Power Systems

Managing OpenBMC-based systems

Note

Before using this information and the product it supports, read the information in “Notices” on page 29.

This edition applies to IBM® Power Systems servers that contain the POWER9™ processor and to all associated models.

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.

- 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 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 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)

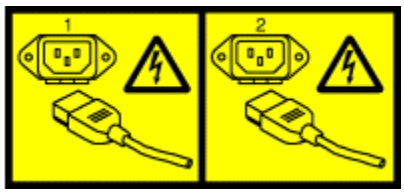
DANGER: Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices. In addition, do not lean on rack-mounted devices and do not use them to stabilize your body position (for example, when working from a ladder). Stability hazard:

- 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)

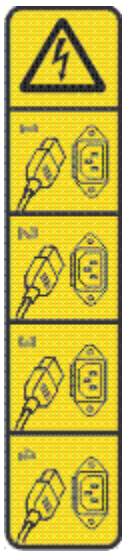
(L003)



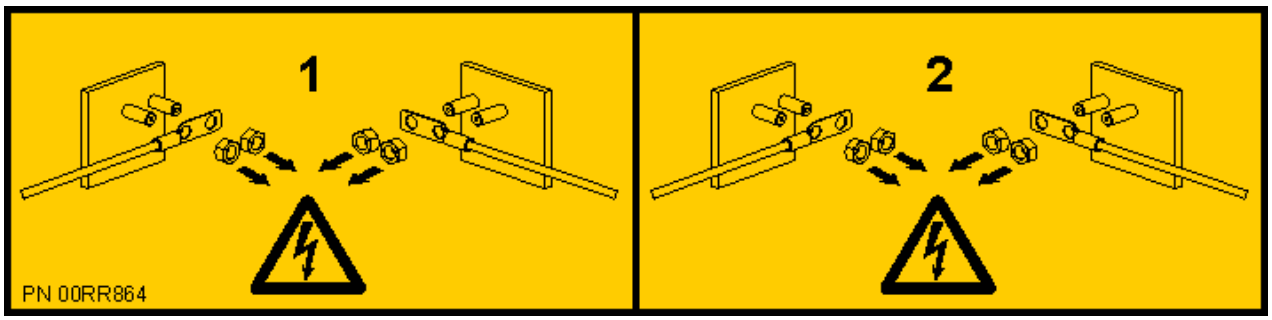
or

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)

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)

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

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

The equipment is suitable for installation in the following:

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

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

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

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

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

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

Managing OpenBMC-based systems

IBM Power Systems servers use a baseboard management controller (BMC) for system service management, monitoring, maintenance, and control. The BMC also provides access to the system event log files (SEL). The BMC is a specialized service processor that monitors the physical state of the system by using sensors. A system administrator or service representative can communicate with the BMC through an independent connection. The OpenBMC tool provides a communication method to the BMC, by using a command-line interface. The OpenBMC tool can be used either from a remote Linux® system, or from the host operating system console window. The OpenBMC tool can be connected remotely to the BMC by using a configured Ethernet port. You can connect your server to a monitor by using the VGA port at the rear of the server.

Managing the system by using the OpenBMC tool

Learn how to configure and manage your system by using the OpenBMC tool.

Downloading and installing the OpenBMC tool

Learn how to download and install the OpenBMC tool.

About this task

To download and install the OpenBMC tool, complete the following steps:

Procedure

1. Go to the IBM Support Portal.
2. In the search field, type: `Scale-out LC System Event Log Collection Tool`.
3. Click **Scale-out LC System Event Log Collection Tool**.
4. Follow the instructions to install and run the OpenBMC tool.

Basic commands and functionality of the OpenBMC tool

The OpenBMC tool provides support for working with system event logs, updating system firmware, identifying the system, powering off the system, and other service-related functions.

Before you begin

The following list gives examples of some basic commands that are supported by the OpenBMC tool:

OpenBMC tool top-level options

Learn more about the top-level options for the OpenBMC tool commands.

About this task

- `-H`: Host name or IP address of the BMC.
- `-U`: User name to log in with.
- `-A`: Provides a prompt to ask for the password.
- `-P`: Password for the user name.
- `-j`: Change output format to JSON.
- `-t`: Location of the policy table to use.
- `-T`: Provides time statistics for logging in, running the command, and logging out.

- -V: Displays current version of the OpenBMC tool.

System event log commands

Learn more about system event log commands for the OpenBMC tool.

Procedure

- To print a list of the system event logs in a readable format, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sel print
  ```

- To list the system event logs in raw data, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sel list
  ```

- To change the status of a system event log to resolved, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sel resolve -n x
  ```
  , where *x* is the system event log number.

- To collect all service data including system event logs, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  collect_service_data
  ```
  .

- To clear gard records for disable hardware, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  gardclear
  ```

- To clear the alert logs of entries, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sel clear
  ```

System firmware update command

Learn more about the system firmware update command.

Procedure

- To update the system firmware, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  firmware flash <bmc or pnor> -f xxx.tar
  ```
  , where *bmc* or *pnor* is the type of image you wish to flash to the system.

  Note: If you are not in the same folder as the TAR file, you must include the full path to the folder where the file resides.

- To activate a firmware image that is available in the BMC, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  firmware activate <firmware image ID>
  ```

System identify commands

Learn more about the system identify commands.

Procedure

- To activate the blue system identify LED, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis identify on
  ```

- To turn off the blue system identify LED, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis identify off
  ```

- To check the status of the blue system identify LED, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis identify status
  ```

System power on and power off commands

Learn more about the system power on and power off commands.

Procedure

- To check the power status of the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis power status
  ```

- To power on the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis power on
  ```

- To power off the system normally, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis power softoff
  ```

- To power off the system immediately, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  chassis power hardoff
  ```

System sensor commands

Learn more about the system sensor commands.

Procedure

- To display a list of all monitoring sensors, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sensors print
  ```

  or

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  sensors list
  ```

System FRU commands

Learn more about the system FRU commands.

Procedure

- To display a list of all inventory items, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  fru print
  ```

  or

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  fru list
  ```

- To display the known status of all FRU items, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  fru status
  ```

  Note: The FRU item must be designated as a replaceable FRU by the BMC.
- To automate the review of FRU status commands and to determine if there is a performance impact on the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  health_check
  ```

  Note: This command does not guarantee a healthy system as there can be system event logs entries that are not associated with the inventory items.

System BMC reset commands

Learn more about the system BMC reset commands.

Procedure

- To do a warm reset of the BMC remotely and without an AC cycle, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  bmc reset warm
  ```
- To do a cold reset of the BMC remotely and without an AC cycle, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  bmc reset cold
  ```

System dump commands

Learn more about the system dump commands.

Procedure

- To create a new dump file, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump create
  ```
- To list all dump files in the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump list
  ```
- To delete a specific dump file from the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump delete -n <dump file entry>
  ```
- To delete all dump files from the system, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump delete all
  ```
- To retrieve a specific dump file, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump retrieve -n <dump file entry>
  ```
- To retrieve a dump file and save it to specific directory, use the following command:

  ```
  openbmctool -U <username> -P <password> -H <BMC IP address or BMC host name>
  dump retrieve -s <location to save dump file>
  ```

Note: If you do not specify a location, the file is saved in the OS where the command is run in the temp directory.

Enabling and disabling local BMC user accounts

Learn more about the **local_users**commands.

About this task

The local user accounts on the BMC, such as root, can be disabled, queried, and re-enabled with the **local_users** sub-command.

Note: After disabling local users, the LDAP user needs to be available for further interaction with the BMC, including enabling local users by using OpenBMC tool.

Procedure

- To view current local user account status, use the following command:

  ```
  openbmctool <connection options> local_users queryenabled
  ```

- To disable all local user accounts, use the following command:

  ```
  openbmctool <connection options> local_users disableall
  ```

- To enable all local user accounts, use the following command:

  ```
  openbmctool <connection options> local_users enableall
  ```

Remote logging by using rsyslog

Learn more about the remote logging commands.

About this task

The BMC can stream out local logs (that go to the systemd journal) by using RSYSLOG. The BMC sends everything in the logs. Any kind of filtering and appropriate storage has to be managed on the rsyslog server.

Procedure

- To configure the rsyslog server for remote logging, use the following command:

  ```
  openbmctool <connection options> logging remote_logging_config -a <IP
  address> -p <port>
  ```

  Note: The IP address and port are for the remote rsyslog server. After the command is run, the remote rsyslog server starts to receive logs from the BMC.

- To disable remote logging, use the following command:

  ```
  openbmctool <connection options> logging remote_logging disable
  ```

  Note: Disable remote logging before you switch remote logging from an existing remote server to a new one.

- To view the remote logging configuration, use the following command:

  ```
  openbmctool <connection options> logging remote_logging view
  ```

  Note: This command prints out the IP address and port of the remote rsyslog server in JavaScript Object Notation (JSON) format.

- To turn REST API logging on, use the following command:

  ```
  openbmctool <connection options> logging rest_api on
  ```

- To turn REST API logging off, use the following command:

```
openbmctool <connection options> logging rest_api off
```

Note: REST API logging is turned off by default.

Certificate management

Learn more about the certificate management commands.

About this task

You can replace the existing certificate and private key file with another (possibly CA signed) certificate and private key file. You can install server, client, and root certificates.

Procedure

- To update the HTTPS server certificate, use the following command:

  ```
  openbmctool <connection options> certificate update server https -f <File>
  ```

  Note: The `<File>` is the privacy-enhanced mail (PEM) file that contains both the certificate and the private key.
- To update the LDAP client certificate, use the following command:

  ```
  openbmctool <connection options> certificate update client ldap -f <File>
  ```

  Note: The `<File>` is the PEM file that contains both the certificate and the private key.
- To update the LDAP root certificate, use the following command:

  ```
  openbmctool <connection options> certificate update authority ldap -f <File>
  ```

  Note: The `<File>` is the PEM file that contains only the certificate.
- To delete the HTTPS server certificate, use the following command:

  ```
  openbmctool <connection options> certificate delete server https
  ```

  Note: Deleting a certificate creates and installs a new self-signed certificate.
- To delete the LDAP client certificate, use the following command:

  ```
  openbmctool <connection options> certificate delete client ldap
  ```
- To delete the LDAP root certificate, use the following command:

  ```
  openbmctool <connection options> certificate delete authority ldap
  ```

  Note: Deleting the root certificate can cause an LDAP service outage.

LDAP configuration

Learn more about the LDAP configuration commands.

About this task

In the BMC, LDAP is used for remote authentication. The BMC does not support remote user-management functionality. The BMC supports both secure and non-secure LDAP configuration.

Procedure

- To create the LDAP configuration (non-secure), use the following command:

  ```
  openbmctool.py <connection options> ldap enable --uri="ldap://
  <ldap server IP/hostname>" --bindDN=<bindDN> --baseDN=<basDN> --
  bindPassword=<bindPassword> --scope="sub/one/base" --serverType="OpenLDAP/
  ActiveDirectory"
  ```

Note: Configuring a fully qualified domain name or hostname in the `uri` parameter requires the domain name system (DNS) server to be configured on the BMC.

- To create the LDAP configuration (secure), use the following command:

  ```
  openbmctool.py <connection options> ldap enable --uri="ldaps://
  <ldap server IP/hostname>" --bindDN=<bindDN> --baseDN=<basDN> --
  bindPassword=<bindPassword> --scope="sub/one/base" --serverType="OpenLDAP/
  ActiveDirectory"
  ```

  Notes:

  1. It is common to encounter the following error when you run the above `openbmctool.py` command string:

     xyz.openbmc_project.Common.Error.NoCACertificate

     This error means that the BMC client needs to verify that the LDAP server certificate is signed by a known certification authority (CA). An administrator needs to upload the CA certificate to the BMC to resolve this error.
  2. The OpenBMC tool does not support individual LDAP configuration property updates. To update a single property, the administrator must recreate the LDAP configuration with the changed values.

- To delete the LDAP configuration, use the following command:

  ```
  openbmctool.py <connection options> ldap disable
  ```

  Note: The root user must be enabled before you run the command, otherwise the BMC is not accessible. To enable all local user accounts, see Enabling and disabling local user accounts.

- To add privilege mapping use the following command:

  ```
  openbmctool.py <connection options> ldap privilege-mapper create --
  groupName=<groupName> --privilege="priv-admin/priv-user"
  ```

- To delete privilege mapping, use the following command:

  ```
  openbmctool.py <connection options> ldap privilege-mapper delete --
  groupName=<groupName>
  ```

- To list privilege mapping, use the following command:

  ```
  openbmctool.py <connection options> ldap privilege-mapper list
  ```

  The normal workflow for LDAP configuration is in the following order:

  1. Configure the DNS server.
  2. Configure LDAP.
     a. Configure the CA certificate for secure LDAP configuration.
     b. Create LDAP configuration with local user.
  3. Configure user privilege.

  Notes:

  1. If you login with LDAP credentials and have not added privilege mapping for the LDAP credentials, then you will get the following error message:

     403, 'LDAP group privilege mapping does not exist'.

     You can avoid this error by adding privilege mapping.
  2. The following error message might mean that user lacks sufficient privileges on the BMC:

     Insufficient privileges

     You can avoid this error by adding privilege mapping.
  3. After you setup the LDAP, the OpenBMC tool connection options work with both LDAP and local users.

Network configuration

Learn more about the network configuration commands.

Procedure

- To enable DHCP, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network enableDHCP -I
  <Interface name>
  ```

- To disable DHCP, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network disableDHCP -I
  <Interface name>
  ```

- To get the host name, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getHostName
  ```

- To set the host name, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network setHostName -H
  <host name>
  ```

- To get the domain name, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getDomainName
  -I <Interface name>
  ```

- To set the domain name, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network setDomainName
  -I <Interface name> -D DomainName1,DomainName2,..
  ```

- To get the media access control (MAC) address, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getMACAddress
  -I <Interface name>
  ```

- To set the MAC address, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network setMACAddress
  -I <Interface name> -MA xx:xx:xx:xx:xx
  ```

- To get the default gateway, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getDefaultGW
  ```

- To set the default gateway, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network setDefaultGW
  -GW <default gw>
  ```

- To view the current network configuration, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network view-config
  ```

- To get the network time protocol (NTP), use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getNTP -I
  <Interface name>
  ```

- To set the NTP, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network setNTP -I
  <Interface name> -N NTP1,NTP2,...
  ```

- To get the domain name system (DNS), use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getDNS -I
  <Interface name>
  ```

- To set the DNS, use the following command:

```
openbmctool.py -H <BMC_IP> -U root -P <root password> network setDNS -I
<Interface name> -d DNS1,DNS2,...
```

- To get the IP address, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network getIP -I
  <Interface name>
  ```

- To set the IP address, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network addIP -a
  <ADDRESS> \-gw <GATEWAY> -l <PREFIXLENGTH> -p <protocol type> -I <Interface
  name>
  ```

- To delete the IP address, use the following command:

  ```
  openbmctool.py -H <BMC_IP> -U root -P <root password> network rmIP -I
  <Interface name> -a <ADDRESS>
  ```

- To enable a virtual local area network (VLAN), use the following command:

  ```
  openbmctool.py <connection options> network addVLAN -I <Interface name> -n
  <IDENTIFIER>
  ```

- To disable a virtual local area network (VLAN), use the following command:

  ```
  openbmctool.py <connection options> network deleteVLAN -I <Interface name>
  ```

- To view the DHCP configuration properties, use the following command:

  ```
  openbmctool.py <connection options> network viewDHCPConfig
  ```

- To configure the DHCP properties, use the following command:

  ```
  openbmctool.py <connection options> network configureDHCP -d <DNSENABLED> -n
  <HOSTNAMEENABLED> -t <NTPENABLED> -s <SENDHOSTNAMEENABLED>
  ```

  Note: DNSENABLED, HOSTNAMEENABLED, NTPENABLED, and SENDHOSTNAMEENABLED are boolean values (true or false).

- To reset the network settings to the factory defaults, use the following command:

  ```
  openbmctool.py <connection options> network nwReset
  ```

  Note: Reset settings are applied after the rebooting of the BMC.

Managing the system by using the IPMI

Learn how to configure and manage your system by using the Intelligent Platform Management Interface (IPMI).

Common IPMI commands

You can use **IPMI** commands to perform various managing tasks for your system.

Table 1. Common IPMI commands

Command option	Description
`ipmitool -I lanplus -H myserver.example.com -P mypass chassis power on`	Powers on the server.
`ipmitool -I lanplus -H myserver.example.com -P mypass chassis power off`	Powers off the server.
`ipmitool -I lanplus -H myserver.example.com -P mypass chassis status`	Checks the server status.
`ipmitool -I lanplus -H myserver.example.com -P mypass chassis power cycle`	Power cycle the server.

Table 1. Common IPMI commands (continued)	
Command option	**Description**
`ipmitool -I lanplus -H myserver.example.com -P mypass sol activate`	Activates SOL system console.
`ipmitool -I lanplus -H myserver.example.com -P mypass sol deactivate`	Deactivates SOL system console.
`ipmitool -I lanplus -H myserver.example.com -P mypass sel list`	Returns an error log.
`ipmitool -I lanplus -H myserver.example.com -P mypass sdr list`	Lists status of all sensors.
`ipmitool -I lanplus -H myserver.example.com -P mypass sol set retry-interval value`	Sets the default retry-interval value in milliseconds.
`ipmitool -I lanplus -H myserver.example.com -P mypass fru print`	Prints the FRU information.
`ipmitool -I lanplus -H myserver.example.com -P mypass user list`	Lists the IPMI users.

Configuring the BMC IP address

Dynamic Host Configuration Protocol (DHCP) is the default network setup for the BMC in Power Systems LC servers. To enable your network connection, you must connect to your system and use the Petitboot bootloader interface to configure the IP address of the BMC. If you do not plan to use DHCP, you can also set up a static IP address.

Before you begin

The system has one shared and one dedicated BMC Ethernet port. The default BMC Ethernet port is the dedicated BMC Ethernet port. For more information about Ethernet port locations, see Installing the cable-management arm and connecting and routing power cables.

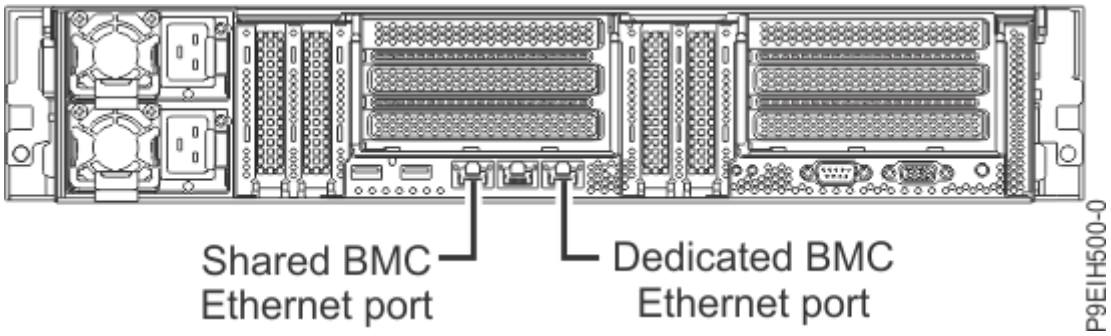


Figure 1. Dedicated and shared BMC Ethernet ports

Configuring the BMC IP address through the dedicated BMC Ethernet port

Before you begin

You must connect the network cable and a VGA monitor before you access the Petitboot bootloader interface.

If you encounter any problems in accessing the Petitboot bootloader interface, see Resolving a BMC access problem.

About this task

To use the Petitboot bootloader interface to set up or enable the network interface through the dedicated BMC Ethernet port, complete the following steps:

Procedure

1. Power on the server by pressing the power button on the front of the system. The system powers on to the Petitboot bootloader menu.

   Note: The boot process takes about 1 to 2 minutes to complete.

   When Petitboot loads, the monitor activates. Press any key to interrupt the boot process.
2. At the Petitboot bootloader main menu, select **Exit to Shell**.
3. Run the following command: `ipmitool lan print 2`. If this command returns an IP address, verify that is correct. To set a static IP address, follow these steps:

   Note: The `ipmitool lan print 2` command cannot display more than one IP address. To avoid this situation, you can set the static IP address to a different subnet from the default zero configuration networking IP address.

   a. Set the mode to static by running the following command: `ipmitool lan set 2 ipsrc static`.
   b. Set your IP address by running the following command: `ipmitool lan set 2 ipaddr ip_address`, where *ip_address* is the static IP address that you want to assign to this system.
   c. Set your netmask by running the following command: `ipmitool lan set 2 netmask netmask_address`, where *netmask_address* is the netmask for the system.
   d. Set your gateway server by running the following command: `ipmitool lan set 2 defgw ipaddr gateway_server`, where *gateway_server* is the gateway for this system.
   e. Confirm the IP address by running the following command: `ipmitool lan print 2`.

Configuring the BMC IP address through the shared BMC Ethernet port

Before you begin

You must connect the network cable and a VGA monitor before you access the Petitboot bootloader interface.

If you encounter any problems in accessing the Petitboot bootloader interface, see Resolving a BMC access problem.

About this task

To use the Petitboot bootloader interface to set up or enable the network interface through the shared BMC Ethernet port, complete the following steps:

Procedure

1. Power on the server by pressing the power button on the front of the system. The system powers on to the Petitboot bootloader menu.

   Note: The boot process takes about 1 to 2 minutes to complete.

   When Petitboot loads, the monitor activates. Press any key to interrupt the boot process.
2. At the Petitboot bootloader main menu, select **Exit to Shell**.
3. Run the following command: `ipmitool lan print 1`. If this command returns an IP address, verify that is correct. To set a static IP address, follow these steps:

Note: The `ipmitool lan print 1` command cannot display more than one IP address. To avoid this situation, you can set the static IP address to a different subnet from the default zero configuration networking IP address.

a. Set the mode to static by running the following command: `ipmitool lan set 1 ipsrc static`.
b. Set your IP address by running the following command: `ipmitool lan set 1 ipaddr ip_address`, where *ip_address* is the static IP address that you want to assign to this system.
c. Set your netmask by running the following command: `ipmitool lan set 1 netmask netmask_address`, where *netmask_address* is the netmask for the system.
d. Set your gateway server by running the following command: `ipmitool lan set 1 defgw ipaddr gateway_server`, where *gateway_server* is the gateway for this system.
e. Confirm the IP address by running the following command: `ipmitool lan print 1`.

Performing a factory reset

Learn how to perform a factory reset on the system.

The factory reset function can take up to 15 minutes to complete. When the LED on the power button starts flashing, the system is ready to start again. Perform the factory reset with the host powered off. If you perform the factory reset while the host is running, the system shuts down immediately and restarts the BMC. If the BMC is on a static network, you must manually power on the system with the physical power button.

To perform a factory reset, run the following command:

```
ipmitool -I lanplus -U <username> -P <password> -H <BMC_IP or Hostname> raw 0x3A 0x11
```

Note: The system does not send a validation response. The following system output is normal:

```
Unable to send RAW command (channel=0x0 netfn=0x3a lun=0x0 cmd=0x11)
```

If you forgot the password of the BMC, you can run the following command while the host is running to perform a factory reset and to restore the default password:

```
ipmitool raw 0x3A 0x11
```

You must set up and configure the BMC IP address after performing the factory reset. For more information, see “Configuring the BMC IP address” on page 10.

Risks of using IPMI on IBM Power Systems and OpenPower Systems

Various risks that are associated with the Intelligent Platform Management Interface (IPMI) have been identified and documented in the information technology (IT) security community.

IBM Power Systems and OpenPower Systems provide IPMI access by default. A subset of these identified risks is applicable to IBM servers.

Note: Model 9080-M9S does not provide IPMI access by default.

Vulnerability Details

The IPMI service can become unresponsive after it receives and rejects multiple authentication attempts. You might receive a `insufficient resources for session` message if you use the IPMI immediately after the failed authentication attempts. This situation lasts for a few seconds and normal service is restored afterward.

Important: Repeated authentication failures can cause denial of service.

A list of common vulnerabilities and exposures (CVE) is listed in Table 2 on page 13.

Table 2. Common vulnerabilities and exposures	
CVE ID	**Description**
CVE-2013-4037	The Remote Authenticated Key-Exchange Protocol (RAKP), which is specified by the IPMI standard for authentication, has flaws. Although the system does not allow the use of null passwords, a hacker might reverse engineer the RAKP transactions to determine a password. The authentication process for IPMI requires the management controller to send a hash of the requested password of the user to the client before the client authenticates. This process is a key part of the IPMI specification. The password hash can be broken by using an offline brute force or dictionary attack.
CVE-2013-4031	IBM Power Systems and OpenPower Systems are preconfigured with one IPMI user account, which has the same default login name and password on all affected systems. If a malicious user gains access to the IPMI interface by using this preconfigured account, the user can power off or on, or restart the host server, and create or change user accounts possibly preventing legitimate users from accessing the system. On OpenPower Systems, the default IPMI user name is `root`. Additionally, if a user fails to change the default user name and password on each of the systems that is deployed, the user has the same login information for each of those systems.
CVE-2013-4786	The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the hash-based message authentication code (HMAC) from a RAKP message 2 response from a BMC.

Configuration options and best practices

- Change the preconfigured user name and password when the server is deployed. This action prevents unauthorized users from gaining access to the system through the preconfigured user account.
- If a user is not managing a server by using the IPMI, you can configure the system to disallow IPMI network access from the user accounts. This task can be accomplished by using the IPMItool utility or a similar utility for managing and configuring the IPMI management controllers. You can use the following IPMItool command to disable the network access for an IPMI user:

  ```
  ipmitool channel setaccess 1 #user_slot# privilege=15
  ```

  Note: Replace #user_slot# in the command with the actual slot number (1 - 12) and repeat for each configured user.

  This example shows the command when it is run directly on the server. If the IPMItool command is run remotely over the network, or if a different utility is used, the command might be different. See the documentation for the utility that you are using to determine the correct command syntax. Disallowing IPMI network access removes the ability to use the weakness that is present in the IPMI RAKP protocol to discover user account credentials.
- Use strong passwords that are at least 16 characters long with a mixture of upper and lowercase letters, numbers, and special characters. By using more complex passwords, it makes it more difficult for malicious users to discover valid user credentials.
- Keep the management network separate from the public network. Keeping the management network separate lessens security exposures by reducing the number of individuals who can access the systems.

Managing the system by using the OpenBMC GUI

Learn how to manage and configure your system by using the OpenBMC GUI.

Logging on to the OpenBMC GUI

Learn how to log on to the OpenBMC GUI.

To log on to the OpenBMC GUI, complete the following steps:

1. Open a supported web browser. In the address bar, enter the IP address of the BMC that you want to connect to. For example, you can use the format `https://<BMC IP>` in the address bar of the web browser.
2. From the **OpenBMC logon** window, enter the **Host** address of the BMC and the **Username** and **Password** that is assigned to you.

   Note: The default user ID is `root` and the default password is `0penBmc`.

   If you are using firmware level OP940.01, or later, the root password is expired by default. You must change the default password before you can access the BMC. For more information about changing the expired default password, see "Setting the password" on page 14.

   If you forgot your password, you can perform a factory reset of the system to restore the default password. To reset the system, see "Performing a factory reset" on page 12.
3. Click **Log in**.

Setting the password

Learn how to change and set the password for your **root** account and to help secure the system.

Improved BMC password policy

The baseboard management controller (BMC) **root** password must be set on first use for newly manufactured systems or after performing a factory reset of the system. This policy change helps to enforce that the BMC is not left in a state with a well-known password.

In firmware level OP940.01, and later, the root password is expired and must be changed before you can access the functions of the BMC. However, if you are upgrading the firmware level from a previous OpenBMC firmware level or if you are performing an operational installation, you do not have to change the password.

The default user ID is `root` and the default password is `0penBmc`. You can use the web application, the Redfish REST APIs, or the OpenBMC tool command to change the password. After changing the password, you can access the BMC with your usual interface. To change the password, you must first access the account with the correct credentials, and then use the password change function. If you attempt to access the BMC with an expired password, you must change the password before accessing other functions.

- To change your expired password by using the web interface, enter `https://<BMC_IP>` into a web browser and then enter the access credentials of the BMC. The web interface prompts you to enter a new password.
- To change your expired password through a network interface, you can use Redfish APIs. For instructions, see "Managing the system by using DMTF Redfish APIs" on page 23.
- To change your expired password by using the OpenBMC tool, run the `openbmctool set_password` subcommand. For example,

```
openbmctool.py -H <BMC IP address or BMC host name> -U <username> -P <password> set_password
-p <new password>
Attempting login...
200
User root has been logged out
```

Where 200 is the response status that indicates success.

Note: The system might take up to 5 minutes to update the new password on the BMC. If you have trouble accessing your account, wait for 5 minutes and try again.

Also, with firmware level OP940.01, the BMC factory reset function resets the BMC password back to its default value and causes the default password to expire. This function means that after you perform the factory reset, you must change the password before you can access the BMC (even if you upgraded from an older firmware level).

To increase account security of the system, the administrator must complete the following steps:

1. Set a strong password for the root account. Strong passwords have at least 15 characters and include nonalphabetic characters. Initially, the password must not exceed 20 characters. Passwords can be changed later to a length greater than 20 characters, but IPMI access will be removed. Avoid using the **root** account, as the **root** account has more access to the BMC than an **Administrator** account. The root account can present a security risk if it is used incorrectly or maliciously. Use the root account only when it is required.
2. Create a separate account for each entity to manage the system. For example, you can create an **Administrator** account for yourself and for xCat, and create an **Operator** account for your staff. You can use the web interface or Redfish APIs to create a new account. When you create a new account, carefully consider which privilege role to assign to the user. Always use the least privilege role that is required.
   - To create a new account by using the web interface, see “Local users” on page 21.
   - To create a new account by using the Redfish APIs, see “Managing the system by using DMTF Redfish APIs” on page 23.

   If your BMC is using Lightweight Directory Access Protocol (LDAP), you can add users to the LDAP server.
3. Log off from the root account and switch to your personal **Administrator** account.

To increase the security of the system, the administrator can optionally configure access to the LDAP server. For more information, see “Basic commands and functionality of the OpenBMC tool ” on page 1.

Dashboard

The dashboard displays the overall information about the server and the BMC.

The following options are available on the title bar (located in the top portion of the dashboard):

- **Server information**: Displays the server name and BMC IP address.
- **Server health**: Displays the status of the server.
- **Server power**: Displays whether the server is powered on, powered off, or in an error state.
- **Date last refreshed**: Displays the date and time that the information was last refreshed. The time zone of the user is determined by the web browser.
- **Refresh**: Click **Refresh** to refresh the information.

The following menus are available from the menu pod (located in the left portion of the dashboard):

- **Server overview**
- **Server health**
- **Server control**
- **Server configuration**
- **Users**

Server overview

Learn about the options that are available from the **Server overview** task.

From the **Server overview** window, you can choose from any of the following available options:

- **Server information**: Displays the model, manufacturer, firmware version, and serial number of the server.
- **BMC information**: Displays the host name, BMC IP address, firmware version, and MAC address of the BMC.
- **Power information**: Displays the power consumption and power cap.
- **High priority events**: View any high priority events. Click **Refresh** to reload the information that is displayed here.
- **BMC time**: Displays the BMC time in the time zone of the user, which is determined by the web browser.
- **Turn on server LED**: Turn on or turn off the server LED.
- **Launch serial over LAN console**: Launches the Serial over LAN (SoL) console.
- **Edit network settings**: Edit the network settings.

Server health

Learn about the tasks that are available from the **Server health** menu.

From this menu, you can choose from any of the following available tasks:

Event log

View all events from the BMC.

Note: For descriptions and service actions for FQPSPxxxxxxx event codes, see Managing BMC-based systems by using the HMC (http://www.ibm.com/support/knowledgecenter/POWER9/p9ia7/p9ia7_kickoff.htm).

You can view and filter event log files from the BMC. From the **Event log** window, you can perform the following actions:

- Search through event logs by entering keywords and clicking **Search**.
- Filter the event logs by severity (**All**, **High**, **Medium**, or **Low**). You can select multiple severity levels.
- Filter the event logs by date range.
- Filter the event logs by event status (**All events**, **Resolved events**, and **Unresolved events**).
- Click any of the events that are listed to expand the event log file for more information. You can click **Copy** to copy the information to the clipboard.
- Select multiple event logs by clicking the checkbox next to event log. After you select the event logs, you can delete the logs by clicking **Delete** and then clicking **Yes** in the confirmation message. You can also mark event logs as read by clicking **Mark as resolved**.

Hardware status

View the hardware status and associated events of all hardware in the server.

You can view the hardware status of various hardware components in your server. Click any of the hardware components to expand the view for more information. You can search for specific hardware components by using the **Filter Hardware Components** search feature and then clicking **Filter**. You can also export the data by clicking **Export**.

Sensors

View all sensors that are present in the system.

You can view and filter sensors from the BMC. From the **Sensors** window, you can perform the following actions:

- Search and filter for specific sensors by using the **Search** feature and then clicking **Filter**.
- Filter sensors by severity (**All**, **Critical**, **Warning**, or **Normal**).
- Export the sensor data by clicking **Export**.

Server control

Learn about the tasks that are available from the **Server control** menu.

From this menu, you can choose from any of the following available tasks:

Server power operations

Learn how to view current server status and select power operations.

To update the **Host OS boot settings**, complete the following steps:

1. Select the boot setting override type from the **Boot setting override** menu.
2. You can optionally select **Enable one time boot**.
3. Select whether to enable or disable the TPM policy by selecting **On** or **Off**.
4. Click **Save**.

To restart the server, complete the following steps:

1. Select the type of reboot from **Operations** > **Reboot server**:
   - Orderly: Operating system shuts down first and then the server reboots.
   - Immediate: Server reboots without the operating system shutting down. This might cause data corruption.
2. Click **Reboot**.

To shutdown the server, complete the following steps:

1. Select the type of shutdown from **Operations** > **Shutdown server**:
   - Orderly: Operating system shuts down first and then the server reboots.
   - Immediate: Server reboots without the operating system shutting down. This might cause data corruption.
2. Click **Shutdown**.

Manage power usage

Learn how to view the power consumption of the server and set a power cap.

To set a power cap, complete the following steps:

1. From the **Server power cap setting** section, set the **power cap** to **On**.
2. Specify the number of watts to keep the server power consumption at or below the specified value.
3. Click **Save settings**.

You can turn off the power cap by setting the **power cap** to **Off** and clicking **Save settings**.

Server LED

Learn how to turn on and turn off the server light-emitting diode (LED).

You can turn on or turn off the server LED by clicking the toggle switch to either **On** or **Off**.

Note: If the server has a liquid crystal display (LCD), you can use this control to display text (**On**) or not to display text (**Off**) on the LCD.

Reboot BMC

Learn how to restart the BMC and view the current BMC boot status.

Click **Reboot BMC** to restart the BMC.

Note: When you restart the BMC, your web browser looses connection with the BMC for several minutes. When the BMC is back online, you must log in again. If the **Log in** button is not available after you restart the BMC, close your web browser. Then, reopen the web browser and enter your BMC IP address.

Serial over LAN console

Learn how to view information over the serial port of the server.

You can launch the Serial over LAN (SoL) console that displays the output of the serial port of the server.

KVM

Learn how to launch the remote keyboard, video, and mouse (KVM) console.

You can launch the KVM console from this task and interact with the remote system.

Virtual media

Learn how to start a session by using a virtual media device.

To start a session, complete the following steps:

1. Under **Virtual media device**, click **Choose file**.
2. Select the file and click **Open**.
3. Click **Start** to start the session.

Server configuration

Learn about the tasks that are available from the **Server configuration** menu.

From this menu, you can choose from any of the following available tasks:

Network settings

Learn how to view and set common network, IPv4, and DNS settings.

To view network settings, select the **Network Interface** that you want to view. The **Hostname**, **MAC Address**, and **Default Gateway** are displayed under **Common settings**. The **DHCP setting**, **IPv4 IP addresses**, **Gateways**, and **Netmasks** are displayed under **IPv4 Settings**. Under **DNS settings**, all DNS servers are displayed.

To set network settings, complete the following steps:

1. Select the **Network Interface** that you want to set.
2. Edit the **Hostname**, **MAC Address**, or **Default Gateway** fields under **Common settings**.
3. Edit the **DHCP setting**, **IPv4 IP address**, **Gateway**, and **Netmask Prefix Length** under **IPv4 Settings**.
4. Click **Save Settings**.

Note: You can edit network settings only on firmware level OP920.01 or later.

To add an IPv4 address, complete the following steps:

1. Click **Add IPV4 address**.
2. Complete the **IPv4 IP address**, **Gateway**, and **Netmask Prefix Length** fields.

3. Click **Save Settings**.

To add a DNS address, complete the following steps:

1. Click **Add DNS Server**.
2. Enter the Internet Protocol (IP) address of the **DNS Server**.
3. Click **Save Settings**.

SNMP settings

Learn how to view and set the simple network management protocol (SNMP) with a hostname or Internet Protocol (IP) address and a port.

To set the SNMP, complete the following steps:

Note: Only SNMPv2 is supported.

1. Click **Add Manager**.
2. Enter the hostname or IP address and the port number.
3. Click **Save Settings**.

You can remove a manager by clicking the trash bin icon next to the manager that you want to remove.

Firmware

Learn how to manage the BMC and server firmware.

You can use the **BMC images** and **Server images** tables to manage firmware image files. The image file that is listed at the top, the image with the highest boot priority, is used the next time that the device is booted. You can change the boot order for the image file by clicking the arrow icons.

Learn about the different image states that are available:

- **Functional**: The running image on the device.
- **Active**: The image is available to boot from, but is not currently the running image. If the image is the top image in the relevant table, it becomes the functional image the next time the device is rebooted.
- **Activating**: The image is in the process of being activated and becomes either **Active** or **Failed**.
- **Failed**: The image failed to activate.
- **Ready**: The image is ready to be activated.
- **Invalid**: This image is an invalid image and cannot be activated.

The system firmware is a combination of the BMC firmware and the PNOR firmware. You must update both the BMC firmware and the PNOR firmware for the system to operate properly. If you update only one type of firmware, but do not update the other type of firmware, system errors might occur.

You can upload an image file from the workstation or from the Trivial File Transfer Protocol (TFTP) server. If you choose **Upload image file from workstation**, click **Choose a file** and specify the location of the image on the workstation storage device. Click **Upload** to upload the image file to the BMC server. If you choose **Download image file from TFTP server**, enter the TFTP server IP address in the **TFTP Server IP Address** field and the file name in the **File Name** field. Click **Download** to download the image file to the BMC server.

After you load the new image file to the BMC server, you can activate the image file to make it available for use. Locate the image in the correct image table, and then click **Activate** > **Continue**. For a BMC image, an option of **Activate Firmware File Without Rebooting BMC** or **Activate Firmware File and Automatically Reboot BMC** is available. If you select **Activate Firmware File Without Rebooting BMC**, the BMC must be rebooted by using the **Reboot BMC** option to make the image become the **Functional** image. If you select **Activate Firmware File and Automatically Reboot BMC**, the BMC automatically reboots after the image is activated and the new image becomes the **Functional** image.

For a server image, after the image is activated, the server must be rebooted (or powered on if the server is off) for the image to become active. The **Reboot** (or **Power on**) option can be accessed from the **Server power operations** menu.

Date and time settings

Learn how to set the date and time.

To automatically set the date and time, complete the following steps:

1. Select **Obtain automatically from a network time protocol (NTP) server**.
2. Click **Add new NTP server**.
3. Enter the NTP server address.
4. Click **Save setttings**.

To manually add the date and time, complete the following steps:

1. Select **Manually set date and time**.
2. Enter the date and time.
3. Change the **Time owner** to the following values:
   - **BMC**: the BMC owns the time and can set the time.
   - **Host**: the host owns the time and can set the time.
   - **Split**: the BMC and the host own separate time.
   - **Both**: both the BMC and the host can set the time.

Access control

Learn about the tasks that are available from the **Access control** menu.

From this menu, you can choose from any of the following available tasks:

LDAP

Learn how to configure lightweight directory access protocol (LDAP) settings and manage role groups.

LDAP authentication

To enable LDAP authentication, complete the following steps:

1. Select the **Enable LDAP authentication** checkbox.

   Note: If you want to secure LDAP by using Secure Sockets Layer (SSL), select the **Secure LDAP using SSL** checkbox. You must have a certificate authority (CA) and LDAP certificate for this function.
2. Select the service type as **Open LDAP** or **Active directory**.
3. Complete the required fields.
4. Click **Save**.

Role groups

To add a new role group, complete the following steps:

1. Click **Add role group**.
2. Enter a name for the role group.
3. Set the privilege of the role group to **Administrator**, **Operator**, **User**, or **Callback**.
4. Click **Save**.

To remove a new role group, complete the following steps:

1. Select the checkbox next to the role group or groups that you want to remove from the table.
2. Click **Remove role groups**.
3. Click **Remove** in the pop-up window.

To modify the privilege of a role group, complete the following steps:

Note: LDAP authentication must be enabled to modify group roles.

1. Select the checkbox next to the role group or groups that you want to modify from the table.
2. Click the **Edit** icon.
3. Change the privilege of the role group to **Administrator**, **Operator**, **User**, or **Callback**.
4. Click **Save**.

Local users

Learn how to add or remove new users, modify user settings, manage user account policy settings, and view privilege role descriptions.

To add a new user, complete the following steps:

1. Click **Add user**.
2. Set the account status to either **Enabled** or **Disabled**.
3. Enter a new username.

   Note: The username cannot start with a number. No special characters are allowed except for an underscore.
4. Set the privilege of the user to **Administrator**, **Operator**, **ReadOnly**, or **NoAccess (Callback)**.
5. Enter the password of the user.

   Note: Initially, the password must be in the range of 8 - 20 characters in length. Passwords can be changed later to a length greater than 20 characters, but IPMI access is removed. The system might take up to 5 minutes for the new password to update on the BMC. If you have trouble accessing your account, wait for 5 minutes and try again.
6. Reenter the password for confirmation.
7. Click **Add user**.

To remove a user, complete the following steps:

1. Click the checkbox next to the user or users that you want to remove from the table.
2. Click **Remove**.
3. Click **Remove** again in the pop-up window.

You can modify user settings by selecting the user from the table and clicking the edit icon. From the **Modify user** window, you can update the following properties:

- Account status: set to **Enabled** or **Disabled**.
- Username: change the name of the user.
- Privilege: change the account privileges of the user to **Administrator**, **Operator**, **ReadOnly**, or **NoAccess (Callback)**.
- User password: update the password of the user.

You can modify user account policy settings by clicking **Account policy settings**. From the **Account policy settings** window, you can update the following properties:

- Maximum failed login attempts: change the number of allowed failed login attempts.
- User unlock method: set to **Automatic after timeout** or **manual**.
- Only non-root accounts can be locked out.

You can view privilege role descriptions by clicking **View privilege role descriptions**.

Table 3. Privilege role descriptions		
Role	**Privileges**	**Guidance**
Administrator	Can configure the BMC and manage users and sessions. Operational control over BMC functions.	Use this role for the most trusted users.
Operator	Operational control over BMC functions.	Use this role for users who manage routine operations.
ReadOnly	Read-only access to BMC functions.	Use this role for users who need to monitor the BMC, but do not need to operate it.
NoAccess (Callback)	No access to BMC functions.	Use this role for users who do not need access to the web interface or REST APIs.

SSL certificates

Learn how to generate a certificate signing request (CSR), add new certificates, and replace existing certificates.

Generating a CSR

To generate a new CSR, complete the following steps:

1. Click **Generate CSR**.
2. Complete the required fields under the **General** section.
3. Under **Private key** > **Key Pair Algorithm**, select the algorithm as **EC** or **RSA**.
4. Click **Generate CSR**.

Certificates

To add a new certificate, complete the following steps:

1. Click **Add new certificate**.
2. Select the certificate type as **HTTPS Certificate**, **LDAP Certificate**, or **CA Certificate**.
3. Click **Choose file** to select the certificate.
4. Click **Open**.
5. Click **Save**.

To replace certificates, complete the following steps:

1. Select the certificate that you want to replace from the table.
2. Click the refresh icon.
3. Click **Choose file** to select the new certificate.
4. Click **Open**.
5. Click **Replace**.

Managing the system by using DMTF Redfish APIs

OpenBMC-based systems can be managed by using the DMTF Redfish APIs.

Overview

Redfish is a REST API used for platform management and is standardized by the Distributed Management Task Force, Inc. (http://www.dmtf.org/standards/redfish).

Redfish enables platform management tasks to be controlled by client scripts that are developed by using secure and modern programming paradigms.

The Redfish API enables provisioning of tunable parameters for better utilization of power.

IBM OpenBMC-based systems support DMTF Redfish API (DSP0266, version 1.7.0, published on 20 May 2019) for systems management.

A copy of the Redfish schema files that are in JSON format are published by DMTF (http://redfish.dmtf.org/schemas/v1/) and are packaged in the firmware image.

The schema files that are distributed in the chip enable proper functioning of the APIs in deployments that have no wide area network (WAN) connectivity.

Note: The Redfish API is enabled by default and the Redfish service cannot be enabled or disabled by the user.

Firmware levels

Redfish APIs are supported on OpenPOWER (OP) firmware level OP940, or later.

Communication prerequisites for Redfish on OpenBMC-based servers

Depending on the current firmware level and network deployment, complete the following prerequisite tasks:

- Upgrade the server firmware level to OP940, or later.
- Identify the IP address of the BMC.
- Install and run cURL (https://curl.haxx.se/) with the method, Uniform Resource Indicator (URI), and the request body as parameters to communicate with the Redfish service.
- Install Python on the client system (typically a Linux host).
- Optionally, install and run DMTF Redfishtool (https://github.com/DMTF/Redfishtool).

Interacting with the Redfish service

To interact with the Redfish service, complete the following steps.

1. Create an authenticated login session (POST method on the `/redfish/v1/SessionService/Sessions` resource).
2. Extract and save the following details:
   - Authentication token (found in the **X-Auth-Token** header of the response)
   - Session URI (found in the **Location** header of the response)
3. To read the properties of a resource, send a **GET** request with the **X-Auth-Token** header for the URI of the resource.
4. To set a property of a resource, send a **PATCH** request with the **X-Auth-Token** header for the URI of the resource, the property name, type, and value encoded as a JSON body.
5. Extract and parse the response from the Redfish service that contains the JSON body.

Redfish service home page URI

The Redfish service home page URI (also known as the service ROOT) can be accessed by retrieving the URI: `https://<ip:port>/redfish/v1`. The response to this URI is a high-level site map that enables a traversal of the Redfish service by using a hypermedia API paradigm.

Interpreting the data returned by the Redfish service

The format and structure of the data is defined in the schema files. Schema files are JSON files that describe the data that is sent by the Redfish service. You can use the schema files to understand the data that is sent by the Redfish service and to validate the response that is sent by the Redfish service.

Location of the schema files

DMTF publishes the schema files for the standard data that is used in Redfish.

The Redfish schema files in JSON format are hosted in the DMTF schema repository at http://redfish.dmtf.org/schemas/v1/

Supported schema files

The following schema files are supported for OpenBMC-based systems:

- Account
- AccountCollection
- AccountService
- Certificate
- CertificateCollection
- CertificateLocations
- CertificateService
- Chassis
- ChassisCollection
- ComputerSystem
- ComputerSystemCollection
- EthernetInterface
- EthernetInterfaceCollection
- LogEntry
- LogService
- LogServiceCollection
- Manager
- ManagerCollection
- ManagerNetworkProtocol
- Memory
- MemoryCollection
- Processor
- ProcessorCollection
- Role
- RoleCollection
- ServiceRoot
- Session

- SessionCollection
- SessionService
- SoftwareInventory
- SoftwareInventoryCollection
- ThermalPower
- UpdateService

Accessing the common system management functions on the Redfish service by using cURL command

The following examples show the client URL (cURL) commands that can be used to access the common functions that are supported by the OpenBMC Redfish APIs:

Note: In all cURL commands, *${BMC}* is the IP address of the BMC.

- To view major collections, run the following commands:
  - Chassis collection:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Chassis
    ```

  - Manager collection:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Managers
    ```

  - System collection:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Systems
    ```

- To view the chassis, manager, and system resources, run the following commands:
  - Chassis resource:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Chassis/chassis
    ```

  - Manager resource:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Managers/bmc
    ```

  - System resource:

    ```
    curl -u root:0penBmc -k -s  https://${BMC}/redfish/v1/Systems/system
    ```

- To perform host power control operations, run the following commands:
  - Host power on:

    ```
    -X POST https://${BMC}/redfish/v1/Systems/system/Actions/ComputerSystem.Reset -d
    '{"ResetType": "On"}'
    ```

  - Host soft power off:

    ```
    -X POST https://${BMC}/redfish/v1/Systems/system/Actions/ComputerSystem.Reset -d
    '{"ResetType": "GracefulShutdown"}'
    ```

  - Host hard power off:

    ```
    -X POST https://${BMC}/redfish/v1/Systems/system/Actions/ComputerSystem.Reset -d
    '{"ResetType": "ForceOff"}'
    ```

  - Restart host:

```
-X POST https://${BMC}/redfish/v1/Systems/system/Actions/ComputerSystem.Reset -d
'{"ResetType": "GracefulRestart"}'
```

- To view the host power control resource, run the following command:

```
curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Systems/system/Actions/
```

- To view the log resource, run the following command:

```
curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Systems/system/LogServices/EventLog/
Entries
```

- To view sensor resources, run the following commands:
  - Power® resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/chassis/Power
    ```

  - Thermal resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/chassis/Thermal
    ```

  - Sensor resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/chassis/Sensors
    ```

- To view inventory resources, run the following commands:
  - Memory resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Systems/system/Memory
    ```

  - Processor resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Systems/system/Processors
    ```

  - Power supply 0 resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/powersupply0
    ```

  - Power supply 1 resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/powersupply1
    ```

  - Motherboard resource:

    ```
    curl -u root:0penBmc -k -s https://${BMC}/redfish/v1/Chassis/motherboard
    ```

- To update the firmware, run the following commands:
  - By using an image file from your system:

    ```
    curl -u root:0penBmc -curl k -s  -H "Content-Type: application/octet-stream" -X POST -T
    <image file path> https://${BMC}/redfish/v1/UpdateService
    ```

  - By using a Trivial File Transfer Protocol (TFTP) server:

    ```
    curl -u root:0penBmc -k -s -d '{"ImageURI":"<TFTP IP Address>/<File name on
    TFTP server>","TransferProtocol":"TFTP"}' -X POST https://${BMC}/redfish/v1/UpdateService/
    Actions/UpdateService.SimpleUpdate
    ```

- To create a new local account, run the following command:

  ```
  curl -X POST https://${BMC}/redfish/v1/AccountService/Accounts/ -d '{"UserName": "admin",
  "Password": "NEWPASSWORD", "RoleId": "Administrator"}'
  ```

Where `admin` is the name of the user that you want to create, `NEWPASSWORD` is the new password, and `RoleId` maps to the privilege role.

- To change the account password, run the following command:

  ```
  curl -X POST https://${BMC}/redfish/v1/AccountService/Accounts/root -d '{"Password":
  "NEWPASSWORD"}'
  ```

  Where `root` is the account name or user ID and `NEWPASSWORD` is the new password.

For more information about selecting a username, password, or role, see “Local users” on page 21.

Managing the system by using the HMC

Learn how to manage and configure your system by using the Hardware Management Console (HMC).

Note: You can manage the following OpenBMC-based and BMC-based systems by using the HMC:

- 8335-GTH
- 8335-GTX
- 9006-12P
- 9006-22P

To use the HMC to manage your supported system, see Managing BMC-based systems by using the HMC (http://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_bmc_kickoff.htm).

Notices

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

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

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

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

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

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

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

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

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

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

Accessibility features for IBM Power Systems servers

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

Overview

The IBM Power Systems servers include the following major accessibility features:

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

The IBM Power Systems servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content

Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power Systems servers.

The IBM Power Systems servers online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Keyboard navigation

This product uses standard navigation keys.

Interface information

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

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

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

Vendor software

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

Related accessibility information

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

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

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

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en/ in the section entitled "Cookies, Web Beacons and Other Technologies".

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.

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

Electronic emission notices

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER9 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.

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： Knowledge Center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

声 明

此为A级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Russia Notice

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Taiwan Notice

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。

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

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.

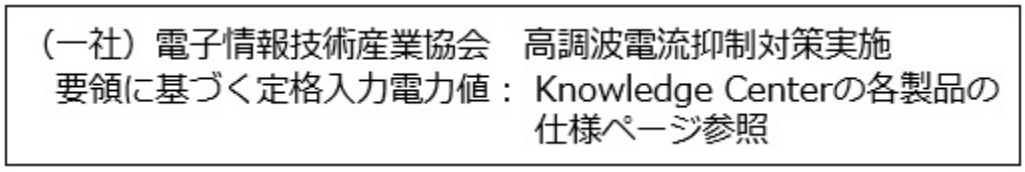
Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

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



This statement applies to products less than or equal to 20 A per phase.

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.