step 2. View the existing HMC machine code level” on page 69.

Step 2. View the existing HMC machine code level

About this task

If you are using HMC Version 10.1.1020, or earlier, to determine the existing level of machine code on an HMC, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**. In the navigation area, click **Updates**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Continue with “Step 3. Back up the managed system's profile data” on page 70.

If you are using HMC Version 10.2.1030, or later, to determine the existing level of machine code on an HMC, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **Update HMC**.
3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Continue with “Step 3. Back up the managed system's profile data” on page 70.

Step 3. Back up the managed system's profile data

About this task

If you are using HMC Version 10.1.1020, or earlier, to back up the managed system's profile data, complete the following steps:

1. Select the system for which you want to save the profile data.
2. Click **Actions** > **View All Actions** > **Legacy** > **Manage Partition Data** > **Backup**.
3. Type a backup file name and record this information.
4. Click **OK**.
5. Repeat these steps for each system.
6. Continue with "Step 4. Back up HMC data" on page 70.

If you are using HMC Version 10.2.1030, or later, to back up the managed system's profile data, complete the following steps:

1. Select the system for which you want to save the profile data, and then click **Config backup** > **Backup profile**.
2. Type a backup file name and record this information.
3. Click **OK**.
4. Repeat these steps for each system.
5. Continue with "Step 4. Back up HMC data" on page 70.

Step 4. Back up HMC data

About this task

Back up HMC data before you install a new version of HMC software so that previous levels can be restored in the event of a problem while you upgrade the software. Do not use this critical console data after a successful upgrade to a new version of the HMC software.

Note: To back up to removable media, you need to have that media available.

If you are using HMC Version 10.1.1020, or earlier, to back up HMC data, complete the following steps:

1. If you plan to back up to media, perform the following steps to format the media:
   a. Insert the media into the drive.
   b. In the navigation area, click **Serviceability**, and then select **Service Management**.
   c. In the content pane, click **Format Media**.
   d. Select the media type.
   e. Select the format type.
   f. Click **OK**.
2. In the navigation area, click **Console Management**, and then select **Console Management**.
3. In the content pane, click **Backup Management Console Data**. The **Backup Management Console Data** window opens.
4. Select an archive option. You can back up to media on a local system, a remote system that is mounted to the HMC file system (for example, NFS), or send the backup to a remote site by using File Transfer Protocol (FTP).
   - To back up to a local system, choose **Back up to media on local system** and follow the instructions.
   - To back up to a mounted remote system, choose **Back up to mounted remote system** and follow the instructions.

- To back up to a remote FTP site, choose **Send back up critical data to remote site** and follow the instructions.

5. Continue with "Step 5. Record the current HMC configuration information" on page 71.

If you are using HMC Version 10.2.1030, or later, to back up HMC data, complete the following steps:

1. If you plan to back up to media, perform the following steps to format the media:
   a. Insert the media into the drive.
   b. In the navigation area, click **HMC management** > **HMC actions** > **Format media**.
   c. Select the media type.
   d. Select the format type.
   e. Click **OK**.
2. In the navigation area, click **HMC management**, and then select **HMC actions** > **Backup HMC data**. The **Back up HMC Data** window opens.
3. Select an archive option. You can back up to media on a local system, a remote system that is mounted to the HMC file system (for example, NFS), or send the backup to a remote site by using File Transfer Protocol (FTP).
   - To back up to a local system, choose **Back up to media on local system** and follow the instructions.
   - To back up to a mounted remote system, choose **Back up to mounted remote system** and follow the instructions.
   - To back up to a remote FTP site, choose **Send back up critical data to remote site** and follow the instructions.
4. Continue with "Step 5. Record the current HMC configuration information" on page 71.

Step 5. Record the current HMC configuration information

About this task

Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information.

If you are using HMC Version 10.1.1020, or earlier, to record the current HMC configuration, complete the following steps:

1. Select a managed system or any partitions that you want to record HMC configuration information.
2. From the menu pod, select **Actions** > **Schedule Operations**. All scheduled operations for the target that you selected are displayed.
3. Select **Sort** > **By Object**.
4. Select each object and record the following details:
   - Object Name
   - Schedule date
   - Operation Time (displayed in 24-hour format)
   - Repetitive (if Yes, complete the following steps):
     a. Select **View** > **Schedule Details**.
     b. Record the interval information.
     c. Close the scheduled operations window.
     d. Repeat for each scheduled operation.
5. Close the **Customize Scheduled Operations** window.
6. Continue with "Step 6. Record remote command status" on page 72.

If you are using HMC Version 10.2.1030, or later, to record the current HMC configuration, complete the following steps:

1. Select a managed system or any partitions for which you want to record HMC configuration information, and click **Connections and operations** > **Schedule operations**. All scheduled operations for the target that you selected are displayed.
2. Select **Sort** > **By Object**.
3. Select each object and record the following details:
   - Object Name
   - Schedule date
   - Operation Time (displayed in 24-hour format)
   - Repetitive (if Yes, complete the following steps):
     a. Select **View** > **Schedule Details**.
     b. Record the interval information.
     c. Close the scheduled operations window.
     d. Repeat for each scheduled operation.
4. Close the **Customize Scheduled Operations** window.
5. Continue with “Step 6. Record remote command status” on page 72.

Step 6. Record remote command status

About this task

If you are using HMC Version 10.1.1020, or earlier, to record remote command status, complete the following steps:

1. In the navigation area, click **Users and Security**, and then select **Systems and Console Security**.
2. In the content pane, click **Enable Remote Command Execution**.
3. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
4. Click **Cancel**.
5. Continue with “Step 7. Save upgrade data” on page 72.

If you are using HMC Version 10.2.1030, or later, to record remote command status, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **HMC settings**.
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” on page 72.

Step 7. Save upgrade data

About this task

You can save the current HMC configuration in a designated disk partition on the HMC or to local media. Save upgrade data only immediately before you upgrade your HMC software to a new release. You can restore the HMC configuration settings after you upgrade.

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

If you are using HMC Version 10.1.1020, or earlier, to save upgrade data, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Save Upgrade Data**. The **Save Upgrade Data** wizard opens.
3. Select the media on which you want to save the upgrade data. If you choose to save to removable media, insert the media now. Click **Next**.
4. Click **Finish**.
5. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

   Note: If the save upgrade data task fails, do not continue the upgrade process.
6. Click **OK**.
7. Continue with "Step 8. Upgrade the HMC software" on page 73.

If you are using HMC Version 10.2.1030, or later, to save upgrade data, complete the following steps:

1. In the navigation area, click **HMC management**.
2. In the content pane, click **HMC actions** > **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 73.

Step 8. Upgrade the HMC software

About this task

To upgrade the HMC software, restart the system with the removable media in the DVD drive.

If you are using HMC Version 10.1.1020, or earlier:

1. Insert the HMC Product Installation media into the DVD drive.
2. In the navigation area, click **Console Management**, and then select **Console Management**.
3. In the content pane, select **Shutdown or Restart the Managment Console**.
4. Ensure **Restart the HMC** is selected.
5. Click **OK**. The HMC restarts and system information scrolls on the window.
6. Select **Upgrade** and click **Next**.
7. Choose from the following options:
   - If you saved the upgrade data during the previous task, continue with the next step.
   - If you did not save the upgrade data previously in this procedure, you must save the upgrade data now before you continue.
8. Select **Upgrade from media** and click **Next**.
9. Confirm the settings and click **Finish**.
10. Follow the prompts.

    Note:

    - If the screen goes blank, press the space bar to view the information.

- The first DVD can take approximately 20 minutes to install.

11. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
12. Continue with "Step 9. Verify that the HMC machine code upgrade installed successfully" on page 74.

If you are using HMC Version 10.2.1030, or later:

1. Insert the HMC Product Installation media into the DVD drive.
2. In the navigation area, click **HMC management**.
3. In the content pane, select **HMC actions** > **Shutdown or restart**.
4. Ensure **Restart the HMC** is selected.
5. Click **OK**. The HMC restarts and system information scrolls on the window.
6. Select **Upgrade** and click **Next**.
7. Choose from the following options:
    - If you saved the upgrade data during the previous task, continue with the next step.
    - If you did not save the upgrade data previously in this procedure, you must save the upgrade data now before you continue.
8. Select **Upgrade from media** and click **Next**.
9. Confirm the settings and click **Finish**.
10. Follow the prompts.

    Note:

    - If the screen goes blank, press the space bar to view the information.
    - The first DVD can take approximately 20 minutes to install.
11. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
12. Continue with "Step 9. Verify that the HMC machine code upgrade installed successfully" on page 74.

Step 9. Verify that the HMC machine code upgrade installed successfully

About this task

If you are using HMC Version 10.1.1020, or earlier, to verify that the HMC upgrade is installed successfully, complete the following steps:

1. In the navigation area, click **Console Management**, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code that is displayed is not the level that you installed, retry the upgrade task by using a new DVD. If the problem persists, contact your next level of support.

If you are using HMC Version 10.2.1030, or later, to verify that the HMC upgrade is installed successfully, complete the following steps:

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

3. In the new window, view and record the information that appears under the Current HMC Driver information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code that is displayed is not the level that you installed, retry the upgrade task by using a new DVD. If the problem persists, contact your next level of support.

Upgrading HMC from remote location by using network upgrade images

Learn how to upgrade the software on an HMC from a remote location by using network upgrade images.

About this task

Learn how to upgrade the software on an HMC from a remote location by using network upgrade images.

Procedure

1. From a computer or server with an internet connection, go to the Hardware Management Console Support and downloads website (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html).
2. Download the appropriate HMC V9 network images and save them on an FTP server.

   You cannot download these files directly to the HMC. You must download the image files to a server that accepts FTP requests.
3. Ensure that you download the following files:
   - img2a
   - img3a
   - base.img
   - disk1.img
   - hmcnetworkfiles.sum
4. Save the upgrade data on the HMC. Run the following commands to save the upgrade data:
   - To save data on both DVD and HDD, run the following commands:

     ```
     mount /media/cdrom
     ```

     ```
     saveupgdata -r diskdvd
     ```
   - To save data on the HDD, run the following command:

     ```
     saveupgdata -r disk
     ```
5. Copy the upgrade files to the bootable disk partition on the HMC. Run the **getupgfiles** command to copy the files.

   Example: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**

   Where,
   - **ftp server** is the host name or IP address of the FTP server where you download the HMC network images.
   - **user id** is a valid user ID on the FTP server. If you do not specify the password with the `--passwd` argument, you are prompted for a password.
   - **remote directory** is the directory on your FTP server where the HMC network images are saved.
6. Restart the HMC to upgrade the code that is copied to the bootable disk partition. Run the **chhmc -c altdiskboot -s enable --mode upgrade** to restart the HMC.
7. Restart the HMC and start the upgrade. Run the **hmcshutdown -r -t now** command to start the upgrade.

Securing the HMC

Learn how to enhance the security of your Hardware Management Console (HMC) that is based on your corporate security standards.

The default configuration of the HMC provides ample security for most enterprise users. With the Hardware Management Console (HMC) Version 8.4.0, or later, you can further enhance the security of the HMC that is based on your corporate security standards. To enhance the security for the HMC, you must set the HMC to a minimum of Level 1 security. You may choose Level 2 and Level 3 security depending on your environment and the corporate security requirements.

Note: Before changing the security level, check with your corporate security compliance team.

Level 1 security

To secure the HMC (level 1 security), complete the following steps:

1. Change the predefined password for the default `hscroot` user. For more information about password policy, see "Enhanced password policy" on page 79.
2. If the HMC does not belong to a physically secure environment, set the `grub` password by running the following command: `chhmc -c grubpasswd -s enable --passwd <new grub password>`
3. If you have configured the Integrated Management Module (IMM) on the HMC, set a strong IMM password.
4. Set a strong password for the *admin* user and general users on all servers.
5. Update the HMC with the latest released security fixes. For more information about the security fixes, see IBM Fix Central.

Level 2 security

If you have multiple users, complete the following steps to enhance the security for the HMC:

1. Create an account for each user on the HMC and assign the required roles and resources to users. For more information about the various roles in the HMC, see HMC tasks, user roles, IDs, and associated commands.

   Note: Ensure that you assign only the required resources and roles for users that are created on HMC. If necessary, you can also create custom roles.
2. Enable user data replication between different Hardware Management Consoles. The user data replication can be performed in Primary HMC-Secondary HMC mode or Peer-Peer mode. For more information about user data replication, see Manage Data Replication.
3. Import a certificate that is signed by the Certificate Authority.

Level 3 security

If you have multiple Hardware Management Consoles and system administrators, complete the following steps to enhance the security for the HMC:

1. Use centralized authentication such as Lightweight Directory Access Protocol (LDAP) or Kerberos. For more information about configuring LDAP, see How to Configure LDAP on HMC.
2. Enable user data replication between different Hardware Management Consoles.
3. Ensure that the HMC is in NIST SP 800-131A mode so that the HMC uses only strong ciphers.
4. Block ports that are not required in the firewall. For information about the HMC ports that can be used, see the following table:

© Copyright IBM Corp. 2021, 2024

Table 24. Port used by the user for interaction with HMC

Port	Description	Type	Protocol version (Default mode)	Protocol Version (NIST mode)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	SNMP Agent	UDP	SNMP v3	SNMP v3
162	SNMP Trap	UDP	SNMP v3	SNMP v3
427	SLP	UDP	N/A	N/A
443	HMC GUI and REST API	TCP	HTTPS (TLS 1.2, TLS 1.3)	HTTPS (TLS 1.2, TLS 1.3)
657	RMC	TCP/UDP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)
2300	5250 Terminal for IBM i	TCP	Plain text	Plain text
2301	5250 Secure terminal for IBM i	TCP	TLS 1.2, TLS 1.3	TLS 1.2, TLS 1.3
5989	CIM (legacy port, nonfunctional)	TCP	Non-functional	Non-functional
9900	FCS: HMC-HMC discovery	UDP	FCS	FCS
9920	FCS: HMC-HMC communication	TCP	HTTPS (TLS 1.2, TLS 1.3)	HTTPS (TLS 1.2, TLS 1.3)
11125	PowerSC profile for HMC	TCP/UDP	TLS 1.2	TLS 1.2
12443	HMC REST API (legacy port)	TCP	HTTPS (TLS 1.2, TLS 1.3)	HTTPS (TLS 1.2, TLS 1.3)
12347	RSCT Peer Domain	UDP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)
12348	RSCT Peer Domain	UDP	RSCT (Plain text + hash and sign)	RSCT (Plain text + hash and sign)
17443	Manage eBMC systems	TCP	HTTPS (TLS 1.2, TLS1.3)	HTTPS (TLS 1.2, TLS1.3)

Notes:

- In future releases, the use of port 12443 will no longer be supported, and it is recommended to exclusively use port 443 instead.
- You must use only SSH (port 22), HTTPS (port 443), and 5250 secure terminal for IBM i (port 2301) that is exposed to an intranet. All other ports must be used in a private or isolated network. You can use a separate Ethernet port and VLAN for the Resource Monitoring and Control (RMC) (port 657), FCS (port 9900 and port 9920), and RSCT Peer Domain (port 12347 and port 12348).
- Ports that are listed in the **`netstat`** command are used for internal processes only.

Enhanced password policy

You can enforce password requirements for locally authenticated users by using the Hardware Management Console (HMC). The enhanced password policy function allows the system administrator to set password restrictions. The enhanced password policy applies to the systems in which an HMC is installed.

System administrators can use the enhanced password policy to define a single password policy for all users. The HMC provides a medium security password policy, which can be activated by the system administrators to set password restrictions. The system administrator can also choose to activate the medium security policy or a new user-defined policy. The HMC medium security password policy cannot be removed from the system. The following table lists the attributes of the medium security policy and the default values.

Table 25. Password attributes for the HMC medium security password policy

Attribute	Description	Default value
`min_pwage`	The minimum number of days for which a password must remain active.	1
`pwage`	The maximum number of days for which a password might remain active.	365
`min_length`	The minimum length of a password.	8
`hist_size`	The number of previously saved passwords that cannot be reused.	10
`warn_pwage`	When the password is about to expire, the number of days before which a user is warned that the password is about to expire.	7
`min_digits`	The minimum number of digits that are required to be used in the password.	None
`min_uppercase`	The minimum number of upper case characters.	1
`min_lowercase`	The minimum number of lower case characters.	6
`min_special_chars`	The minimum number of special characters that must be used in the password.	None
`inactivity_expiration`	The number of days that can elapse before an HMC user account is disabled due to inactivity.	180

Consider the following items about the HMC medium security password policy:

- The policy features for password age, login disablement and inactivity expiration are not applicable to the **hscroot**, **hscpe**, and **root** user IDs. The password character validation is applicable for these user IDs.
- The policy affects only the locally authenticated users that are managed by the HMC and the policy cannot be enforced on LDAP or Kerberos users.
- The HMC medium security password policy or the user-defined policy allows the system administrators to set password reuse restrictions.
- The HMC medium security password is read-only and the attributes of HMC medium security password cannot be changed. You can create a new user-defined password to set password restriction.

You can use the following commands to configure the HMC medium security password policy:

mkpwdpolicy
Imports the password policy from a file, which contains all the parameters, or creates a password policy.

lspwdpolicy
Lists all the available password policy profiles and searches for specific parameters. You can also view the password policy that is currently active.

rmpwdpolicy
Removes an existing inactive password policy.

Note: You cannot remove an active medium security policy and the default read-only password policy.

chpwdpolicy
Changes parameters of an inactive password policy.

Enabling PowerSC profile for the HMC

Learn how to enable PowerSC agent on the Hardware Management Console (HMC). You can apply and monitor the PowerSC profile from the HMC. The PowerSC Standard Edition product is delivered with HMC profiles along with the basic security hardening features.

Installing the PowerSC server

About this task

If you do not have the PowerSC server setup or the latest version of the PowerSC server, install the PowerSC server. For more information, see https://www.ibm.com/docs/en/powersc-standard

Enabling the PowerSC Agent

To enable the PowerSC agent, complete the following steps:

Procedure

1. Ensure that the incoming of IP addresses is allowed in **Firewall Settings** for the port 11125. In the HMC, open the firewall port 11125.
2. Get the `endpointTrustore.jks` file from the `powersc-uiServer`. You can find the file in the PowerSC server in the following location:

   ```
   /etc/security/powersc/uiServer/endpointTrustore.jks
   ```

   Use the **`getfile`** command to deploy it in the correct location in the HMC:

   ```
   getfile -t powersctrust -l s -f /etc/security/powersc/uiServer/
   endpointTruststore.jks -h <powerSc_server> -u <user>
   ```
3. Start the **powersc-uiAgent** service with the **chhmc** command.

   ```
   chhmc -s enable -c powerscuiagent
   ```
4. Log in to PowerSC server either from the GUI or ssh to complete the **`Generate Keystore`** operation. Click the **Keystore Requests** tab.

   a) From the **UI Endpoint Admin** page, click **Settings** > **Endpoint** > **Keystore** > **Generate Keystore**.

   b) Alternatively, you can use the following command to generate keystore: `/opt/powersc/uiServer/bin/generate_endpoint_keystore_uiServer.sh <endpoint FQDN>`
5. Check whether the agent is enabled by running the following command:

   ```
   lshmc -r
   ssh=enable,sshprotocol=2,sshusedns=enable,remotewebui=enable,xntp=disable,xn
   tpstatus=,xntpserver=,syslogserver=,syslogtcpserver=,syslogtlsserver=,altdis
   kboot=disable,ldap=disable,kerberos=disable,kerberos_default_realm=,kerberos
   _realm_kdc=,kerberos_clockskew=,kerberos_ticket_lifetime=,kpasswd_admin=,tra
   ce=,kerberos_keyfile_present=,security=legacy,sol=disabled,powerscuiagent=en
   abled
   ```
6. Go to the `powersc-uiServer` system and select **Endpoint admin** under the settings icon. The HMC will show up under the **Endpoints** tab of the **Endpoint admin page**.

Applying the HMC profile in the PowerSC server

About this task

After you enable PowerSC communication with the HMC, you can apply the HMC profile in the PowerSC server. For more information, see https://www.ibm.com/docs/en/powersc-standard/2.1?topic=concepts-hmc-hardening-profile

Disabling the PowerSC Agent

About this task

To disable the PowerSC agent service in the HMC, run the following command:

```
chhmc -s disable -c powerscuiagent
```

Example

```
lshmc -r
ssh=enable,sshprotocol=2,sshusedns=enable,remotewebui=enable,xntp=disable,xntps
tatus=,xntpserver=,syslogserver=,syslogtcpserver=,syslogtlsserver=,altdiskboot=
disable,ldap=disable,kerberos=disable,kerberos_default_realm=,kerberos_realm_kd
c=,kerberos_clockskew=,kerberos_ticket_lifetime=,kpasswd_admin=,trace=,kerberos
_keyfile_present=,security=legacy,sol=disabled,powerscuiagent=disabled
```

Solving common problems while securing the HMC

Learn how to solve some problems that you might encounter when you secure the HMC.

How to secure the connection between the Hardware Management Console (HMC) and the system?

The HMC connects to the system through the Flexible Service Processor (FSP). A proprietary binary protocol called Network Client protocol (NETC) is used for managing both FSP and Power hypervisor. The following table lists ports that are used by the HMC:

Table 26. Ports on FSP that are used to interact with the HMC

Port on FSP	Description	Protocol version (Default mode)	Protocol Version (NIST mode)
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Falls back to SSLv3 for support of older firmware.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). Falls back to SSLv3 for support of older firmware.	NETC (TLS 1.2)

How to lock the HMC?

If you want to enhance the security for your infrastructure, you can use an Intrusion Prevention System (IPS) device or add all Hardware Management Consoles and IBM Power systems servers behind a firewall. Also, you can disable network services on the HMC if you do not use it remotely or if you want to lock the HMC down. To disable network services on the HMC, complete the following steps:

1. Disable remote command execution by using the SSH port.
2. Disable remote virtual terminal (VTerm).
3. Disable remote web access (HMC graphical user interface and REST API).
4. Block ports in firewall by using HMC network settings for each configured Ethernet port.

How to set the HMC in NIST SP 800-131A compliance mode?

With HMC Version 8.1.0, or later, when you set the HMC in the compliance mode, only strong ciphers listed by NIST SP 800-131A are supported. You might not be able to connect to older Power systems servers such as, POWER5 servers that do not support Transport Layer Security (TLS 1.2). For more information about changing the security mode, see HMC V8R8 NIST mode.

How to view and change ciphers that are used by the HMC?

With HMC Version 8.1.0, or later, the HMC supports more secure cipher sets that are defined in NIST 800-131A. Ciphers that are used in the default mode are strong. For more information about encryption ciphers that are used by the HMC, run the **lshmcencr** command. If your corporate standards requires the use of a different set of ciphers, run the **chhmcencr** command to modify the encryption ciphers.

To list the encryption ciphers that are used by the HMC to encrypt user password, run the following command:

```
lshmcencr -c passwd -t c
```

To list the encryption ciphers that can currently be used by the HMC web user interface and REST API, run the following command:

```
lshmcencr -c webui -t c
```

To list the encryption ciphers and MAC algorithm that can currently be used by the HMC SSH interface, run the following command:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

How to check the strength of the certificate on the HMC?

The self-signed certificates on the HMC use SHA256 with 2048-bit RSA encryption, which is strong. If you are using CA signed certificates, ensure that you are not using the 1024-bit encryption, which is weak. The following certificates can be used for the HMC:

- The CA signed certificate can be used for the HMC graphical user interface and REST API (port 443).
- The port 9920 is used for HMC to HMC communication. You cannot replace this certificate with your own certificate.

How to choose between a self-signed certificate (default) or a CA signed certificate?

The HMC auto-generates a certificate during installation. However, you can generate a Certificate Signing Request (CSR) from the HMC and get a new certificate that is issued by a Certificate Authority. You can import this certificate into HMC. Ensure that you also obtain a domain name for the HMC. For more details about managing the certificates in HMC, see Manage Certificates.

How to audit the HMC?

The audit on the Hardware Management Consoles focuses on configured ciphers and the usage activity of the various HMC users. Use the following commands to view the usage activity of various HMC users:

Table 27. Ciphers that are used by the HMC

Purpose	Command
Password encryption (global setting)	`lshmcencr -c passwd -t c`
Password encryption for each user	`lshmcusr -Fname:password_encryption`
SSH ciphers	`lshmcencr -c ssh -t c`
SSH MAC	`lshmcencr -c sshmac -t c`
Cipher that are used for the HMC graphical user interface and REST API	`lshmcencr -c webui -t c`

Use the following commands to monitor various console and serviceable events information for uses in the HMC:

Table 28. Commands to view the logged on users and console or serviceable events information in the HMC

Information	Command
GUI users	`lslogon –r webui –u`
GUI tasks	`lslogon –r webui –t`
CLI users	`lslogon –r ssh –u`
CLI tasks	`lslogon –r ssh –t`
Operations on HMC	`lssvcevents -t console -d <number of days>`
Operations on System	`lssvcevents –t hardware –m <managed system> -d <number of days>`

Centralized monitoring events for the HMC: If you have many Hardware Management Consoles, set the `rsyslog` file to collect all the usage data.

How does IBM fix the HMC security vulnerabilities?

IBM has a security incidence response process named IBM Product Security Incident Response Team (PSIRT). The IBM Product Security Incident Response Team (PSIRT) is a global team that manages the receipt, investigation and internal coordination of security vulnerability information related to IBM offerings. Open Source and IBM components that are shipped with the HMC are actively monitored and analyzed. Interim fixes and security fixes are provided by IBM for all supported releases of the HMC.

How to track new interim fixes on the HMC?

The security bulletin contains information about the vulnerability and interim fixes for supported HMC versions. To track interim fixes on the HMC, you can:

- Search the latest security bulletins at IBM Security Bulletin.
- Follow @IBMPowereSupp on Twitter for notifications.
- Subscribe to email notifications at IBM Support.

Security profiles: Global Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI-DSS)

Learn about how the Hardware Management Console (HMC) handles the privacy information of the users.

The Hardware Management Console (HMC) is a closed appliance that does not store any cardholder data. Hence, only a subset of requirements and security assessment procedures of IT security that are defined by PCI-DSS are applicable for the HMC. Only trusted code that is distributed by IBM can be installed on the HMC. When any vulnerability is known through the IBM PSIRT process, interim fixes are published. The requirements and recommendations include the following items:

GDPR queries

Table 29. GDPR queries . The table provides information about the questions related to GDPR.

Questions	Answers
What kind of data is stored in the HMC?	HMC stores configuration information of Power hardware, PowerVM virtualization, and the performance metrics information.
Does the HMC process any personal data?	You can provide contact information for the call home function. Providing contact information for the call home function is optional.
Which predefined accounts are used for system administration of the HMC?	The system administrator user uses the *hscroot* username.
Do any of the accounts in the HMC relate to a specific person?	No.
Is it mandatory to provide personal data in the HMC?	No. You do not need to provide personal data information. However, providing this information is optional.
Does the HMC log file have any personal data information?	No.
Is it possible to delete personal data completely and permanently?	Yes. Unconfigure the call home function.

PCI-DSS queries

Table 30. PCI-DSS queries . The table provides information about the questions related to PCI-DSS

Questions	Answers
How to install and maintain a firewall configuration to protect the data of the cardholder?	The HMC does not store or access any cardholder data. However, the HMC has a firewall configuration and the user can control and enable specific ports.
Can I use vendor-supplied default value for system passwords and other security parameters?	Before you install a system on the network, change all the predefined passwords of the *hscroot* user.
How does the HMC protect the stored data of the cardholder?	The HMC does not store or access any cardholder data.
How does the HMC encrypt the data of the cardholder when the data is transmitted across open public networks?	The HMC does not store or access any cardholder data.

Table 30. PCI-DSS queries . The table provides information about the questions related to PCI-DSS *(continued)*

Questions	Answers
How to use and regularly update anti-virus software programs?	The HMC is a closed appliance. Therefore, malware cannot infect the HMC.
How to develop and maintain secure systems and applications?	You must install the required patches to your system manually from the IBM Fix Central website. Only trusted code that are distributed by IBM can be installed on the HMC.
Does the HMC restrict access to the cardholder data?	The HMC does not store or access any cardholder data.
How to assign a unique ID to each person who has access to the computer?	You can implement this requirement by ensuring that there are no shared IDs and by following the password policies.
How to restrict the physical access to the data of the cardholder?	The HMC does not store or access any cardholder data
How to track and monitor the access to network resources and to the cardholder data?	The HMC does not store or access any cardholder data.
How does the HMC test the security of the system and processes?	Scan tools are used to run security scans on all the released versions of the HMC. The scan tools include: *Qualys*, *Nessus*, *testssl*, *sslscan* and *ASoC*.
How to maintain a security policy that includes information security for employees and contractors?	System administrator disables the remote user login, activates the user login on a need basis, and deactivates the user login when the access is no longer required.

Managing the HTTPS ciphers of the HMC web interface by using the HMC

You can manage the HyperText Transfer Protocol Secure (HTTPS) ciphers by using the Hardware Management Console (HMC) for secure communication.

By default, HMC supports Transport Layer Security (TLS) and HTTPS communication with secure cipher sets that are bundled with the HMC. Ciphers that are used in the default mode have strong encryption. These ciphers are used for secure communication on ports 443, 17443, 2301, 5250 proxy, and for internal communication within the HMC. For more information about encryption ciphers that are used by the HMC, you can run the **`lshmcencr`** command in the HMC command-line interface (CLI). If the corporate standards of your organization require the use of an alternative set of ciphers, you must run the **`chhmcencr`** command to modify the encryption ciphers.

HMC supports both self-signed and CA-signed certificates for encryption. With the HMC Version 10.2.1040.0, or later, you can select the key size of the certificate when you are generating the certificate signing request (CSR). The following values are allowed for the key size of the certificate: 2048, 3072, and 4096. If you are using CA-signed certificates, make sure that you are using a minimum of 2048-bit RSA encryption. By default, HMC uses a self-signed certificate, which has SHA256 algorithm with 2048-bit RSA encryption.

Note: By default, 2048-bit RSA encryption is used if you do not specify any value for the key size of the certificate.

Generating a certificate for the HMC

This certificate is used for the HMC graphical user interface and REST API through the port 443.

- You can run the following commands to generate a self-signed certificate in the HMC:

```
chhmccert -o apply -t self -i
org=IBM,org_unit=HMC,country=US,state=Texas,locality=Austin,days_to_expire=30,email=<email_id>
,key_size=2048
```

```
mkhmccert -t self -i
"org=TEST,org_unit=HMC,country=<country>,state=<state>,locality=<locality>,email=<email_id>,da
ys_to_expire=365,ipaddrs=<ipaddr>,dns=<dns>,key_size=3072"
```

- You can run the following command to generate and save the CSR in the HMC:

```
hscroot@vhmccloudtst34:~> mkhmccert -t ca -f csr.crt -i
"org=TEST,org_unit=HMC,country=<counrty>,state=<state>,locality=<locality>,email=<email_id>,da
ys_to_expire=365,ipaddrs= <ipaddr>,dns=<dns>,common_name=<dns>, key_size=4096"
```

  Note: After you generate the CSR, you must send that CSR to your CA authority to receive a CA-signed certificate.

For more information about generating a certificate, see HMC Manual Reference Pages - CHHMCCERT

Configuring the HMC to retain the HMC in a functional state

Based on a security scan report or due to an organization requirement, you might want to modify the list of the supported ciphers for secure communication. These ciphers are common for legacy and NIST modes. Security scanners might report issues with weak ciphers that are detected. You can work with your security team or the scanner vendor to identify the list of specific ciphers that do not align with their requirements. After the list of weak ciphers is identified, remove the identified ciphers from the active cipher list in the HMC.

When you remove weak ciphers from the active ciphers list, some necessary ciphers might also be removed. If the necessary list of ciphers is not present in the HMC, you cannot run any HMC management tasks or commands in the CLI. Also, you cannot initialize the GUI. To retain the HMC in a functional state, you must complete the configuration of ciphers.

Transport Layer Security (TLS) and Secure Socket Layer (SSL) ciphers are used in various external and internal communications through different ports. The following ports are used as standard ports for external usage: 443, 2301, and 5250 proxy ports.

- You can run the following command to list all TLS and SSL ciphers that are configurable:

```
lshmcencr -c <the encryption configuration to list e.g:- webui [Web user interface encryption
ciphers]>  -t <the type of encryptions to list a [ available encryptions] or c [current
supported encryption(s)] >
```

- You can run the following command with an administrator privilege to view the list of available ciphers:

```
lshmcencr –c webui –t a
```

  The following example shows a sample output of available cipher sets on the HMC Version 10.1.1022.0:

```
"avail_encryptions=TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_
WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA
384,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_A
ES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA38
4,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WI
TH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_A
ES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WIT
H_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AE
S_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WI
TH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_EC
DH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_S
HA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SH
```

```
A,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TL
S_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
```

- You can run the following command to list ciphers that can be used in the HMC web user interface and REST API:

  ```
  lshmcencr –c webui –t c
  ```

  The following example shows a sample output of available ciphers:

  ```
  "curr_encryptions=TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE
  _DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_
  128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RS
  A_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_CBC_
  SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECD
  SA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM
  _SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE
  _ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_2
  56_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_E
  CDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_
  256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EC
  DH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM
  _SHA256,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WI
  TH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WIT
  H_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH
  _AES_256_GCM_SHA384,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256
  "
  ```

Note: The list of supported ciphers sets might be a subset of or equal to the list of the available cipher sets. Only the list of the supported cipher sets is configurable. The list of the available cipher sets is not configurable.

Modifying the ciphers that are used in secure communication

You can modify the ciphers that are used in secure communication. You can remove the ciphers that you are aware of, or you can add a cipher in case you accidentally removed a necessary cipher. To modify any ciphers, complete the following steps:

1. Run the following command to view the list of cipher sets that are supported which can be used in the secure communication:

   ```
   lshmcencr -c webui -t c
   ```

2. Run the following command to remove the weak ciphers that you are aware of, or that are mentioned in the scan reports, or that your organization policy does not recommend:

   ```
   chhmcencr -c webui -o r -e <single/multiple comma separated current supported encryption/
   ciphers which need to be removed> -r <reboot>
   ```

   Note: You might also want to remove a cipher in cases where the scan tool does not specify the algorithm but shows a generic message about a weak cipher. The following examples list a few samples of messages from the scan tool:

   -
     ```
     TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)
              TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
              TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ---> (Found in HMC)
              SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
     ```

     In this case, the server is using a common or default prime number as a parameter during the Diffie-Hellman key exchange. The use of common prime numbers does not impact all cipher suites that are used by TLS or SSL protocols since not every cipher suite incorporates the Diffie-Hellman algorithm.

   -
     ```
     TLS/SSL Server Supports the Use of Static Key Ciphers (ssl-static-key-ciphers)
              Ports 443 and 2301:
              TLS_RSA_WITH_AES_128_CBC_SHA
              TLS_RSA_WITH_AES_128_CBC_SHA256
              TLS_RSA_WITH_AES_128_GCM_SHA256
     ```

```
          TLS_RSA_WITH_AES_256_CBC_SHA
          TLS_RSA_WITH_AES_256_CBC_SHA256
          TLS_RSA_WITH_AES_256_GCM_SHA384
```

In this case, you must work with your security team or scanner vendor to identify the specific list of ciphers that do not align with their requirements. After the cipher list is identified, you can run the following command to remove ciphers from the active cipher list in the HMC:

```
chhmcencr -c webui -o r -e <Single or multiple comma separated Values> -r chhmcencr -c
webui -o r -e TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
```

3. Run the following command to add a cipher to the active cipher list if you accidentally removed any cipher:

   ```
   chhmcencr -c webui -o a -e <Single or multiple comma separated Values> -r
   ```

   Note: If you do not specify the **-r** option in the command, you will receive a prompt to confirm to restart the system. If you specify **1**, the operation completes by modifying the ciphers and restarting the HMC. If you specify **0**, modifications are not initiated.

4. Verify that the following ciphers are present in the active list of ciphers to properly start the HMC:

   - TLS_AES_256_GCM_SHA384
   - TLS_AES_128_GCM_SHA256
   - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA
   - TLS_RSA_WITH_AES_256_GCM_SHA384
   - TLS_RSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
   - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

5. Restart the HMC to apply changes.

Note: The enterprise baseboard management controller (eBMC) system with firmware level FW1050 requires TLS version 1.3 for managing the event notification mechanisms. Consequently, HMC version 10.3.1050.0 must support TLS version 1.3 ciphers to manage eBMC systems with firmware level FW1050.

Notices

This information was developed for products and services offered in the US.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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

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

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

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

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

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

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Accessibility features for IBM Power servers

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

Overview

The IBM Power servers include the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Power servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with ICT Accessibility 508 Standards and 255 Guidelines (https://www.access-board.gov/ict/) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power servers.

The IBM Power servers online product documentation in IBM Documentation is enabled for accessibility. For more information about IBM's commitment to accessibility, see the IBM accessibility website at IBM Accessibility (https://www.ibm.com/able/).

Keyboard navigation

This product uses standard navigation keys.

Interface information

The IBM Power servers user interfaces do not have content that flashes 2 - 55 times per second.

The IBM Power servers web user interface relies on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The IBM Power servers web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

The IBM Power servers include certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name and IP address for purposes of session management. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

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

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Red Hat®, JBoss®, OpenShift®, Fedora®, Hibernate®, Ansible®, CloudForms®, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following Class A statements apply to the IBM servers that contain the Power10 processor and its features unless designated as electromagnetic compatibility (EMC) Class B in the feature information.

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

The following Class A statements apply to the servers.

Canada Notice

CAN ICES-3 (A)/NMB-3(A)

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization 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 may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Germany Notice

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

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

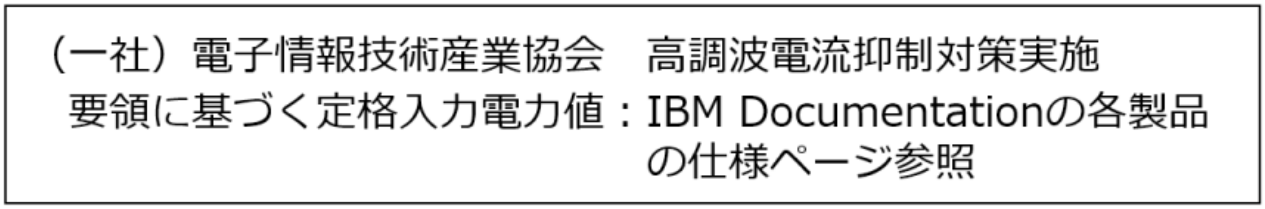
Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

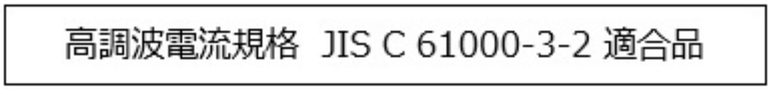
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Japan Electronics and Information Technology Industries Association (JEITA) Notice



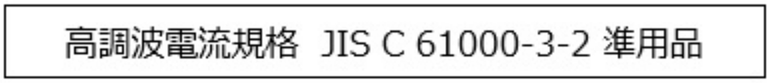
（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：IBM Documentationの各製品
の仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

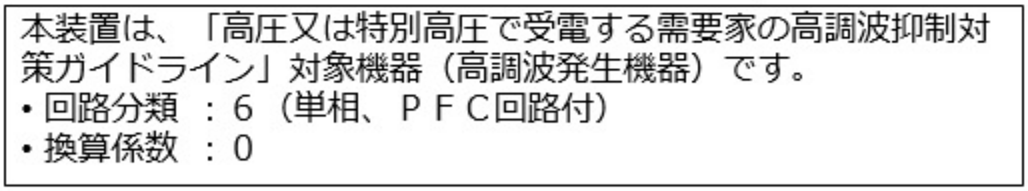


高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.



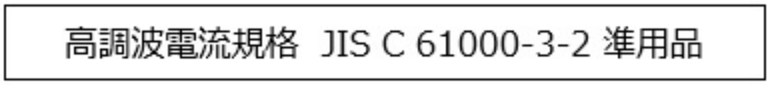
高調波電流規格 JIS C 61000-3-2 準用品



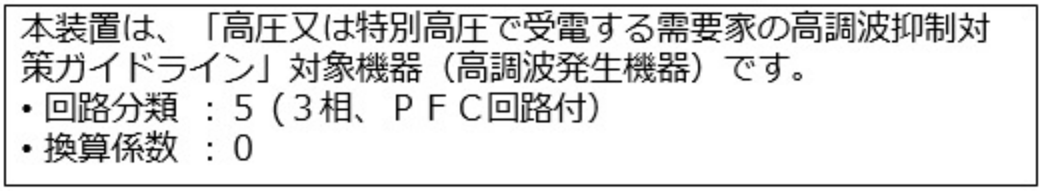
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 ：６（単相、ＰＦＣ回路付）
- 換算係数 ：０

This statement applies to products greater than 20 A per phase, three-phase.



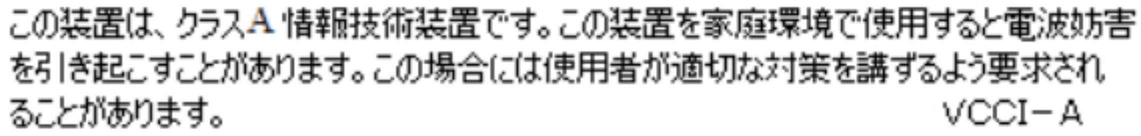
高調波電流規格 JIS C 61000-3-2 準用品



本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

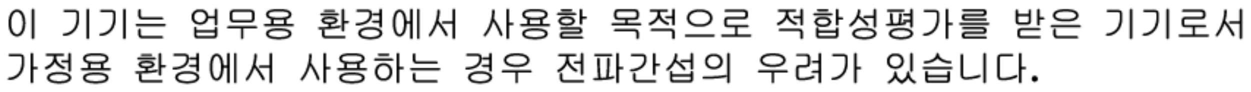
- 回路分類 ：５（３相、ＰＦＣ回路付）
- 換算係数 ：０

Japan Voluntary Control Council for Interference (VCCI) Notice



この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Korea Notice

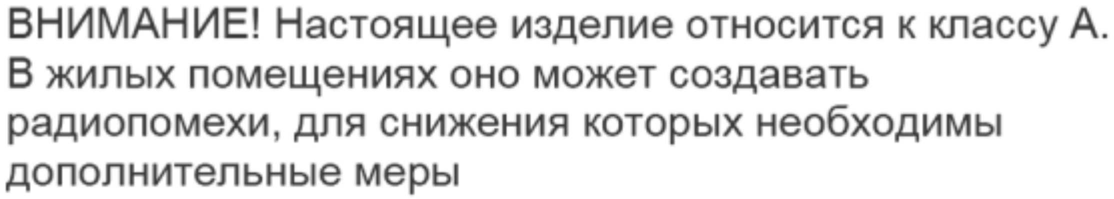


이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

People's Republic of China Notice

警告:在居住环境中,运行此设备可能会造成无线电干扰。

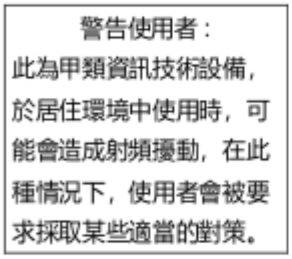
Russia Notice



ВНИМАНИЕ! Настоящее изделие относится к классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Taiwan Notice

CNS 13438:



警告使用者：
此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

CNS 15936:

警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。

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

United States Federal Communications Commission (FCC) Notice

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. Proper cables and connectors are available from IBM-authorized dealers. 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.

Responsible Party:
International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

United Kingdom Notice

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC) Class B in the feature installation information.

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Canada Notice

CAN ICES-3 (B)/NMB-3(B)

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization 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.

German Notice

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

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

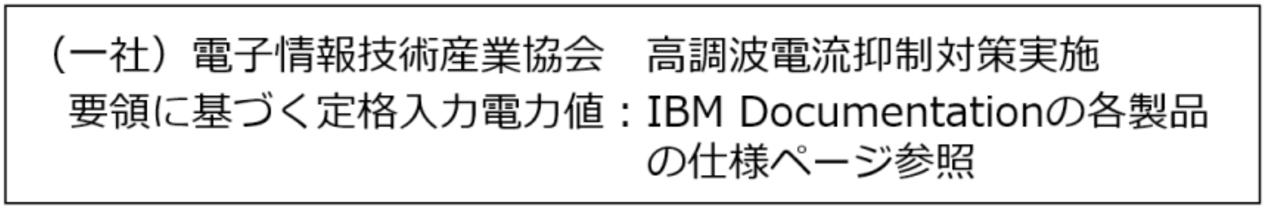
Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

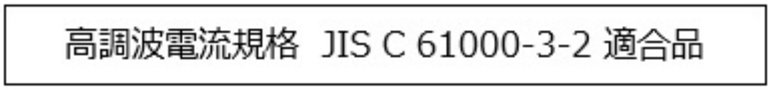
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B

Japan Electronics and Information Technology Industries Association (JEITA) Notice



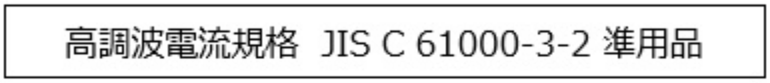
（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：IBM Documentationの各製品
の仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

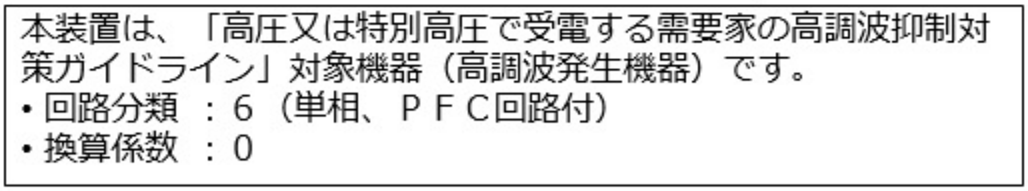


高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.



高調波電流規格 JIS C 61000-3-2 準用品



本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
- 回路分類 ：6（単相、ＰＦＣ回路付）
- 換算係数 ：0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
- 回路分類 ：５（３相、ＰＦＣ回路付）
- 換算係数 ：０

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は，クラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。 ＶＣＣＩ－Ｂ

Taiwan Notice

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

United States Federal Communications Commission (FCC) Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by 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.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

Terms and conditions

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

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

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

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

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

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

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

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