Power Systems

Managing the Advanced System Management Interface

IBM

Note

Before using this information and the product it supports, read the information in "Safety notices" on page v, "Notices" on page 77, the *IBM Systems Safety Notices* manual, G229-9054, and the *IBM Environmental Notices and User Guide*, Z125–5823.

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.

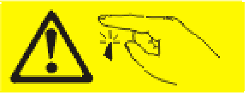
DANGER: When working on or around the system, observe the following precautions:

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.

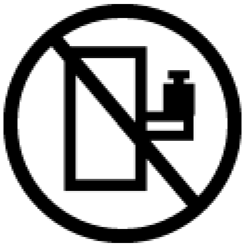
  - Ensure that there are little-to-no empty U-levels between devices installed in the rack cabinet below the 32U level, unless the received configuration specifically allowed it.
- If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.
- If 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)



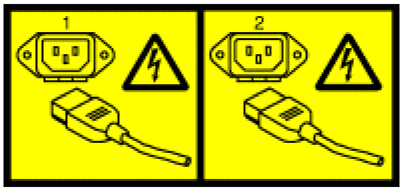
⚠ **DANGER:** Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices. In addition, do not lean on rack-mounted devices and do not use them to stabilize your body position (for example, when working from a ladder). Stability hazard:

- The rack may tip over causing serious personal injury.
- Before extending the rack to the installation position, read the installation instructions.

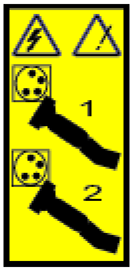
- Do not put any load on the slide-rail mounted equipment mounted in the installation position.
- Do not leave the slide-rail mounted equipment in the installation position.

(L002)

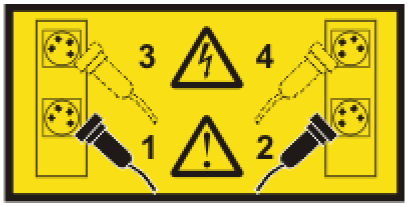
(L003)



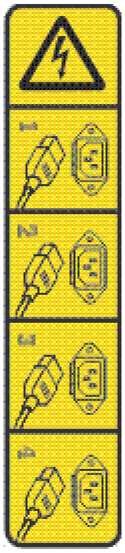
or



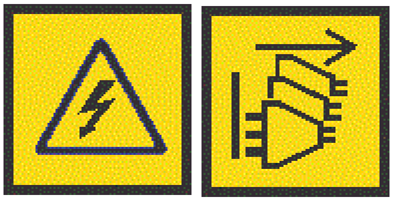
or

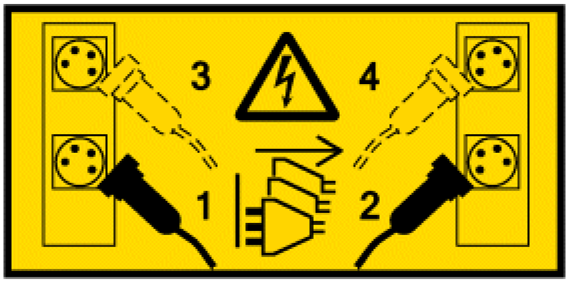


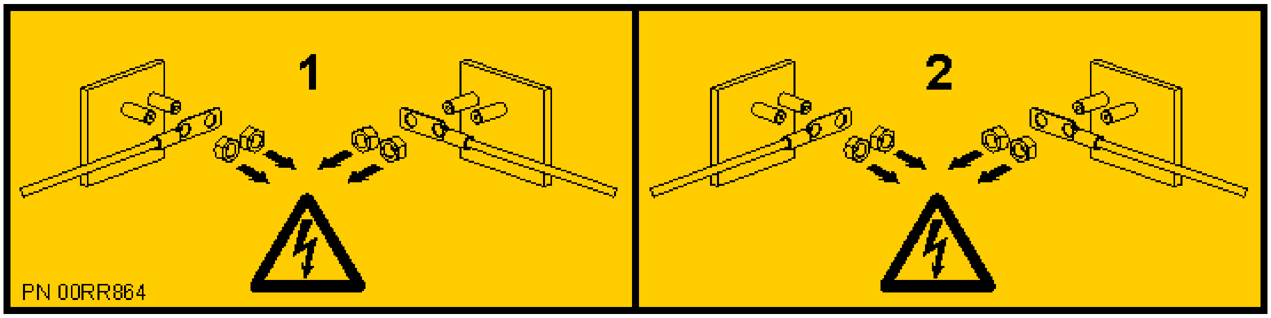
or



or





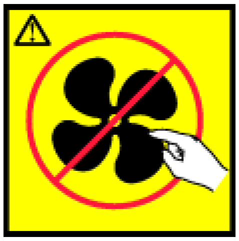


DANGER: Multiple power cords. The product might be equipped with multiple AC power cords or multiple DC power cables. To remove all hazardous voltages, disconnect all power cords and power cables. (L003)

(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 the Advanced System Management Interface

Advanced System Management Interface (ASMI) is a graphical interface that is part of the service processor firmware. The ASMI manages and communicates with the service processor. The ASMI is required to set up the service processor and to perform service tasks, such as reading service processor error logs, reading vital product data, and controlling the system power.

The ASMI might also be referred to as the service processor menus.

Note: JAWS screen reader version 16.0 or later might not work correctly when using certain versions of Microsoft Internet Explorer (including version 11.0). If you experience any difficulties when using JAWS while accessing the AMSI, use Mozilla Firefox (for example, version ESR 31.5.0) instead.

What's new in Managing the ASMI

Read about new or significantly changed information in Managing the Advanced System Management Interface (ASMI) since the previous update of this topic collection.

November 2020

- Updated the following topic:
  - "Protecting your 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22H, 9223-22S, 9223-42H, and 9223-42S servers against "Spectre" and "Meltdown"" on page 2
- Added the following topic to include information about the secure storage policy:
  - "Secure storage policy" on page 51

May 2020

- Updated the following topic:
  - "Protecting your 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22H, 9223-22S, 9223-42H, and 9223-42S servers against "Spectre" and "Meltdown"" on page 2

November 2019

- Updated the following topic:
  - " Validating cables in the 9080-M9S system" on page 72
- Added the following topics:
  - "Validating FSP, UPIC, and SMP cables in the 9080-M9S system at the FSP standby state " on page 73
  - "Validating UPIC cables in the 9080-M9S system with the system power turned on " on page 73
  - "Displaying the status of FSP, UPIC, and SMP cables in the 9080-M9S system " on page 74

March 2019

- Updated the following topics for setting the IP address:
  - "Setting the IP address in Windows XP and Windows 2000" on page 9
  - "Setting the IP address in Windows Vista" on page 10

- “Setting the IP address in Windows 7” on page 10

August 2018

- Added the following new topics:
  - “ Validating cables in the 9080-M9S system” on page 72
  - “ Speculative execution control” on page 35

Setting up and accessing the ASMI

Depending on your configuration, you can access the Advanced System Management Interface (ASMI) through a web browser, an ASCII terminal, or the Hardware Management Console (HMC).

If your system is managed by an HMC, you can access the ASMI through the HMC.

If your system is not managed by an HMC you must connect the server to a terminal or PC and apply power. You can power the system on and off using the power button on the control panel (operator panel) or the ASMI.

Protecting your POWER9 servers against “Spectre” and “Meltdown”

Resources are available to protect your system from "Spectre" and "Meltdown" vulnerabilities.

Protecting your 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22H, 9223-22S, 9223-42H, and 9223-42S servers against “Spectre” and “Meltdown”

Protect your 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22H, 9223-22S, 9223-42H, and 9223-42S servers from “Spectre” and “Meltdown” vulnerabilities.

Introduction

Three security vulnerabilities that allow unauthorized users to bypass the hardware barrier between applications and kernel memory are available public. These vulnerabilities use speculative execution to execute side-channel information disclosure attacks.

The first two vulnerabilities, CVE-2017-5753 and CVE-2017- 5715 (collectively known as Spectre) allow user-level code to infer data from unauthorized memory.

The third vulnerability, CVE-2017-5754 (known as Meltdown), allows user-level code to infer the contents of kernel memory. The vulnerabilities are all variants of the same class of attacks but differ in the way that speculative execution might be used.

While these vulnerabilities do not allow an external unauthorized party to gain access to a machine, they might allow a party with access to a system to access unauthorized data.

Since the customer-specific operating environments, including system (including use of Power® Hypervisor) application, and operating systems are varied, POWER9 systems (5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22H, 9223-22S, 9223-42H, and 9223-42S) provide the option for customers to control speculative execution at a system level, to meet their individual security standards.

Options for speculative execution control on 9008-22L, 9009-22A, 9009-41A, 9009-42A, 9223-22H, and 9223-42H systems are as follows.

1. Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks
2. Speculative execution controls to mitigate user-to-kernel side-channel attacks
3. Speculative execution fully enabled

Options for speculative execution control on 5105-22E, 9009-22G, 9009-41G, 9009-42G, 9223-42S, and 9223-22S systems are as follows.

1. Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks
2. Speculative execution fully enabled

Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks

This mode is designed for systems that need to mitigate exposures of the hypervisor, operating systems, and user application data to untrusted code. For the 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-22S and 9223-42S models this mode is set as the default.

Speculative execution controls to mitigate user-to-kernel side-channel attacks

This mode is designed for systems that need to mitigate against the threat of lower privileged code accessing operating system secrets as described in CVE-2017-5753, CVE-2017- 5715, and CVE-2017-5754. For the 9223-22H, 9223-42H models this mode is set as the default.

Note: Enabling this option can expose any user-accessible data in the system to CVE-2017-5753, CVE-2017- 5715, and CVE-2017-5754. This includes any partitions that are migrated (using Live Partition Mobility) to this system.

Speculative execution fully enabled

This optional mode is designed for systems where the hypervisor, operating system, and applications can be fully trusted.

Note: Enabling this option could expose the system to CVE-2017-5753, CVE-2017- 5715, and CVE-2017-5754. This includes any partitions that are migrated (by using Live Partition Mobility) to this system.

Accessing speculative execution control options

Speculative execution control options can be accessed using the Advanced Systems Management Interface (ASMI) menu under **System Configuration > Speculative Execution Control**. This setting can be changed when the system is in powered off state.

Protecting your 9040-MR9, 9080-M9S servers against “Spectre” and “Meltdown”

Protect your 9040-MR9, 9080-M9S servers from “Spectre” and “Meltdown” vulnerabilities.

Introduction

Four security vulnerabilities that allow unauthorized users to bypass the hardware barrier between applications and kernel memory were made public earlier this year. These vulnerabilities make use of speculative execution to perform side-channel information disclosure attacks.

The first three vulnerabilities, CVE-2017-5753 and CVE-2017- 5715 (collectively known as Spectre) and CVE-2018-3639 (known as Speculative Store Bypass) allow user or kernel-level code to infer data from unauthorized memory.

The fourth vulnerability, CVE-2017-5754 (known as Meltdown), allows user-level code to infer the contents of kernel memory.

The vulnerabilities are all variants of the same class of attacks but differ in the way that speculative execution could be exploited.

While these vulnerabilities do not allow an external unauthorized party to gain access to a machine, they could allow a party with access to a system to access unauthorized data.

Since the customer-specific operating environments, including system (including use of hypervisors) application, and operating systems are varied, POWER9 systems (9040-MR9, 9080-M9S) provide the option for customers to control speculative execution at a system level, to meet their individual security standards.

Options for speculative execution control on 9040-MR9, 9080-M9S systems are as follows.

1. Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks
2. Speculative execution fully enabled

Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks

This mode is designed for systems that need to mitigate exposures of the hypervisor, operating systems, and user application data to untrusted code. For the 9040-MR9, 9080-M9S models this mode is set as the default.

Speculative execution fully enabled

This optional mode is designed for systems where the hypervisor, operating system, and applications can be fully trusted.

Note: Enabling this option could expose the system to CVE-2017-5753, CVE-2017- 5715, and CVE-2017-5754. This includes any partitions that are migrated (by using Live Partition Mobility) to this system.

Accessing speculative execution control options

Speculative execution control options can be accessed using the Advanced Systems Management Interface (ASMI) menu under **System Configuration > Speculative Execution Control**. This setting can be changed when the system is in powered off state.

ASMI requirements

Learn about ASMI access and usage requirements.

To successfully access and use the ASMI, note the following requirements:

- The ASMI requires password authentication.
- The ASMI provides a Secure Sockets Layer (SSL) web connection to the service processor. To establish an SSL connection, open your browser using https://.
- Supported web browsers are Netscape (version 9.0.0.4), Microsoft Internet Explorer (version 7.0), Mozilla Firefox (version 2.0.0.11), and Opera (version 9.24). Later versions of these browsers might work but are not officially supported. The JavaScript language and cookies must be enabled.
- Clicking **Back** in the browser might display outdated data. To display the most up-to-date data, select the item you want from the navigation pane.
- The browser-based ASMI is available during all phases of the system operation, including initial program load (IPL) and run time. Some menu options are not available during the system IPL or run time to prevent usage or ownership conflicts if corresponding resources are in use during that phase.

  Note: The ASMI should not be used during the firmware installation process.
- The ASMI that is accessed on a terminal is available only if the system is at platform standby.
- All requested input must be provided in English-language characters regardless of the language selected to view the interface.

Related concepts

Setting up and accessing the ASMI
Depending on your configuration, you can access the Advanced System Management Interface (ASMI) through a web browser, an ASCII terminal, or the Hardware Management Console (HMC).

Accessing the ASMI by using the HMC

You can access the Advanced System Management Interface (ASMI) through the Hardware Management Console (HMC) interface.

About this task

To access the Advanced System Management Interface (ASMI) by using the HMC, complete the following steps:

Note: Only one active ASMI connection can be launched by using the HMC. To launch multiple ASMI connections, use the Secure Shell (SSH) tunnel.

Procedure

1. In the navigation pane, click **Resources** > **All Systems** to view all the systems that are associated with your Hardware Management Console (HMC).
2. Select the server that you want to work with.
3. Click **Actions** > **View all options** > **Launch Advanced Systems Management (ASM)**. The **Launch ASM Interface** window is displayed.
4. If the HMC of the system that you selected is configured to access the ASMI, the details of the system are displayed. Ensure that the details of the selected system and the IP address of the service processor associated with that system are correct. Then, click **OK**.

   The ASMI window is displayed.

Accessing the ASMI without an HMC

Find out how to access the Advanced System Management Interface (ASMI) with a Power Systems server that is not managed by an HMC.

Connecting your server to a PC or notebook

Connect your server to a PC or notebook to interface with the Advanced System Management Interface (ASMI).

The web interface to the ASMI is available during all phases of system operation including the initial program load (IPL) and run time.

Accessing the ASMI using a PC or notebook and web browser

If your system is not managed by a Hardware Management Console (HMC), you can connect a PC or notebook to the server to access the Advanced System Management Interface (ASMI). You need to configure the web browser address on the PC or notebook to match the manufacturing default address on the server.

About this task

The web interface to the ASMI is available during all phases of system operation including the initial program load (IPL) and run time. The ASMI is used to perform general and administrator-level service tasks. These tasks include reading service processor error logs, reading vital product data, setting up the service processor, and controlling the system power.

The following instructions apply to systems that are not connected to an HMC. If you are managing the server using an HMC, you can access the ASMI by using the HMC.

To set up the web browser for direct or remote access to the ASMI, complete the following tasks:

Procedure

1. If the server is not powered on, perform the following steps:
   a) Connect your power cord or cords to the server.
   b) Plug the power cord or cords into the power source.
   c) Wait for the control panel to display 01. A series of progress codes are shown before 01 appears.

      Notes:

      - The system is powered on if the light on the control panel is green.
      - To view the control panel, press the blue switch to the left, then pull out the control panel all the way, and then pull it down.

   Important: Do not connect an Ethernet cable to either the HMC1 port or the HMC2 port until you are directed to do so later in this procedure.
2. Select a PC or notebook that has Netscape 9.0.0.4, Microsoft Internet Explorer 7.0, Opera 9.24, or Mozilla Firefox 2.0.0.11 to connect to your server.

   Note: If the PC or notebook on which you are viewing this document does not have two Ethernet connections, another PC or notebook needs to be connected to your server to access the ASMI.

   If you do not plan to connect your server to your network, this PC or notebook is your ASMI console.

   If you plan to connect your server to your network, this PC or notebook temporarily connects directly to the server for setup purposes only. After setup, you can use any PC or notebook on your network that is running Netscape 9.0.0.4, Microsoft Internet Explorer 7.0, Opera 9.24, or Mozilla Firefox 2.0.0.11 as your ASMI console.

   Note: Complete the following steps to disable the TLS 1.0 option in Microsoft Internet Explorer to access the ASMI using Microsoft Internet Explorer 7.0 running on Windows XP:

   a. From the **Tools** menu in Microsoft Internet Explorer, select **Internet Options**.
   b. From the Internet Options window, click the **Advanced** tab.
   c. Clear the **Use TLS 1.0** check box (in the Security category) and click **OK**.
3. Connect an Ethernet cable from the PC or notebook to the Ethernet port labeled HMC1 on the back of the managed system. If HMC1 is occupied, connect an Ethernet cable from the PC or notebook to the Ethernet port labeled HMC2 on the rear of the managed system.

   Important: The service processor's Ethernet ports are configured for DHCP by default. If the service processor is attached to a live Ethernet network equipped with a DHCP server and the service processor is turned on, an IP address is assigned. The default IP address of the service processor is no longer valid. To restore the service processor default IP addresses, perform one of the following tasks:

   - Attach an ASCII terminal to the service processor using a serial cable. For details, see Accessing the ASMI using an ASCII terminal.
   - Set the Type of IP address to `Dynamic` using the ASMI. Ensure that the FSP is not connected to the live network. This action sets the FSP to the default IP address as shown in Table 1 on page 7 below.
4. Use Table 1 on page 7 to help you determine and record the information needed to set the IP address on the service processor on the PC or notebook. The Ethernet interface on the PC or notebook needs to be configured within the same subnet mask as the service processor so that they can communicate with each other. For example, if you connected your PC or notebook to HMC1, the IP address for your PC or notebook could be 169.254.2.140 and the subnet mask would be 255.255.255.0. Set the gateway IP address to the same IP address as the PC or notebook

Table 1. Network configuration information for the service processor in a POWER9 processor-based system

POWER9 processor-based systems	Server connector	Subnet mask	IP address of the service processor	Example of an IP address for your PC or notebook
Service processor A	HMC1	255.255.255.0	169.254.2.147	`169.254.2.140`
	HMC2	255.255.255.0	169.254.3.147	`169.254.3.140`

5. Set the IP address on your PC or notebook using the values from the table. For details, see "Setting the IP address on your PC or notebook" on page 9.
6. To access the ASMI using a web browser, complete the following steps:
   a) Use Table 1 on page 7 to determine the IP address of the service processor Ethernet port to which your PC or notebook is connected.
   b) Type the IP address in the **Address** field on the web browser of your PC or notebook and press enter. For example, if you connected your PC or notebook to HMC1, type `https://169.254.2.147` in the web browser on your PC or notebook.

   Note: It might take 2 - 5 minutes for the service processor to reach standby. The ASMI menus can be accessed with a web browser only after the service processor reaches standby. Function code 30 on the control panel cannot be used to view the service processor's IP addresses until the service processor reaches standby.
7. When the Login display appears, enter `admin` for the user ID and password.
8. Change the default password when prompted.
9. Choose from the following options:
   - If you plan to connect your service processor to your network, continue with step "10" on page 7.
   - If you do not plan to connect your service processor to your network, continue with step "14" on page 8.
10. If you plan to connect your service processor to your network, complete the following steps:
    a) From the navigation area, expand **Network Services**.
    b) Click **Network Configuration**.
    c) From the Network Configuration display, select **IPv4** or **IPv6**, and click **Continue**.
11. If you selected IPv4, use Table 2 on page 7, and if you selected IPv6, use Table 3 on page 8 to complete the appropriate fields.
    - If your PC or notebook is connected to HMC1, complete the section labeled Network interface eth0.
    - If your PC or notebook is connected to HMC2, complete the section labeled Network interface eth1.

    Ensure that the fields are completed correctly.

Table 2. Fields and values for IPv4 network configuration

Field	Value
Configure this interface?	Selected
IPv4	Leave enabled.
Type of IP address	**Link local** if configuring IP address 1, **Static** if configuring IP address 2 or 3.
Host name	Enter the name of the host system.
IP address	This is a set IP address obtained from the network administrator.

Table 2. Fields and values for IPv4 network configuration (continued)

Field	Value
Subnet mask	This is a set subnet mask obtained from the network administrator.
Default gateway	If configuring IP address 2 or 3, enter the default gateway address obtained from the network administrator.
Domain name	Enter the domain name obtained from the network administrator.
IP address of the first, second, or third Domain Name System (DNS)	Enter the IP address of the DNS obtained from the network administrator.

Table 3. Fields and values for IPv6 network configuration

Field	Value
Configure this interface?	Selected
IPv6	Leave enabled.
DHCP	The default value is enabled.
Auto-configured IP address	The default value is enabled.
Host name	Enter a new value.
Type of IP address	Static
IP address	This is a set IP address obtained from the network administrator. **Note:** To verify that you are using the correct IP address, perform a function 30 on the control panel to show the service processor IP address and port location.
Default gateway	If configuring IP address 2 or 3, enter the default gateway address obtained from the network administrator.
Domain name	Enter a new value.

12. Click **Continue**.
13. Click **Save Settings**.
14. Remove the cable from HMC1 to the PC or notebook. Attach an Ethernet cable to HMC1 that is connected to the network switch.
15. Go to the system on which the ASMI will be accessed. Open a browser window and access the ASMI to verify the network connection.
16. If you were sent here from another procedure, return to that procedure now.

Related concepts

ASMI authority levels
Several authority levels are available for accessing the service processor menus by using the ASMI.

Related tasks

Accessing the ASMI by using the HMC

You can access the Advanced System Management Interface (ASMI) through the Hardware Management Console (HMC) interface.

Changing the time of day
You can display and change the current date and time on your system. The time is stored as UTC (Coordinated Universal Time).

Configuring network interfaces
You can configure network interfaces on the system. The number and type of interfaces vary according to the specific needs of your system.

Setting the IP address on your PC or notebook

To access the ASMI through a Web browser, you first need to set the IP address on your PC or notebook. The following procedures describe setting the IP address on PC and notebooks running the Microsoft Windows XP, 2000, and Vista, and Linux operating systems.

Setting the IP address in Windows XP and Windows 2000
To set the IP address within Windows XP and Windows 2000, complete these steps.

Procedure

1. Click **Start** > **Control Panel**.
2. On the control panel, double-click **Network Connections**.
3. Right-click **Local Area Connection**.
4. Click **Properties**.
5. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.

   ⚠ **Attention:** Record the current settings before making any changes. This will allow you to restore these settings if you disconnect the PC or notebook after setting up the ASMI web interface.

   Note: If Internet Protocol (TCP/IP) does not appear in the list, complete the following steps:

   a. Click **Install**.
   b. Select **Protocol**, and then click **Add**.
   c. Select **Internet Protocol (TCP/IP)**.
   d. Click **OK** to return to the Local Area Connection Properties window.
6. Select **Use the Following IP Address**.
7. In the **IP address**, and **Subnet mask** fields, enter the values that are obtained in step “4” on page 6 from Accessing the ASMI using a Web Browser.
8. Click **OK** on the Local Area Connection Properties window. It is not necessary to restart your PC.

Setting the IP address in Linux
To set the IP address on Linux operating system, complete these steps.

About this task

During this procedure, you need the IP address and **Subnet mask** values obtained in step “4” on page 6 in Accessing the ASMI using a web Browser.

Procedure

1. Make sure that you are logged on as a root user.
2. Start a terminal session.
3. Type `ifconfig -a` at the command prompt.

⚠ **Attention:** Record or print the current settings and the eth1 or eth2 interfaces before making changes. This action allows you to restore these settings if you disconnect the PC or notebook after setting up the ASMI web interface.

4. Type `ifconfig ethx xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx`, where the *xxx.xxx.xxx.xxx* values are the values from step "4" on page 6 for IP address and Subnet mask.

   Replace `ethx` with the interface shown in step 3.
5. Press Enter.

Setting the IP address in Windows Vista
To set the IP address within Windows Vista, complete these steps.

Procedure

1. Click **Start** > **Control Panel**.
2. Ensure **Classic View** is selected.
3. Select **Network and Sharing Center**.
4. Select **View status** in the Public network area.
5. Click **Properties**.
6. If the security dialog appears, click **Continue**.
7. Highlight **Internet Protocol Version 4**.
8. Click **Properties**.
9. Select **Use the following IP address**.
10. In the **IP address**, and **Subnet mask** fields, enter the values that are obtained in step "4" on page 6 from Accessing the ASMI using a web Browser.
11. Click **OK** > **Close** > **Close**.

Setting the IP address in Windows 7
To set the IP address on the Windows 7 operating system, complete the following steps.

Procedure

1. Click **Start** > **Control Panel**.
2. Select **Network and Sharing Center**.
3. Click the network that is displayed in **Connections**.
4. Click **Properties**.
5. If the security dialog box is displayed, click **Continue**.
6. Highlight **Internet Protocol Version 4**.
7. Click **Properties**.
8. Select **Use the following IP address**.
9. In the **IP address**, and **Subnet mask** fields, enter the values that are obtained in step "4" on page 6 from the Accessing the ASMI by using a web browser topic.
10. Click **OK** > **Close** > **Close**.

Connecting a system running AIX or Linux to a terminal

You can connect a system that is running in AIX® or Linux environment to an ASCII terminal or a graphics terminal to communicate with the system management services (SMS) menus.
Related information

Starting system management services

Accessing the ASMI by using an ASCII terminal

The ASCII terminal is connected to the server through a serial link. The ASCII interface to the ASMI provides a subset of the web interface functions. The ASCII terminal is available only when the system is in the platform standby state. It is not available during the initial program load (IPL) or run time.

About this task

This connection also allows you to access the system management services. Use the system management services menus to view information about your system and to perform steps such as changing the boot list and setting the network installation parameters.

To set up the ASCII terminal for direct or remote access to the ASMI, complete the following steps:

Procedure

1. By using a serial cable that is equipped with a null modem, connect the ASCII terminal to system connector 1 (P1-T1, which is the default) or 2 (P1-T2) on the rear of the server.
2. Connect the power cord from the server to a power source.
3. Wait for the green light on the control panel to start flashing.
4. Ensure that your ASCII terminal is set to the following general attributes.

   These attributes are the default settings for the diagnostic programs. Be sure that your terminal is set according to these attributes before proceeding to the next step.

Table 4. Default settings for the diagnostic programs

General setup attributes	3151 /11/ 31/41 settings	3151 /51/ 61 settings	3161 /64 settings	Description
Line speed	19,200	19,200	19,200	Uses the 19,200 (bits per second) line speed to communicate with the system unit.
Word length (bits)	8	8	8	Selects 8 bits as a data word length (byte).
Parity	No	No	No	Does not add a parity bit and is used together with the word length attribute to form the 8–bit data word (byte).
Stop bit	1	1	1	Places a bit after a data word (byte).

5. Press a key on the ASCII terminal to allow the service processor to confirm the presence of the ASCII terminal.
6. When the login display appears for the ASMI, enter `admin` for the user ID and password.
7. Change the default password when you are prompted.

   You have completed the setup for an ASCII terminal, and have started the ASMI.
8. On the ASMI, change the time of day on the server.
9. Set the system boot mode to boot by using the power on/off system menus on the ASMI.
10. If an operating system is installed (for example, in the factory), the operating system now boots. If no operating system is installed, the system boots to system management services (SMS menus).

    Note: Use the SMS menus to view information about your system and to perform tasks, such as changing the boot list and setting the network installation parameters.
11. If the operating system is not installed, you can install the AIX operating system or the Linux operating system now.

Related concepts

ASMI authority levels
Several authority levels are available for accessing the service processor menus by using the ASMI.

Related tasks

Changing the time of day
You can display and change the current date and time on your system. The time is stored as UTC (Coordinated Universal Time).

Powering the system on and off
View and customize various initial program load (IPL) parameters.

Related information

Managing system management services

Accessing the graphics console

A graphics console can be used to manage your AIX or Linux servers Linux server, but it cannot be used to access the Advanced System Management Interface (ASMI). A graphics console can be used in text (ASCII) mode and as a graphical interface.

About this task

To set up and use the graphics console, complete the following steps:

Procedure

1. Locate the graphics adapter at the rear of the server.
2. Connect a standard monitor to the adapter to use the console and if you need, connect a keyboard and mouse to the USB ports.
3. Power on the console.
4. Connect the power cables for the server and wait for the green light on the operator panel to start flashing.
5. Press the white start button to start the server. If an operating system is installed (for example, at the factory), it boots. If no operating system is installed, the system boots to system management services (SMS menus).

   Note: Use the SMS menus to view information about your system and to perform tasks, such as changing the boot list and setting the network installation parameters.
6. If the operating system is not installed, you can install the AIX operating system or the Linux operating system now.

Related information

Managing system management services

Controlling the system power using the control panel

Learn how to start or stop a system using the control panel.

Starting a system that is not managed by an HMC

You can use the power button or the Advanced System Management Interface (ASMI) to start a system that is not managed by a Hardware Management Console (HMC).

Stopping a system that is not managed by an HMC

You might need to stop the system to complete another task. If your system is not managed by the Hardware Management Console (HMC), use these instructions to stop the system by using the power button or the Advanced System Management Interface (ASMI).

Before you begin

Before you stop the system, follow these steps:

1. Ensure that all jobs are completed and end all applications.
2. If a Virtual I/O Server (VIOS) logical partition is running, ensure that all clients are shut down or that the clients have access to their devices by using an alternative method.

Initiating a delayed power off

You can use the power button on the control panel to initiate the delayed power off (DPO) feature.

Before you begin

⚠ **Attention:** Using the power button on the control panel to power off the system might cause unpredictable results in the data files, and the next IPL will take longer to complete.

Some servers do not respond to the power-off sequence unless the system is in manual operating mode. If necessary, set the system operating mode to **manual** mode.

About this task

To initiate a DPO, complete the following steps:

Procedure

1. Press and hold the power button on the control panel for four seconds.

   After one second, a countdown time is displayed. The default countdown time is four seconds.
2. Continue to press and hold the power button until the countdown time reaches zero, and then release the power button.

   The DPO is initiated.

What to do next

To cancel the DPO before it starts, release the power button before the countdown reaches zero. If the power button is depressed for less than one second, no countdown time is displayed, and the power-off function is not initiated.

Related information

Putting the physical control panel in manual operating mode

Initiating a fast power off

You can use the power button on the control panel to initiate the fast power off (FPO) feature.

Before you begin

⚠ **Attention:** Using the power button on the control panel to power off the system might cause unpredictable results in the data files, and the next IPL will take longer to complete.

Some servers do not respond to the power-off sequence unless the system is in manual operating mode. If necessary, set the system to manual operating mode.

About this task

To initiate an FPO, complete the following steps:

Procedure

1. Press and hold the power button on the control panel for four seconds.

   After one second a countdown time is displayed. The default countdown time is four seconds.
2. Continue to press and hold the power button until the countdown time reaches zero and until after the delayed power off (DPO) is initiated.

   A new DPO-FPO separation count of 10 seconds is started. The separation count is used to distinguish a DPO from an FPO. During this interval, DPO progress codes are displayed, followed by the countdown time.
3. Continue to press and hold the power button for 10 seconds until the DPO-FPO separation count reaches zero, and then release the power button.

   When the FPO count expires, `A100800A` is displayed and the FPO is initiated. This action is equivalent to entering a function 08.

What to do next

If you release the power button during the DPO-FPO separation count, the FPO is canceled, and the DPO continues.

If you continue to press the power button after the DPO-FPO separation interval has expired, or if you press and hold the power button while a DPO is in progress, the FPO countdown begins again and `A1008009` is displayed.

Related information

Putting the physical control panel in manual operating mode

Controlling the system power using the ASMI

Use the Advanced System Management Interface (ASMI) to manually and automatically control the system power.

Powering the system on and off

View and customize various initial program load (IPL) parameters.

About this task

You can start and shut down the system in addition to setting IPL options.

To perform these operations, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Several IPL options that you can set pertain to the server firmware. Firmware is an integral part of the server that is stored in flash memory, whose contents are preserved when the system is powered off. The firmware is code that automatically starts when the server is turned on. Its main purpose is to bring the server to a state where it is ready to operate, which means the server is ready to install or boot an operating system. Firmware also enables the handling of exception conditions in the hardware and provides extensions to the functions of the server hardware platform. You can view the current firmware level of the server on the Advanced System Management Interface (ASMI) Welcome pane.

This server has a permanent firmware boot side, or P side, and a temporary firmware boot side, or T side. When updating the firmware, install new levels of firmware on the temporary side first to test the compatibility with your applications. When the new level of firmware has been approved, copy it to the permanent side.

To view and change IPL settings, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Power On/Off System**.
3. Set the boot settings as required.

   Note: In KVM mode, the following power on and power off options are not available:

   - AIX/Linux partition mode boot: Selects the boot type for an AIX/Linux partition. This option is enabled only when the system is not managed by a Hardware Management Console (HMC). Select from the following boot type options:
     - Continue to operating system: The partition boots to the operating system without stopping.
     - Boot to SMS menu: The partition stops at the System Management Services (SMS) menu.
     - Service mode boot from saved list: The system boots from the saved service mode boot list.

       Note: This option can be used to execute the diagnostics on a partition. The partition operating system must support diagnostic boot and the diagnostics must be loaded on the partition disk drive.
     - Service mode boot from default list: The system boots from the default boot list.

       Note: This option can be used to run the stand-alone diagnostics from a CD-ROM drive.
     - Boot to open firmware prompt: The system stops at the open firmware prompt.

       Notes:

       - For managed systems with the firmware at the level FW920 and FW930, Open Firmware OK prompt cannot be used if the partition setting for Secure Boot is enabled and enforced.
       - For managed systems with firmware at the level FW940, or later, the Open Firmware OK prompt is a restricted environment in which only certain commands are allowed. Type `macro_help` to see the list of commands that are supported.
   - i5/OS partition mode boot: Selects the i5/OS partition mode for next system boot. This option is available only when the system is not managed by the HMC.
   - Default partition environment

   Normal
   The service processor firmware runs diagnostic tests based on the state of the hardware. This is the default setting.

   Firmware boot side for next boot
   Select the side from which the firmware boots the next time: `permanent` or `temporary`. You can test firmware updates by booting from the temporary side before you copy the firmware updates to the permanent side.

   System operating mode
   Select the operating mode: `manual` or `normal`. Manual mode overrides various automatic power-on functions, such as auto-power restart, and enables the power button.

   AIX/Linux partition mode boot
   Select the stopping point during the boot process. This option is available only if the system is not managed by the HMC. **Service mode boot from saved list** is the preferred way to run online AIX diagnostics. **Service mode boot from default list** is the preferred way to run stand-alone AIX diagnostics.

This option is applicable only when the managed system is using the manufacturing default configuration, which is the initial partition setup as received from service and support. When the system is not using the manufacturing default configuration, any changes to this option do not take effect. However, when the system is using the manufacturing default configuration, you can change the setting for the next restart by changing this option.

Server firmware start policy

Select the starting state for the server firmware: **Standby (User-Initiated)**, **Running (Auto-Start Always)**, or **Auto-Start (Automatic Restarts Only)**. When the server is in the server firmware standby state, logical partitions can be set up and activated.

System power off policy

The system power off policy is a system parameter that controls the system's behavior when the last partition (or the only partition in the case of a system that is not managed by an HMC) is powered off. Select from following the system power off policies:

- **Automatic**: Allows the HMC to control when the power off occurs, when necessary, and ensures the shortest lapsed time.
- **Power off**: When the last partition powers off, the system powers off.
- **Stay on**: When the last partition powers off, the system remains powered up.

  Note: If the flash boot side is changed before the last partition is powered off, the system automatically reboots to complete the side-switch action.

Default partition environment

Select **Default** (valid only if the RB keyword is not S0), **AIX**, **IBM i**, or **Linux**.

Notes:

- If the default partition environment is changed from any other value to IBM i, the IBM i enable/disable setting is automatically changed to `Enabled`.
- If the default partition environment is changed from IBM i to any other value, the IBM i enable/disable setting is not affected.

4. Perform one of the following steps:

   - Click **Save settings** to save the selected options. The power state does not change.
   - Click **Save settings and power on/off**. All selected options are saved and the system turns on or off. The power-on option is available only if the system is powered off. The power-off option is available only if the system is powered on.

Related concepts

Programming vital product data
The Advanced System Management Interface (ASMI) enables you to program the system vital product data (VPD), such as system brand, system identifiers, and system enclosure type. To access any of the VPD-related panels, your authority level must be administrator or authorized service provider.

Related tasks

Setting the system identifiers
Set the system-unique ID, system serial number, machine type, and machine model.

Setting the system brand
The system brand identifies your system using a 2-character system brand value.

Setting auto-power restart

Enable or disable the function that automatically restarts the system.

About this task

You can set your system to automatically restart. This function is useful when power has been restored and any backup power supply has recharged after a temporary power failure or after an unexpected power-line disturbance that caused the system to shut down.

To perform this operation, your authority level must be one of the following authority levels:

- Administrator
- Authorized service provider

To use auto-power restart, the system operating mode must be set to **normal** in the power on and power off system settings.

To set the auto-power restart function, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Auto Power Restart**.
3. Select either **Enable** or **Disable** from the selection list. By default, the state for auto-power restart is *Disable*.
4. Click **Save settings** to save the selected options.

Results

When the system restarts, it returns to the state it was in at the time of the power loss. If the system is not managed by a Hardware Management Console (HMC), the system reboots the operating system. If the system is managed by an HMC, all of the partitions that were running before the power loss are reactivated.

Related tasks

Powering the system on and off
View and customize various initial program load (IPL) parameters.

Performing an immediate power off

You can power off your system faster by using the immediate power off function. Typically, this option is used when an emergency power off is needed. The operating system is not notified before the system is powered off.

About this task

⚠ **Attention:** To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system prior to performing an immediate power off.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To perform an immediate power off, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Immediate Power Off**.
3. Click **Continue** to perform the operation.

Performing a system reboot

You can reboot your system without a complete system shutdown.

About this task

Important: Rebooting the system immediately shuts down all partitions.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To perform a system reboot, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **System Reboot**.
3. Click **Continue** to perform the operation.

ASMI authority levels

Several authority levels are available for accessing the service processor menus by using the ASMI.

The following levels of access are supported:

General user
The menu options presented to the general user are a subset of the options available to the administrator and authorized service provider. Users with general authority can view settings in the ASMI menus. The login ID is `general` and the default password is `general`.

Administrator
The menu options presented to the administrator are a subset of the options available to the authorized service provider. Users with administrator authority can write to persistent storage, and view and change settings that affect the server's behavior. The first time a user logs into the ASMI after the server is installed, a new password must be selected. The login ID is `admin` and the default password is `admin`.

Authorized service provider
This login gives the authorized service provider access to all functions that could be used to gather additional debug information from a failing system, such as viewing persistent storage, and clearing all deconfiguration errors. There are three authorized service provider login IDs: **celogin**, **celogin1**, and **celogin2**.

- **celogin** is the primary service provider account. It is enabled by default, and it can enable or disable the other two service provider IDs (celogin1 and celogin2). The login ID is **celogin**; the password is generated dynamically and must be obtained by calling IBM technical support. **celogin** can be disabled by the **admin** user.

Important:

IBM Power Systems include a **celogin** or **service** login ID, which is used to perform advanced functions within the ASMI. The customer can request a temporary password from IBM to gain access to these features. IBM reserves the right to charge a service fee to provide this support. Any additional support that is provided will be subject to IBM’s business rules, hourly services rates, and other associated terms.

- **celogin1** and **celogin2** are disabled by default. If the IDs are enabled, a static password must be set for them. The default password for both IDs is **celogin**. The default password must be changed the first time the ID is enabled. The **admin** user can also disable and enable these login IDs.
- To reset the password for **celogin1** or **celogin2**, the **admin** user can disable, then re-enable the ID. As soon as the ID is re-enabled, the password must be changed.
- If enabled, **celogin**, **celogin1**, or **celogin2** can be used to reset the admin password, if necessary.

During the initial administrator and general user logins, the only menu option available is **Change Password**. To gain access to additional ASMI menus, you must change the administrator and general user default passwords. If you are an authorized service provider, you cannot change your password.

Related tasks

Changing ASMI passwords
Change the general user, administrator, and HMC access passwords.

ASMI login restrictions

Learn about ASMI login restrictions, including the maximum number of user logins allowed.

Only three users can log in at the same time. For example, if three people are logged in to the ASMI and a person with a higher authority level than one of the current logged in users attempts to log in, the ASMI forces one of the lowest-privileged users to log out. In addition, if you are logged in and not active for 15 minutes, your session expires. You receive no immediate notification when your session expires. However, when you select anything on the current page, you are returned to the ASMI Welcome pane.

To see who is logged in to the ASMI, view **Current users** on the ASMI Welcome pane after you log in.

Note: The **User ID Status** table is not shown on the ASMI Welcome pane until you log in.

If you make five login attempts that are not valid, your user account is locked out for five minutes and none of the other accounts are affected. For example, if the administrator account is locked, the general user can still log in using the correct password. This login restriction applies to the general user, administrator, and authorized service provider IDs. This login restriction also applies to the managed system HMC access ID, which is set using the HMC.

Related concepts

ASMI authority levels
Several authority levels are available for accessing the service processor menus by using the ASMI.

Setting up an ASMI login profile

Learn how to change passwords, view login audits, change the default language, and update the installed languages.

Changing ASMI passwords

Change the general user, administrator, and HMC access passwords.

About this task

You can change the general user, administrator, and HMC access passwords. If you are a general user, you can change only your own password. If you are an administrator, you can change your password and the passwords for general user accounts. If you are an authorized service provider, you can change your password, the passwords for general and administrator user accounts, and the HMC access password.

Passwords can be any combination of up to 64 alphanumeric characters. The default password for the general user ID is `general`, and the default password for the administrator ID is `admin`. After your initial login to the ASMI and after the reset toggle jumpers are moved, the general user and administrator passwords must be changed.

The HMC access password is usually set from the HMC during initial login. If you change this password using the ASMI, the change takes effect immediately.

Note: The IPMI password can be changed or reset on any OPAL supported system.

To change a password, follow these steps:

Note: As a security measure, you are required to enter the current user's password into the **Current password for current user** field. This password is not the password for the user ID you want to change.

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Change Password**.

4. Specify the required information, and click **Continue**.

Retrieving ASMI login audits

You can view the login history for the ASMI to see the last 20 successful logins and the last 20 logins that failed.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To retrieve login audits, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Retrieve Login Audits**. The content pane displays the login history.

Viewing user access policy

You can view the user access policy for the ASMI.

About this task

You can view the access levels associated with each user in the ASMI.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the user access policy, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **User Access Policy**. The content pane displays the user access policy.

Changing the default language for the ASMI

Select the language that will be used to display the Advanced System Management Interface (ASMI) web and teletype (tty) menus.

About this task

You can select the language that is displayed on the ASMI welcome screen prior to login and during your ASMI session if you do not choose an alternative language at the time of login. You must provide all requested input in English-language characters regardless of the language selected to view the interface.

Note: You can change the language for each ASMI session by selecting the desired language from the menu found on the ASMI Welcome pane prior to logging in to the ASMI.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator

- Authorized service provider

To change the default language, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Change Default Language**.
4. In the content pane, select the required default language and click **Save setting**.

Updating installed languages

Select additional languages to install in the service processor.

About this task

A maximum of five languages can be supported on the service processor at any given time. By default, English is always installed. Languages installation changes take effect when the firmware is updated.

Note: You must provide all requested input in English-language characters regardless of the language selected to view the interface.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To update the installed language, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Update Installed Languages**.
4. In the content pane, select the required languages and click **Save setting**.

Managing your server using the ASMI

Many tasks can be performed using the ASMI if you have successfully logged in with the requisite authority level.

The service processor and the ASMI are standard on all Power Systems servers.

Related concepts

ASMI authority levels
Several authority levels are available for accessing the service processor menus by using the ASMI.

Viewing system information

View system information such as vital product data (VPD), persistent storage, system power control network (SPCN) trace data, and progress indicator data.

Note: The Firmware update license key expiration date is always shown in the upper-right corner of the ASMI status page.

Important: Clicking **Back** in the browser might display outdated data. To display the most up-to-date data, select the required item from the navigation pane.

Viewing vital product data

View selected or all the manufacturer's vital product data (VPD), such as serial numbers and part numbers.

About this task

You can view manufacturer's vital product data (VPD) stored from the system boot prior to the one in progress now.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view the VPD, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Vital Product Data**.
3. A list of field replaceable units (FRUs) that exist on the system and their descriptions are displayed. Select a single FRU or multiple FRUs from this list that you would like to view.
4. Click **Display Details** to display the details for selected FRUs, or click **Display all details** to display details for all VPD entries.

Viewing persistent storage

Learn how to display the contents of the registry.

About this task

You can gather additional debug information from a failing system by viewing the contents of the registry. The term *registry key* can refer to either the key part of a registry entry or the entire registry entry, depending on the context. The registry key hierarchy and the contents of any key can be viewed in both ASCII and hexadecimal formats.

Each registry entry is identified by a two-part key. The first part is the component name, and the second part is the name of the key. For example, the `TerminalSize` key of the esw_menu component is identified as *menu/TerminalSize*. Each registry key also has a value, which is up to 255 bytes of binary data.

To view persistent storage, your authority level must be authorized service provider.

To view the component names of the contents of the registry, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Persistent Storage**.
3. Click the component names to view a list of registry entries.
4. Click the requied registry entry to view the contents of a registry entry.

Viewing file system

View the file system that is in use.

About this task

You can view the file system that is currently is use.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view the file system, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **File System**.
3. The file systems that exist on the system and their descriptions are displayed.

Viewing SPCN trace

View system power control network (SPCN) trace data that was dumped from the processor subsystem or server drawer.

About this task

You can dump the system power control network (SPCN) trace data from the processor subsystem, or server drawer, to gather additional debug information. Producing a trace may take an extended period of time based on your system type and configuration. This delay is due to the amount of time the system requires to query the data.

Important: Due to the amount of time required to produce a trace, select this option only if it is recommended by an authorized service provider.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view this trace data, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Power Control Network Trace**. Trace data is displayed as single continuous data in two columns.
3. View the raw binary data in the left column and an ASCII translation in the right column.

Viewing progress indicator from previous boot

Learn how to display the boot progress indicator from the previous system boot. You can view the progress indicator that displayed in the control panel during the previous failed boot.

About this task

During a successful boot, the previous progress indicator is cleared. If this option is selected after a successful boot, nothing is displayed.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

The progress indicator information is stored in nonvolatile memory. If the system is powered off using the power-on button on the control panel, this information is retained. If the ac power is disconnected from the system, this information is lost.

To view the progress indicator from the previous boot, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **Previous Boot Progress Indicator**. The results are displayed in the content pane.

Viewing progress indicator history

You can view progress codes that appeared in the control panel display during the last boot. The codes display in reverse chronological order.

About this task

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view the progress indicator history, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **Progress Indicator History**.
4. Select the desired progress indicator to view additional details and click **Show Details**. The progress indicator codes are listed from top (latest) to bottom (earliest).

Viewing real-time progress indicator

You can view the progress and error codes that currently display on the control panel. Viewing progress and error codes is useful when diagnosing boot-related problems.

About this task

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view the progress indicator, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **System Information**.
3. Select **Real-time Progress Indicator** to display a small box that contains the current progress and error codes. If no value is currently set on the control panel, the small box is displayed but remains empty.

Viewing memory data

If your next level of support suspects a conflict with original equipment manufacturer (OEM) dual inline memory modules (DIMMs), support might request that you perform this procedure.

To view memory data, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select the **Memory serial presence detect data** option to view general information about the OEM DIMMs that are installed in the system. A report is shown. Your next level of support can interpret the results.

Viewing firmware maintenance history

You can view the firmware maintenance history.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the firmware maintenance history, perform the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **Firmware Maintenance History** to display the firmware history.

Viewing memory data

View the system's memory data.

About this task

You can view system's memory eRepair data.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view the VPD, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Memory eRepair Data**.
3. A list of memory data that exist on the system and their descriptions are displayed.

Changing system configuration

View and perform custom system configurations, such as enabling PCI (Peripheral Component Interconnect) error injection policies, viewing system identification information, and changing memory configuration.

Changing system name

You can change the name that is used to identify the system. This name helps your operations team (for example, your system administrator, network administrator, or authorized service provider) to more quickly identify the location, configuration, and history of your server.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

The system name is initialized to the 31-character value `Server-tttt-mmm-` SN ooooooo, where the substitution characters have the following meaning:

Characters	Description
tttt	Machine type
mmm	Model number
ooooooo	Serial number

The system name can be changed to any valid ASCII string. It does not have to follow the initialized format.

To change the system name, complete the following steps:

Procedure

1. In the navigation area, expand **System Configuration**.
2. Select **System Name**.
3. Enter the desired system name using the previous naming convention.
4. Click **Save settings** to update the system name to the new value.

Results

The new system name is displayed in the status frame, the area where the logout button is located. If another method, such as the HMC, is used to change the system name, the status frame does not reflect the change.

Configuring I/O enclosures

View and change various I/O enclosure attributes.

About this task

After the server firmware has reached the *standby* or *running* state, you can configure the following I/O enclosure when :

- List the status, location code, rack address, unit address, power control network identifier, and the machine type and model of each enclosure in the system.
- Change the identification indicator state on each enclosure to *identify* or *off*.

- Update the power control network identifier, enclosure serial number, and the machine type and model of each enclosure.
- Change the identification indicator state of the SPCN firmware in a enclosure to *Enable* or *Disable*.
- Remove rack and unit addresses for all inactive enclosures in the system.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure I/O enclosures, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and select **Configure I/O Enclosures**.
3. Select the enclosure and the required operation. If you select **Change settings**, click **Save setting** to complete the operation.

Changing the time of day

You can display and change the current date and time on your system. The time is stored as UTC (Coordinated Universal Time).

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: You can change the time of day only when the system is powered off. When the system is powered on, the time of day information is displayed and cannot be changed.

To change the time of day, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Time of Day**. If the system is powered off, the content pane displays a form that shows the current date (day, month, and year) and time (hours, minutes, and seconds).
4. Change either the date value or the time value or both, and click **Save settings**.

Viewing the firmware update policy on a System i model

If you are using a System i model, you can view the firmware update policy from either the Hardware Management Console (HMC) or through the IBM i operating system.

About this task

These options are only valid if you are using a System i model that is managed by an HMC.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the firmware update policy, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Firmware Update Policy**.

Related information
Getting firmware fixes

Changing the PCI error policy

Change the PCI error injection policy that forces errors to be injected to PCI cards.

About this task

You can enable or disable the injection of errors on the PCI bus. For example, independent software vendors who develop device drivers can inject errors to test the error handling code in the device driver.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: To inject errors, you must have special hardware in addition to having advanced PCI bus knowledge.

To enable or disable the PCI error injection policy, do the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **PCI Error Injection Policy**.
4. In the right pane, select **Enabled** or **Disabled**.
5. Click **Save settings**.

Configuring monitoring

Configure the server firmware, HMC, and service processor connection monitoring.

About this task

You can configure your service processor to monitor the system and the system to monitor the service processor. By enabling the various monitoring options, the service processor can ensure that critical system components are functioning while the system is in the *Power off*, *IPL*, and *Running* states.

To configure monitoring, your authority level must be an authorized service provider.

Monitoring is accomplished by periodic samplings called *heartbeats*, which can detect a service processor, HMC, or server firmware connection failure. For example, if the service processor connection monitoring is enabled, each service processor monitors redundant service processor communication to keep track of the status of the other service processor. When the service processor detects no heartbeat from the other service processor, the heartbeat-initiating service processor logs an error due to this communication failure. If this condition persists, the service processor leaves the machine powered on, logs an error, and performs recovery.

To configure monitoring, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Monitoring**.

4. Select **Enabled** or **Disabled** for the server firmware, service processor connection monitoring, and HMC. All connection monitoring fields are enabled by default.
5. Click **Save settings**. Monitoring does not take effect until the next time the operating system is started.

Changing the number of HSL OptiConnect connections

If you are using the IBM i operating system, you can view and change the maximum number of high-speed link (HSL) OptiConnect connections allowed for your system.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To change the number of HSL OptiConnect connections, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **HSL OptiConnect connections**.
4. Type a new value into the **Custom** field, or to permit the system to automatically determine the maximum number of HSL OptiConnect connections allowed for the system, and select **Automatic**.
5. Click **Save settings**.

Changing the memory allocation

Enable or disable the I/O Adapter Enlarged Capacity task. Once enabled, you can increase the amount of Peripheral Component Interconnect (PCI) memory space allocated to specified PCI slots.

About this task

You can increase the amount of I/O adapter memory for specified PCI slots. When the **I/O Adapter Enlarged Capacity** option is enabled, you can specify the PCI slots to receive the largest memory-mapped address spaces that are available.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To enable or disable I/O adapter memory allocation, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **I/O Adapter Enlarged Capacity**.
4. In the content pane, select **Enabled** or **Disabled**. When enabling the **I/O Adapter Enlarged Capacity**, you must specify the number of slots to enable.
5. Click **Save settings**.

Removing HMC connection data

Display and remove disconnected HMC data.

About this task

By default, HMC connection data expires on the managed system after 14 days of disconnection from the HMC. If you want to perform a task that requires all HMCs to be disconnected from the managed system, you can remove the HMC connection data prior to the 14-day period.

To disconnect an HMC, your authority level must be an authorized service provider.

To disconnect an HMC, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Hardware Management Consoles**.
4. Select the required HMC.
5. Click **Remove connection**.

Configuring virtual I/O connections

This setting is used to enable or disable all virtual input/output connectivity between partitions. If this setting is disabled, only virtual tty sessions to the hardware management console are allowed.

Managing virtual I/O connectivity

Use the Advanced System Management Interface (ASMI) to set the policy for virtual input/output connectivity.

Before you begin

About this task

Specifying this configuration setting enables you to control virtual I/O activity between partitions. The policy is set to `enabled` by default, which allows all virtual I/O connectivity between partitions. If this setting is disabled, only virtual terminal type (tty) sessions to the Hardware Management Console (HMC) are allowed.

Important: Before you change the policy setting, turn off the system. Your authority level must be an authorized service provider.

To set the policy for virtual I/O connections, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log in**.
2. In the navigation area, expand **System Configuration** and click **Virtual I/O Connections**.
3. Select either **Enable** or **Disable** to change the setting.
4. Click **Save Settings**.

Related information

Virtual Adapters

Configuring virtual resources for logical partitions

Viewing the firmware license agreement

You can view the firmware license agreement

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the firmware license agreement, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Firmware License Agreement**.

Running the floating-point test

With the configuration setting, you can control when you want to run the floating-point unit computation test. You can set it to run immediately or to run at various times.

About this task

To perform this operation, your authority level must be an authorized service provider. There are three authorized service provider login IDs: **celogin**, **celogin1**, and **celogin2**. For more information, see "ASMI authority levels" on page 18

To specify when to run this test, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log in**.
2. In the navigation area, expand **System Configuration**, and click **Floating point unit computation test**.
3. In the content pane, select the setting that you want, and then click **Save Settings** or **Run the test immediately**.

Configuring the Virtual Trusted Platform Module

Learn how to configure the Virtual Trusted Platform Module.

About this task

You can configure the Virtual Trusted Platform Module.

To configure the Virtual Trusted Platform Module, your authority level must be an authorized service provider.

To configure the Virtual Trusted Platform Module, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Virtual Trusted Platform Module**.
4. Select **Enabled** or **Disabled**.
5. Click **Save settings**.

Configuring the Hypervisor Dispatch Wheel Time

Learn how to configure the Hypervisor Dispatch Wheel Time.

About this task

You can configure the Hypervisor Dispatch Wheel Time.

To configure the Hypervisor Dispatch Wheel Time, your authority level must be an authorized service provider.

To configure the Hypervisor Dispatch Wheel Time, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Hypervisor Dispatch Wheel Time**.
4. In the content pane, update the available options as required.
5. Click **Save settings**.

Configuring the PCIe Hardware Topology

You can configure the Peripheral Component Interconnect Express (PCIe) links for the managed system. You can also view attributes of the cables comprising the link, the indicators few the specific link, and reset a link for a recovery operation.

About this task

You can configure the PCIe hardware topology, such as the link type, link status, and link width.

To configure the PCIe hardware topology, your authority level must be an authorized service provider.

To configure the PCIe hardware topology, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **PCIe Hardware Topology**.
4. In the content pane, update the available options as required.

   To view additional details for the links, select the link and click the following options:

   Identify Indicators

   Activate or deactivate the identify indicators for the FRUs and connectors associated with the selected link.

   Cable Attributes
   View the attributes of the cables associated with the specific link.

   Reset Link
   Reset a link for link recovery.

   Note: The Reset Link option is available only for **celogin** accounts.
5. Click **Save**.

Configuring the Hardware Page Table Size

Learn how to configure the Hardware page table size.

About this task

You can configure the Hardware Page Table Size.

To configure the Hardware Page Table Size, your authority level must be an authorized service provider.

To configure the Hardware Page Table Size, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Hardware Page Table Size**.
4. In the content pane, update the available options as required.
5. Click **Save settings**.

Configuring firmware

You can use the Advanced System Management Interface (ASMI) to configure the firmware on your system.

About this task

Note: This task is available only on systems that are using the firmware type as OPAL.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure the firmware, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **Firmware Configuration**.
4. From the **Firmware Type** list, select **PowerVM** or **OPAL**. Update the available configurations as required.
5. Click **Save settings** to save the firmware configuration.

Viewing estimated corrosion rates

You can use the Advanced System Management Interface (ASMI) to view the estimated corrosion rate of the system.

About this task

The estimated corrosion rate is read from the system corrosion sensors. It is a read-only value.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the estimated corrosion rate, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Estimated Corrosion Rates**.

Selecting console type

You can use the Advanced System Management Interface (ASMI) to select the console type.

About this task

You can select the console type as **IPMI** or **Serial**.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To select the console type, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **Console Type**.
4. Select either **IPMI** or **Serial**.
5. Click **Save settings** to save the current configuration.

Setting the predictive memory deallocation

You can use the Advanced System Management Interface (ASMI) to enable or disable the predictive memory deallocation.

About this task

When the predictive memory deallocation is enabled, the system automatically deallocates memory to provide optimal performance.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To enable or disable the predictive memory deallocation, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Predictive Memory Deallocation**.
4. In the content pane, select **Enabled** or **Disabled**.
5. Click **Save settings**.

Speculative execution control

Security vulnerabilities use speculative execution to perform side-channel information disclosure attacks. You can use the speculative execution control to control speculative execution at a system-level to meet your individual security standards.

About this task

You can set the speculative execution control only when the system is in `stand-by` state. To select the required speculative execution control for your system, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Speculative Execution Control**.
3. Select one of the following options:
   - **Speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks**: To mitigate exposures of the hypervisor, operating systems, and user application data to untrusted code.
   - **Speculative execution controls to mitigate user-to-kernel side-channel attacks**: To mitigate against the threat of lower privileged code accessing operating system secrets.
   - **Speculative execution fully enabled**: For systems where the hypervisor, operating system, and applications can be fully trusted.
4. Click **Save Settings** to save the changes.

Related reference

Protecting your POWER9 servers against “Spectre” and “Meltdown”
Resources are available to protect your system from "Spectre" and "Meltdown" vulnerabilities.

Setting the frequency and voltage by using high frequency policy

You can use the Advanced System Management Interface (ASMI) to enable or disable the high frequency policy.

Before you begin

To perform this operation, your authority level must be an authorized service provider.

About this task

When the high frequency policy is enabled, you can set the Nest frequencies and voltages for higher performance.

Note: When the high frequency trading function is enabled, the following features are disabled:

- On-chip controller (OCC)
- Ability to guard the system from hardware failures (also called as Gard)

To enable or disable the high frequency policy, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **High Frequency Policy**.
4. From the **High Frequency Policy** list, select **Enabled** or **Disabled**.
5. Click **Save settings**.

Deconfiguring hardware

Set deconfiguration policies, change processor configuration, change memory configuration, view deconfigured resources, and clear all deconfiguration errors.

Deconfiguring hardware cannot be performed while the service firmware is in the running state.

Setting deconfiguration policies

Set various processor and memory configuration and deconfiguration policies.

About this task

You can set various policies to deconfigure processors and memory in certain situations. You can enable policies that deconfigure the processor when failures occur, such as a predictive failure (for example, correctable errors generated by a processor exceeding the threshold). You can also enable the firmware to power off a processing unit (also called a node) for concurrent maintenance when any of the resources in that node are deconfigured. The field core override value can also be set.

To set the deconfiguration policies or the field core override value, you must have one of the following authority levels. Any user can view the deconfiguration policies.

- Administrator
- Authorized service provider

To set deconfiguration policies or the field core override value, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Hardware Deconfiguration**.
3. Select **Deconfiguration Policies**.
4. In the content pane, select **Enabled** or **Disabled** for each policy.
5. Click **Save settings**.

Field core override function overview

The factory uses the field core override function to reduce the number of processor cores when feature code 2319, Factory deconfiguration of one core, is ordered with a new system.

About this task

On specific IBM Power Systems servers, the field core override function is available on the Advanced System Management Interface (ASMI). The feature code must be ordered when a new system is ordered, and it cannot be ordered as a miscellaneous equipment specification (MES) after a system is installed. The feature code instructs the factory to reduce the number of active processor cores in the system to reduce software licensing costs. Each feature code 2319 that is ordered reduces the number of processor cores by one.

The field core override function indicates the number of cores that are active in the system. With the field core override function, you can increase or decrease the number of active processor cores in the system. The system firmware sets the number of active processor cores to the entered value. The value takes effect during the next system boot operation. The field core override value can be changed only when the system is powered off.

You must use this function to increase the number of active processor cores due to increased workload on the system. For example, consider a system that has eight active processor cores. When the system was ordered, six feature codes were ordered, which reduced the number of active cores to two. If the workload on the system increased and you wanted to activate two additional cores for a total of four active cores, you would set the field core override value to 4. The new value would go into effect during the next system boot operation. The allocation of processors to logical partitions must be reviewed after the system boot operation.

If several processor cores are configured, the system continues to run with a single core and the core is unconfigured at run time due to the recovered error threshold being exceeded or due to an unrecoverable machine check. The field core override function affects the number of cores when the system is powered on. If a runtime error occurs on a processor core, the field core override function does not affect the remaining cores on the system. On the next boot operation, after a runtime error on a processor core, the system unconfigures the core and uses spare cores that are not activated with the field core override value in the previous boot operation.

Note: When processor cores are added by using the field core override function, you must process an order for MES to maintain the system records.

If the vital product data (VPD) card and the service processor are replaced, the field core override value must be reentered. After adding a processor card, you must set the field core override value to the number of configured cores and ensure that the number of software licenses on the resulting system is in compliance with the software terms and conditions.

In the processor deconfiguration function on the ASMI, cores that are unconfigured by the field core override function are displayed as `system deconfigured`, and the error type is displayed as `By Association`. If a processor core fails and if a processor core is unconfigured by the system, the error type is displayed as `Fatal` or `Predictive`, and the error type is not displayed as `By Association`.

Setting the field core override value
The factory reduces the number of processor cores when feature code 2319, Factory deconfiguration of one core, is ordered with a new system and when the field core override value is set.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To set a field core override value, complete the following steps:

1. Ensure the system is powered off.
2. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
3. In the navigation area, expand **System Configuration** > **Hardware Deconfiguration**.
4. Click **Field Core Override**.
5. Enter the total processor quantity that should be configured. The number should be between 1 and the total number of processor cores in the system.
6. Click **Save settings**.

Determining why processor cores were unconfigured
The processor cores might be unconfigured because the field core override function was ordered, and not because of a hardware failure.

To verify the reason for processor deconfiguration, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Error/Event Logs and System Service Aids** and **Deconfiguration Records**.
3. View the processor-related error log entries. If no processor-related error log entries are not found, the processor cores were unconfigured because the field core override function was ordered.

Note: When the system is powered off and the service processor is in standby mode, access the ASMI, and click **System Configuration** > **Hardware Deconfiguration** > **Field Core Override**, to see the total number of field core override cores in the system that will be powered on. This option is not available at run time.

Examples: The reason processor cores were unconfigured
The examples shows the reason for processor deconfiguration.

Example 1: The field core override function is enabled and there are no processor errors in standby mode

The following table shows the example field core override value during the standby mode.

Table 5. Field core override value

Field	Value
Current field core override setting	5
Requested FCO setting	5

Note: The FCO value must be in the range 1 - 8.

The empty processor deconfiguration records in the **System Service Aids** > **Deconfiguration Records** window display the processors that are unconfigured only by the field core override function.

The following table shows an example of processor cores that are configured by the field core override function. The processors do not have hardware errors.

Table 6. Processor deconfiguration

Processing units: 0

Processor ID	Location code	State	Error type	Change settings
0	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
1	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
2	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
3	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
4	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
5	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable
6	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable
7	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable

Example 2: The field core override function is enabled and there are no processor errors at run time

The following table shows an example where resources are guarded because of processor errors. Note the system reference codes (SRCs).

Table 7. Deconfiguration records

Total Unconfigured Units: 3			
Unit	**Unit type**	**Error type**	**SRC**
0	Fabric	Predictive (E6)	B114E504
1	L2 Controller	Predictive (E6)	B112E504
2	Processor PSI	Predictive (E6)	B15CE504

The following table indicates that the processor cores are unconfigured because of the hardware errors at run time after the field core override function is activated at initial program load (IPL).

Table 8. Processor deconfiguration

Processing Units: 0				
Processor ID	**Location code**	**State**	**Error type**	**Change settings**
0	U78AA.001.WZSG334-P1-C11	System-deconfigured	None (EF)	Deconfigured
1	U78AA.001.WZSG334-P1-C11	System-deconfigured	None (EF)	Deconfigured
2	U78AA.001.WZSG334-P1-C11	System-deconfigured	None (EF)	Deconfigured
3	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
4	U78AA.001.WZSG334-P1-C11	Configured	None (0)	Configured
5	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable
6	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable
7	U78AA.001.WZSG334-P1-C11	FCO-deconfigured	None (0)	Not Applicable

Notes:

- Processor IDs, 0, 1, and 2 show system-deconfigured because of the fault in the processor cores.
- Error type, None (EF) indicates a fault in the processor core.

Changing the processor configuration

Learn how to display data and change the state for each processor.

About this task

All processor failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic call out for service repair. To prevent the recurrence of intermittent problems and to improve the availability of the system until a scheduled maintenance window, processors with a failure history are marked *deconfigured* to prevent them from being configured on subsequent boots.

A processor is marked *deconfigured* under the following circumstances:

- A processor fails a built-in self-test or power-on self-test testing during boot (as determined by the service processor).

- A processor causes a machine check or check stop during run time, and the failure can be isolated specifically to that processor (as determined by the processor run-time diagnostics in the service processor firmware).
- A processor reaches a threshold of recovered failures that results in a predictive call to service (as determined by the processor run-time diagnostics in the service processor firmware).
- You ordered feature code 2319, Factory deconfiguration, of one core to reduce the number of configured processor cores in the system.

During system start time, the service processor does not configure processors that are marked *deconfigured*. The deconfigured processors are omitted from the hardware configuration. The processor remains offline for subsequent reboots until it is replaced or the deconfiguration policy is disabled. The deconfiguration policy also provides the user with the option of manually deconfiguring a processor or re-enabling a previously manually deconfigured processor. This state is displayed as *deconfigured by user*.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: The state of the processor can be changed only if the system is powered off. At run time, users can view but not change the state of each processor. If the deconfiguration policy is disabled, the states of the processors cannot be changed.

To view or change the processor configuration, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Hardware Deconfiguration**.
3. Select **Processor Deconfiguration**.
4. In the right pane, select a node from the list of nodes displayed.
5. Click **Continue** to change the state of each processor to configured, or deconfigured if it is not already deconfigured by the system.
6. Reboot the system for the changes to take effect.

Changing the memory configuration

Display data for each memory unit and bank. You can change the state of each bank.

About this task

Each memory bank contains two DIMMs (dual inline memory module). If the firmware detects a failure, or predictive failure, of a DIMM, it deconfigures the DIMM with the failure, as well as the other DIMM, in the memory bank. If memory DIMMs are being monitored for errors, each memory bank will be in one of the following states:

- Configured by system (cs)
- Manually configured (mc)
- Deconfigured by system (ds)
- Manually deconfigured (md)

Each physical DIMM can contain a maximum of eight logical DIMMs. Each of the logical DIMMs can be configured or deconfigured individually.

With the ASMI, you can change the state of the memory bank from *cs* to *md*, from *mc* to *md*, and from *md* to *mc* for one or more DIMMs. If one DIMM is deconfigured, the other DIMM in the memory bank automatically becomes deconfigured.

Note: You can change the state of the memory bank only if the deconfiguration policy is enabled for the memory domain. If this policy is not enabled and you try to change the state, an error message is displayed.

The error type is the cause of memory deconfiguration and applies to the bank in the *ds* state. The error type is displayed only when the bank is in the *ds* state.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view or change the memory configuration, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Memory Deconfiguration**.
4. In the content pane, select a node from the list of nodes displayed.
5. Click **Continue** to change the state of memory to configured or deconfigured, if it is not already deconfigured by the system.

   Note: The state of the memory bank can be changed only if the system is powered off. At run time, users can view, but not change, the state of each memory bank. If the deconfiguration policy function is disabled, the state of the memory bank cannot be changed.
6. Click **Submit**. A report page is displayed, which indicates success or failure when the state of the memory bank has been changed.

Changing the processor unit configuration

Learn how to display data and change the state for the processor unit (node).

About this task

You can change the state of the processor unit (node) by using the Advanced System Management Interface (ASMI).

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: This task is only supported on multiple node systems.

To view or change the processor unit (node) configuration, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Processor Unit Deconfiguration**.
4. In the content pane, select a node from the list of nodes.
5. Click **Continue** to change the state of processor unit to configured or deconfigured, if it is not already deconfigured by the system.

   Note: The state of the processor unit can be changed only if the system is powered off. At run time, you can view, but cannot change the state of each processor. If the deconfiguration policy function is disabled, the state of the processor unit cannot be changed.
6. Click **Submit**. A report page displays whether the state of the processor unit is changed.

Clearing all deconfiguration errors

Clear error records for specific or for all resources in the system.

About this task

To clear all deconfiguration errors, your authority level must be an authorized service provider.

Note: Before performing this operation, record error messages or ensure that the error record data is no longer needed; otherwise, you lose all error data from the hardware resources.

You can choose from the following available options (resources):

- All hardware resources
- Processor node
- Processor
- Memory components
- Memory DIMMs
- I/O
- Clock
- System bus
- Processor support interface
- Service processor

To clear all deconfiguration errors, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Clear All Deconfiguration Errors**.
4. In the content pane, select the required hardware resource from the menu.

   You can select **All hardware resources** or an individual resource.
5. Click **Clear errors for selected hardware resource**.

Programming vital product data

The Advanced System Management Interface (ASMI) enables you to program the system vital product data (VPD), such as system brand, system identifiers, and system enclosure type. To access any of the VPD-related panels, your authority level must be administrator or authorized service provider.

Note: You cannot boot the system until valid values are entered for the system brand, system identifiers, and system enclosure type.

Related tasks

Powering the system on and off
View and customize various initial program load (IPL) parameters.

Setting the system brand

The system brand identifies your system using a 2-character system brand value.

About this task

Use the following table to find the system brand for your system.

Table 9. System brand values

System brand	Description
D0	IBM Storage
S0	IBM Power Systems
E0	OEM system

Important: Changing the system brand is only allowed if the value has not been set, or if the current value is **P0** and the new value will be **D0**. Additionally, for IBM Storage, each of the systems that constitutes the storage facility must be set to D0 for storage to be accessible online.

Notes:

- You cannot boot the system until valid values are entered for all fields.
- Use this procedure only under the direction of service and support.
- The field is case-sensitive. You must use uppercase letters.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To change the system brand, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Program Vital Product Data**.
3. Select **System Brand**. In the content pane, the current system brand is displayed. If the system brand has not been set, you will be prompted to enter the system brand. Enter the values as specified by service and support.

   Note: You must use capitalization because the field is case sensitive.
4. Click **Continue**. Your system brand setting and the following notice are displayed:

   ```
   Attention: Once set, this value cannot be changed unless it is 'P0', and
   then only to 'D0'.
   ```
5. Click **Save settings** to update the system brand and save it to the VPD.

Setting the system brand name

The system brand name allows you to specify the brand name for the system.

About this task

Notes:

- The option to set the system brand name is allowed only if the value of the system brand is **E0**.
- The system brand name can be changed only when the FSP is in standby state.

You must have one of the following authority levels to specify the system brand name:

- Administrator
- Authorized service provider

To specify the system brand name, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **System Configuration** and **Program Vital Product Data**.
3. Click **System Brand Name**.
4. In the **System Brand Name** field, type the name.

   The system brand name can be 16 characters in length.
5. Click **Save settings** to update the system brand and to save it to the vital product data (VPD).

Setting the system identifiers

Set the system-unique ID, system serial number, machine type, and machine model.

About this task

You can set the system-unique ID, serial number, machine type, and machine model. If you do not know the system-unique ID, contact your next level of support.

To perform this operation, you must be one of the following authority levels:

- Administrator
- Authorized service provider

Notes:

- You cannot boot the system until valid values are entered for all fields.
- You can change these entries only once.
- The field is case-sensitive. You must use uppercase letters.

To set the system keywords, complete the following steps:

Procedure

1. On the Advanced System Management Interface (ASMI) Welcome window, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Program Vital Product Data**.
3. Select **System Keywords**.
4. In the right pane, enter the values for the system serial number, machine type, and machine model, and system-unique identifier using the naming convention shown in the ASMI help. Set the **Reserved** field to blanks unless directed otherwise by service and support.

   Note: Only the machine model and the system-unique identifier can be changed after these values have been set.
5. If the system brand (RB) keyword is S0, you must set RB keyword0 to define the default logical partition environment. (If the RB keyword is any other value, setting RB keyword0 is optional.) Valid values for RB keyword0 include:

   0

   The default value (valid only if the RB keyword is not S0)

   1

   AIX

   2

   IBM i

   3

   Linux
6. If the RB keyword value is being changed because the IBM i enable or disable value has not been initialized or needs to be changed, enter the new value in RB keyword1. Valid values for RB keyword1 include:

   1

   Enables IBM i

2
Disables IBM i

If RB keyword0 is 2 or I0, indicating that the preferred operating system or default logical partition environment is IBM i, the only valid value for RB keyword1 is 1 (enables IBM i).

7. If the RB keyword value is being changed because the IBM i enable or disable value has not been initialized or needs to be changed, enter the new value in RB keyword1. Valid values for RB keyword1 include:

   1
   Enables IBM i

   2
   Disables IBM i

   If RB keyword0 is 2 or I0, indicating that the preferred operating system or default logical partition environment is IBM i, the only valid value for RB keyword1 is 1 (enables IBM i).
8. Click **Continue**. The data validation window shows the settings you entered.
9. Click **Save settings** to update the system keywords and save them to the vital product data (VPD).

Setting the system enclosure type

Set values that uniquely identify the type of enclosures attached to the system.

About this task

When setting the system enclosure type, ensure that the enclosure serial number field matches the original value, which can be found on a label affixed to the unit. Updating the enclosure serial number field keeps the configuration and error information synchronized, and this information is used by the system when creating the location codes. This task must be done using the ASMI, not with the control panel. However, if you do not have access to the ASMI, the system will still operate without updating this information.

For example, when replacing the system backplane, you must re-enter the original enclosure serial number into the enclosure serial number field to overwrite the serial number that is recorded for the new system backplane. Failure to enter the correct enclosure serial number will result in logical partition mappings being incorrect.

Notes:

- You cannot boot the system until valid values are entered for all fields in the enclosure-type information.
- The field is case-sensitive. You must use uppercase letters.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To change the system enclosure type, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Program Vital Product Data**.
3. Select **System Enclosures**. In the content pane, the current system enclosures are displayed.
4. Enter the settings for the following fields using the information from the label that is located on your enclosure and the naming conventions described in the ASMI help:
   - **Enclosure location**
   - **Feature Code/Sequence Number**

- **Enclosure serial number**: This value is different from the serial number of the system. The enclosure serial number can be found on a barcode label on the front, top, or rear of the system unit.
- **Reserved**: Set the **Reserved** field to blank spaces unless directed otherwise by service and support.

5. Click **Save settings** to update the system enclosure type information and save it to the VPD.

Changing service indicators

Turn off the system attention indicator, enable enclosure indicators, change indicators by location code, and perform an LED test on the control panel.

The service indicators alert you that the system requires attention or service. It also provides a method for identifying a field-replaceable unit (FRU) or a specific enclosure within the system.

A hierarchical relationship exists between FRU indicators and enclosure indicators. If any FRU indicator is in an *identify* state, then the corresponding enclosure indicator will change to an *identify* state automatically. You cannot turn off the enclosure indicator until all FRU indicators within that enclosure are in an *off* state.

Turning off the system attention indicator

The system attention indicator provides a visual signal that the system as a whole requires attention or service.

About this task

Each system has a single system attention indicator. When an event occurs that either needs your intervention or that of service and support, the system attention indicator lights continuously. The system attention indicator is turned on when an entry is made in the service processor error log. The error entry is transmitted to the system level and operating system error logs.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To turn off the system attention indicator, do the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **System Attention Indicator**.
4. In the right pane, click **Turn off system attention indicator**. If the attempt is unsuccessful, an error message is displayed.

Enabling enclosure indicators

Find out how to display and change Field Replaceable Unit (FRU) indicators within each enclosure.

About this task

You can turn on or off the *identify* indicators in each enclosure. An *enclosure* is a group of indicators. For example, a processing unit enclosure represents all of the indicators within the processing unit and an I/O enclosure represents all of the indicators within that I/O enclosure. Enclosures are listed by their location code.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To enable the enclosure indicator states, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **Enclosure Indicators**.
4. Select the enclosure of choice and click **Continue**.
5. Make the necessary changes to the selection list located next to each location code.
6. To save the changes made to the state of one or more FRU indicators, click **Save settings**.

   To turn off all of the indicators for this enclosure, click **Turn off all**. A report page is displayed indicating success or failure.

Changing indicators by location code

You can specify the location code of any indicator to view or modify its current state. If you provide the wrong location code, the Advanced System Management Interface (ASMI) attempts to go to the next higher level of the location code.

About this task

The next level is the base-level location code for that field replaceable unit (FRU). For example, a user types the location code for the FRU located on the second I/O slot of the third enclosure in the system. If the location code for the second I/O slot is incorrect (the FRU does not exist at this location), an attempt to set the indicator for the third enclosure is initiated. This process continues until a FRU is located or no other level is available.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To change the current state of an indicator, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **Indicators by Location code**.
4. In the content pane, enter the location code of the FRU and click **Continue**.
5. Select the preferred state from the list.
6. Click **Save settings**.

Performing an LED test on the control panel

You can perform an LED test on the control panel to determine whether one of the LEDs is not functioning properly.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To perform an LED test on the control panel, complete the following steps:

Procedure

1. In the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.

3. Select **Lamp Test**.
4. In the Lamp Test pane, click **Continue** to perform the lamp test. When a lamp test is started, the firmware-controlled indicators in the central electronics complex (CEC) and on the expansion units are turned on solid for 4 minutes, and then restored to their previous states.

Power management

Learn how to improve the performance of the processor by adjusting the server power consumption, by setting the idle power saving, and by setting the tuning parameters.

Controlling server power consumption

Control the server power consumption by adjusting the processor voltage and clock frequency.

About this task

By enabling the power saver mode, the power consumption can be reduced by adjusting the processor voltage and clock frequency. If power saver mode is disabled, the processor voltage and clock frequency are set to their default values.

Note: You can enable this option only when the server firmware is in the standby state or the running state.

To enable this option, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To control server power consumption, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Power Management** > **Power Mode Setup**.
3. In the content pane, select any of these options:

   - **Disable all modes**: Enabling this option allows the processor clock frequency to be set to the fixed, nominal value.
   - **Enable Static Power Saver mode**: Enabling this option reduces power consumption by lowering the processor clock frequency and voltage to fixed values. This option reduces the power consumption of the system while delivering predictable performance.
   - **Enable Dynamic Performance mode**: Enabling this option causes the processor frequency to vary based on workload and active core count. As the workload or active core count decrease, the processor uses less power, which enables the frequency to be increased above nominal. During periods of very low utilization, the processor frequency is reduced to save energy. This mode provides consistent performance across all environmental operating conditions.
   - **Enable Maximum Performance mode**: Enabling this feature causes the processor frequency to vary based on the workload and active core count. As the workload or active core count decrease, the processor uses less power, which enables the frequency to be increased above nominal. In this mode, the allowed socket power is increased to the maximum value, which results in top performance with increased fan noise and higher power consumption. In more stressful environmental conditions, performance may vary.

   Note: Enabling any of the power saver modes causes changes in the processor frequencies, changes in processor use, changes in power consumption, and varying performance.
4. Click **Continue**.

Setting the idle power saver

Save the power during the idle stage by setting the idle power delay time and the idle usage threshold.

About this task

By enabling this option, the power consumption during the idle time can be reduced by setting the idle power delay time and the idle usage threshold for enter and exit. Enabling the idle power saver function causes the system to use less power when certain thresholds are met.

To enable this option, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To set the idle power saver, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Power Management** > **Idle Power Saver**.
3. In the right pane, select **Enabled** or **Disabled** for the **Idle power saver**.
4. In the **Delay Time to Enter Idle Power** field, type the number of seconds to delay before the system enters the idle power saving mode.
5. In the **Utilization Threshold to Enter Idle Power** field, type the percentage of the use threshold for the system to reach before entering the idle power saving mode.
6. In the **Delay Time to Exit Idle Power** field, type the number of seconds to delay before the system ends the idle power saving mode.
7. In the **Utilization Threshold to Exit Idle Power** field, type the percentage of the use threshold for the system to reach before ending the idle power saving mode.
8. Click **Save settings**.

   Note: Selecting a usage threshold to enter idle power that is higher than the usage threshold to exit idle power results in unexpected behavior.

Setting the tuning parameters

Learn how to use the tuning parameters to improve the power performance.

About this task

To enable this option, you must have one of the following authority levels:

- Administrator
- Authorized service provider

The tunable parameters can be used to modify the system behavior while the dynamic power saver function is enabled. This might be useful to properly balance the performance that is required with the desired energy savings. These parameters must not be changed unless you are working directly with an IBM representative or unless you have the proper level of expertise in the effects of these parameter changes.

Certificate management

You can generate self-signed certificate or upload trusted certificates signed by the chosen Certificate Authority (CA) to ensure trusted access. Use the steps in this procedure to manage certificates.

About this task

You can manage certificates for single system or multiple systems in any of the following methods:

- Using Advanced System Management Interface (ASMI) for individual systems.
- Using Hardware Management Console (HMC)-based interface to enable single path for certificate management on multiple systems.

To complete this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To manage certificates, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **Security** > **Certificate management**.
4. Select one of the following options:
   - Generate a new key and a self-signed certificate
   - Generate a new key and a certificate signing request (CSR)
   - Export a certificate signing request (CSR)
   - Import a signed certificate
   - Export a signed certificate
5. Click **Continue** and follow the instructions to work with certificates.

Managing the external services

You can use the ASMI to selectively disable the applications that are not required at any given point in time.

About this task

You can enable or disable the Intelligent Platform Management Interface (IPMI), Common Information Model (CIM), and Service Location Protocol (SLP) services. To complete this operation, you must be an administrator.

To enable or disable services, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **Security** > **External Services Management**.
4. For each of the following services, select **Enable** or **Disable** depending on your requirement:
   - IPMI
   - CIM
   - SLP
   - RTAD
5. Click **Save settings** to save the changes.

TPM Required policy

The trusted platform module (TPM) Required Policy determines whether a node (or system, if the system has a single node) is allowed to boot without a functional TPM.

About this task

To change the TPM Required Policy, complete the following steps:

Note: Enabling the TPM Required Policy results in termination of a node (or a system, if only one node is active) when both of the following conditions are true:

- No functional TPMs are available during the boot.
- The system is in secure mode (due to a planar jumper setting).

If either of the conditions is not true, the boot operation continues. Disabling the TPM Required Policy stops the node or system termination when there are no functional TPMs. The policy does not prevent an available TPM from being used.

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Click **Security** > **TPM Required Policy**.
4. Select **Enable** or **Disable** depending on your requirement.
5. Click **Save settings** to save the changes.

Secure storage policy

You can use the secure storage policy to clear the sensitive data on the system.

About this task

Choose the **Secure storage policy** menu to clear the sensitive data for the following activities:

- Returning the system to IBM Global Asset Recovery Services (GARS).
- Resale of the system.
- When there are changes in the customer workloads such as moving a system from development environment to production use.
- When the encryption or decryption keys are compromised or lost.

Notes:

- You can use the secure storage policy to clear the sensitive data on the system. Due to the sensitivity of the data that might be cleared, the procedure requires physical access to the system to authorize the operation.
- **Warning: This operation is not reversible.** If the sensitive data that is cleared contains data or storage encryption keys, you will also lose the encryption keys. Additionally, if the encryption keys or data are not replicated to another location, the system also loses the ability to decrypt data that is encrypted by using those encryption keys.

To change the secure storage policy, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** > **Security** > **Secure Storage Policy.**
3. On the content pane, select any one of the following options:

- **Clear None:** This option is the default option. No sensitive data is cleared on the next power-on.
- **Clear All:** Select this option to clear or reset all the sensitive data that is controlled by the platform firmware.
- **Clear OS Secureboot Key:** Select this option to enable the OpenPower Abstraction Layer (OPAL) to clear the secure boot keys of the operating system.
- **Clear PowerVM System Key:** Select this option to enable the PowerVM® to clear the system key to the default state. The trusted system key is used for virtual Trusted Platform Module (vTPM) and Platform Keystore data encryption.

4. Click **Save settings** to save the changes.
5. Power-on the system. The system detects the request to change the secure storage policy and enables the physical presence detection to authorize the operation. The system then automatically powers off.
6. Power-on the system manually by using the power button. The system performs the requested operation and the selected operation returns to the default option that is **Clear None**.

Setting performance options

You might enhance the performance of your managed system by changing the logical-memory block size and enabling cache locking mode.You might enhance the performance of your managed system by changing the logical-memory block size and increasing the system-memory page size.

This information describes how you might enhance the performance of your managed system.

Changing the logical-memory block size

You might enhance the managed system performance by manually or automatically changing the logical-memory block size.

About this task

The system kernel uses the memory block size to read and write files. By default, the logical-memory block size is set to **Automatic**. This setting allows the system to set the logical-memory block size that is based on the physical memory available. You can also manually change the logical-memory block size.

To select a reasonable logical block size for your system, consider both the performance that is wanted and the physical memory size. Use the following guidelines when selecting logical block sizes:

- On systems with a small amount of memory installed (2 GB or less), a large logical-memory block size results in the firmware taking an excessive amount of memory. Firmware must use at least one logical-memory block. Generally, select the logical-memory block size to be no greater than one eighth the size of the system's physical memory.
- On systems with a large amount of installed memory, small logical-memory block sizes result in many logical-memory blocks. Because each logical-memory block must be managed during boot, many logical-memory blocks can cause boot performance problems. Generally, limit the number of logical-memory blocks to 8 K or less.

Note: The logical-memory block size can be changed at run time, but the change does not take effect until the system is restarted.

To change logical-memory block size, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Procedure

To configure logical-memory block size, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Performance Setup**.

3. Select **Logical Memory Block Size**.
4. In the content pane, select the logical-memory block size and click **Save settings**.

Increasing the system-memory page size

You can improve system performance by setting up the system with larger memory pages.

About this task

Performance improvements vary depending on the applications running on your system. Only change this setting if advised by service and support.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To set up your system with larger memory pages, do the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Performance Setup**.
3. Select **System Memory Page Setup**.
4. In the right pane, select the settings that you want.
5. Click **Save settings**.

Configuring network services

Use Advanced System Management Interface (ASMI) to configure network interfaces, configure network access, and debug the virtual tty.

Configuring network interfaces

You can configure network interfaces on the system. The number and type of interfaces vary according to the specific needs of your system.

About this task

⚠ **Attention:** This operation can be performed when the system is powered on as well as powered off. Because network configuration changes occur immediately, existing network sessions, such as HMC connections, are stopped. If a firmware update is in progress, do not perform this operation. The new settings must be used to re-establish any network connections. Additional errors might also be logged if the system is powered on.

You can change the network configurations when the system is in any state.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure network interfaces, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Click **Network Configuration**.

Important: If you are attempting to configure a network connection on a multi-drawer system, you must select the primary or secondary service processor, and then click **Continue**.

4. Specify one of the following network configurations and click **Continue**:
   - In the **Interface Configuration** section, click one the following configurations:
     - **IPv4**
     - **IPv6**
   - In the **Static Route Configuration**, click **IPv4**.

     Note: This settings cannot be used for sibling service processor. For example, if the user is logged in from primary service processor, then this settings cannot be used for secondary service processor
5. Skip to one of the following steps depending on the networking configuration you specified:
   - If you selected **IPv4** in **Interface Configuration**, continue with the next step.
   - If you selected **IPv6** in **Interface Configuration**, continue with step 7.
   - If you selected **IPv4** in **Static Route Configuration**, skip to step 12.
6. Select **Configure this interface** to specify the configuration details for the required interface. You can specify the details for eth0 and eth1 network interfaces.

   a) From the **IPv4** list, select **Enabled**.

   b) From the **Type of IP address** list, select one of the following options:

   Static
   If you select this option, then you must specify the host name, IP address, subnet mask, broadcast address, and the default gateway.

   Dynamic
   No additional input is required.
7. Select **Configure this interface** to specify the configuration details for the required interface. You can specify the details for eth0 and eth1 network interfaces.

   a) From the **IPv6** list, select **Enabled**.

   b) From the **DHCP** list, select **Enabled**.

   c) From the **Auto-configured IP address** list, select **Enabled**.

   d) In the **Host name** field, specify the host name.
8. Provide the configuration details for the IP addresses.
9. Provide the following details and skip to step 12
   - **Domain name**
   - **IP address of first DNS server**
   - **IP address of second DNS server**
   - **IP address of third DNS server**
10. Select the network interface that you want to configure. You can select eth0 or eth1.
11. Specify the **IP address**, **Subnet mask**, and **Gateway address** for the network interface.
12. Click **Continue** to verify the IP settings that you specified.

    ⚠ **Attention:** If incorrect network configuration information is entered, you may not be able to use the ASMI after the changes are made. To remedy this situation, you must reset the service processor to the default settings by removing the service processor assembly from the server and moving the reset jumpers. Resetting the service processor also resets all user IDs and passwords to their default values.

    Note: To reset network configuration settings to the default factory settings, click **Reset Network Configuration**.
13. Click **Save settings** to make the changes.

Configuring network access

Specify which IP addresses can access the server.

About this task

When you configure network access, you specify which IP addresses can access the service processor. You can specify a list of allowed IP addresses and a list of denied IP addresses.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure network access, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Select **Network Access**. In the content pane, the **IP address** field displays the IP address of the server that your browser is running on and that connects to the ASMI.

   Note: On systems running system firmware Ex340 or later, you will be asked to select IPv4 or IPv6 before proceeding to the network configuration screen. If IPv6 is selected, the following instructions can still be generally followed.
4. Specify up to 16 addresses each for the list of allowed addresses and the list of denied addresses. ALL is a valid IP address.

   If a login is received from an IP address that matches a complete or partial IP address in the allowed list, access to the service processor is granted. Access to the service processor is not allowed if a login is received from an IP address that matches a complete or partial IP address from the denied list.

   Notes:

   - The allowed list takes priority over the denied list, and an empty denied list is ignored.
   - When the allowed list has ALL, then access from all the IP addresses that are reachable are allowed and the IP addresses mentioned in the denied list are ignored.
   - ALL is not allowed in the denied list when the allowed list is empty.
5. Click **Save settings** to validate the data.

Using extended services

Specify the IP address and directory path for remote systems.

About this task

The ASMI allows you to mount a directory at a fixed mounting point on the service processor in order to enable utilities, such as telnet, ftp, and rsh. You can also clear the current mount settings. To mount a directory, the IP addresses of the remote system and path to the directory on the remote system must be provided. The targeted directory will be mounted at a fixed location on the host service processor. By default, the mount point is /nfs.

This option is beneficial for gathering additional debug information from a failing system. To enable utilities, such as telnet, the name and relative path to a shell script on the remote system along with the IP address and path to mount the directory on the remote system must be provided. This shell script, when executed on the host service processor, enables utilities such as telnet and ftp.

To perform this operation, you must have one of the following authority levels:

- Authorized service provider

To configure extended services, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Extended Services**.
3. In the content pane, specify the IP address of the remote machine, directory path to mount on the remote machine, and relative path name of the shell script you desire to execute on the remote machine. The relative path of the shell script field is optional.
4. Click **Save settings** to mount the remote directory using your entered data or click **Clear mount** to unmount the previously mounted remote directory.

Debugging the virtual tty

Debug the virtual teletype (tty) from the master service processor.

About this task

You can gather additional debug information from a failing system by using the debug virtual server (DVS). The DVS enables communication with the server firmware and partition firmware. DVS allows a maximum of eight open connections. External interfaces such as the ASMI and service processor remote application can communicate with the server firmware and partition firmware through DVS. This communication is bidirectional. External interfaces can send a message to the server firmware and partition firmware through DVS.

DVS uses the partition ID and session ID to distinguish between the server firmware and partition firmware. The range for both the partition ID and session ID is 0 to 255. Clients, such as the ASMI, interact with DVS using a TCP/IP socket. Port 30002 on the service processor is used for this communication.

The partition ID and the session ID parameters must be specified to start communicating. After specifying both parameters, a telnet session must be opened to send messages. The telnet session must be started and messages must be sent within the time-out period of 15 minutes. If both actions are not taken within the time-out period, the connection is closed.

To perform this operation, your authority level must be authorized service provider.

To debug the virtual tty, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Select **Debug Virtual TTY**.
4. In the content pane, enter the partition and session IDs.
5. Click **Save settings**.

Using on-demand utilities

Activate inactive processors or inactive system memory without restarting your server or interrupting your business.

Capacity on Demand (CoD) allows you to permanently activate inactive processors or inactive system memory without requiring you to restart your server or interrupt your business. You can also view information about your CoD resources.

Important: Use this information if a hardware failure causes the system to lose its Capacity On Demand or Function On Demand purchased capabilities, and if there has never been an HMC managing the system. If an HMC is managing the system, use the HMC to complete the following tasks instead of the ASMI.

Order Capacity on Demand

Generate the system information that is required when you order processor or memory activation features.

About this task

After you determine that you want to permanently activate some or all of your inactive processors or memory, you must order one or more processor or memory activation features. You then enter the resulting processor or memory-activation key that is provided by your hardware provider to activate your inactive processors or memory.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To order processor or memory activation features, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **On Demand Utilities**.
3. Select **CoD Order Information**.

   The server firmware displays the information that is necessary to order a Capacity on Demand activation feature.
4. Record the information that is displayed.

Activating Capacity on Demand or PowerVM by using the ASMI

You can use the Advanced System Management Interface (ASMI) to activate Capacity on Demand processors or memory, or enable PowerVM features (formerly known as Advanced POWER® Virtualization).

Before you begin

When you obtain processor or memory activation features, you receive an activation key that you use to activate your inactive processors or memory.

About this task

If your system did not come with the PowerVM feature enabled, you must use the ASMI to enter the activation code that you received when you ordered the feature. This activation code also enables you to use the Micro-Partitioning® feature on the system.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To permanently activate some or all of your inactive processors or memory, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **On Demand Utilities**.
3. Select **CoD Activation**.
4. Enter the activation key into the field.

5. Click **Continue**. If you entered the code for the PowerVM feature, the feature is enabled. If you entered the code for Capacity on Demand, continue with the steps in Resuming server firmware after CoD activation.

Resuming server firmware after CoD activation

Resume the booting process of the server firmware after the Capacity on Demand (CoD) activation keys are entered.

About this task

You can resume the server firmware after the CoD activation keys are entered. Resuming the server firmware causes the CoD key to become recognized and the hardware to become activated. This option allows the server to complete the startup process that has been delayed up to one hour in order to place the server into the *On Demand Recovery* state that was needed to enter the CoD activation keys.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To resume the server firmware, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **On Demand Utilities**.
3. Select **CoD Recovery**.
4. Click **Continue** to perform the specified operation.

Use Capacity on Demand commands

As directed by service and support, you can run a Capacity On Demand-related command that is sent to the server firmware.

About this task

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To run a Capacity On Demand command, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **On Demand Utilities**.
3. Select **CoD Command**.
4. Enter the Capacity On Demand command into the field and click **Continue**.

   The response to the command from the server firmware is displayed.

Viewing information about CoD resources

When Capacity on Demand (CoD) is activated on your system, you can view information about the CoD processors, the memory that is allocated as CoD memory, and Virtualization Engine technology resources.

About this task

To view the CoD resource information, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view information about CoD resources, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **On Demand Utilities**.
3. Select one of the following options for the type of information you want to view:
   - **CoD Processor Information** to view information about the CoD processors
   - **CoD Memory Information** to view information about available CoD memory
   - **CoD Vet Capability Settings** to view information about the CoD capabilities that are enabled on Virtualization Engine technologies

What to do next

Note: You can also view the CoD capability settings from the Hardware Management Console (HMC).

Viewing and customizing ASMI service aid menus

View and customize troubleshooting information with various Advanced System Management Interface (ASMI) service aids (such as viewing error logs and initiating service processor dumps).

This topic provides information about using the following ASMI service aids.

Note: Each system port is disabled when a Hardware Management Console (HMC) is attached to the server and the server is booted beyond the service processor standby state.

Displaying error and event logs

Display a list of all of the error and event logs in the service processor.

About this task

You can view error and event logs that are generated by various service processor firmware components. The content of these logs can be useful in solving hardware or server firmware problems.

To perform this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

Informational, error, and miscellaneous logs can be viewed by all authority levels. Hidden error logs can be viewed by authorized service providers.

The following table shows error log types that might be displayed, the conditions that make an error log specific to that error log type, and the user authority level that will allow you to view specific types of error logs:

Table 10. Error log types

Error log type	Conditions		User availability
	Severity	Action	
Informational logs	Informational	Report to operating system (OS) but not hidden	Available to all users
Error logs	Not informational	Report to OS but not hidden	Available to all users
Hidden logs	Not informational and informational	Report to OS, hidden, or both	Available only to the authorized service provider and users with higher authority.
Miscellaneous	Informational	Not reported to OS	Available to all users

To view and clear error and event logs in summary or full detailed format, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Error/Event Logs**.

   If log entries exist, a list of error and event log entries is displayed in a summary view.
3. To view the full detail format of any of the logs listed, select the log's corresponding check box and click **Show details**.

   When multiple logs are selected, any action applies to each selected log. The full detail information might span several pages. The contents and layout of the full detail output is defined by the event or error logging component.
4. Click **Mark as reported** to mark platform error entries whose underlying causes have been resolved.

   By doing so, these entries are not reported to the operating system again when the system reboots. After they are marked, these errors can be overwritten by other errors logged in the service processor history log.

   Note: The **Mark as reported** button is available only when your authority level is authorized service provider.
5. Click **Show error/event log repository information** button to view the error or event log repository information of the managed system. The error/event log repository might get full when the errors are logged. If the errors are not acknowledged periodically, new errors might not be logged. This option displays the information for the following parameters:

   - error/event log repository
   - service processor
   - hypervisor
   - last log details
   - other vital information
6. To clear any of the error/event log entries, select the appropriate entries that you want to delete and click **Clear selected error/event log entries**.

Enabling serial port snoop

Specify parameters (including the snoop string) for enabling a serial port (system port) snoop.

About this task

You can disable or enable a snoop operation on a system port. When enabled, data received on the selected port is examined, or snooped, as it arrives. You can also specify the snoop string, a particular sequence of bytes that resets the service processor if detected. The system port S1 serves as a *catchall* reset device.

Note: Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To complete this operation, you must have one of the following authority levels:

- General
- Administrator
- Authorized service provider

To view and change the current Serial Port Snoop settings, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and select **Serial Port Snoop**.
3. Disable or enable snooping on system port S1.

   The default is *Disabled*.
4. Enter the desired snoop string, up to 32 bytes, into the **Snoop string** field.

   The current value displayed is the default. Ensure that the string is not a commonly used string. A mixed-case string is recommended.
5. Click **Update snoop parameters** to update the service processor with the selected values.

   Note: After the snoop operation is correctly configured, at any point after the system is booted, the system uses the service processor reboot policy to restart whenever the reset string is typed on an ASCII terminal attached to system port S1.

Using the ASMI to perform a system dump

Control how frequently a system dump is performed and the amount of data collected from the hardware and server firmware.

About this task

You can initiate a system dump in order to capture overall system information, system processor state, hardware scan rings, caches, and other information. This information can be used to resolve a hardware or server firmware problem. A *system dump* can also be automatically initiated after a system malfunction, such as a checkstop or hang. It is typically 34 MB.

Note: Use this procedure only under the direction of your service provider.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure and initiate a system dump, complete the following steps:

Procedure

1. Perform a controlled shutdown of the operating system if possible.
2. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
3. In the navigation area, expand **System Service Aids** and click **System dump**.
4. From the selection list labeled **Dump policy**, select the policy to determine when an automatic system dump is collected.

   The dump policy is used whenever a system error condition is automatically detected by the system. In addition to the dump policy, the platform firmware determines whether a dump is recommended, based on the type of error that has occurred. This recommendation is combined with the dump policy to determine if a system dump will be initiated.

   The dump policy include the following options:

   As needed
   Collects the dump data only for specific reasons. This is the default setting for the dump policy.

   Always
   Collects the dump data after the system locks up or after a checkstop. This setting overrides the firmware recommendation and forces a system dump, even when it is not recommended.

   Note: The dump policy only defines when a system dump is performed. It does not define what to dump nor the size of the information to be dumped. Those parameters are controlled by the **Hardware content** settings.
5. Select the policy to determine how much data to dump from the selection list labeled **Hardware content**.

   The system firmware makes a recommendation for the dump content based on the type of error that has occurred. This recommendation is combined with the hardware content to determine how much dump data is actually collected.

   The dump policy includes the following options:

   - **Automatic** Collects dump data automatically. The firmware decides which dump content is best, depending on the type of failure. This is the default setting for the hardware content.
   - **Minimum** Collects the minimum amount of dump data. Collection of hardware dump data can be time-consuming. This selection allows the user to minimize the content of the hardware portion of the system dump. It also allows the system to reboot as quickly as possible.

     Note: If this option is selected, the debug data collected for some errors may be insufficient. The capturing of relevant error data for some errors may be sacrificed for less system downtime.
   - **Medium** Collects a moderate amount of hardware error data. More data is captured with this setting than the minimum setting, and less time is needed for dump data collection in comparison to the maximum setting.
   - **Maximum** Collects the maximum amount of hardware error data. This setting gives the most complete error coverage but requires more system downtime in relation to the other policies. It is expected to be used in rare cases by authorized service providers if you are willing to sacrifice reboot speed for error capture on a first failure, or if difficult problems are being analyzed.

     Note: If this option is selected, the collection of hardware dump data can be time-consuming, especially for systems with a large number of processors.
6. In the **Server firmware content** field, select the content level that indicates the amount of data to dump for the server firmware portion of the system dump.
7. Click **Save settings** to save the setting changes.

   To save the setting changes and instruct the system to immediately process a dump with the current settings, click **Save settings and initiate dump**.

What to do next

For information about copying, reporting, and deleting the dump, see Manage dumps (http://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_managedumps_sys.htm)

Using the ASMI to perform a service processor dump

You can use the Advanced System Management Interface (ASMI) to initiate a service processor dump.

About this task

Use this procedure only under the direction of your hardware service provider. With this function, you can preserve error data after a service processor application failure, external reset, or user request for a service processor dump. The existing service processor dump is considered valid if neither the server firmware nor Hardware Management Console (HMC) has collected the previous failure data.

To perform this operation, your authority level must be authorized service provider.

To enable or disable the service processor dump and view the status of the existing service processor dump, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Service Processor Dump**.
3. Select either **Enable** or **Disable** from the selection list.

   By default, the state is *Enable*. The current setting is displayed and the status of an existing service processor dump is displayed as valid or invalid.

   Note: You cannot perform a user-requested service processor dump when this setting is disabled.
4. Click **Save settings** to save the setting changes.

   To instruct the system to immediately process a service processor dump, click **Initiate dump**.

Initiating a partition dump

Enable or disable the partition dump in addition to immediately initiating a partition dump.

About this task

Important: This feature is not available when the system is managed by a Hardware Management Console (HMC).

Use this procedure only under the direction of your hardware service provider. By initiating a partition dump, you can preserve error data that can be used to diagnose server firmware or operating system problems. The state of the operating system is saved on the hard disk and the partition restarts. This function can be used when the operating system is in an abnormal wait state, or endless loop, and the retry partition dump function is not available.

⚠ **Attention:** You might experience data loss when using this operation. This feature is only available on systems not managed by an HMC that have the system server firmware in the Running state.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To perform a partition dump, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **System Service Aids** and click **Partition Dump**.

   If you are using the IBM i operating system, and the initial partition dump attempt failed, select **Retry partition dump**.

Initiating the performance dump

Learn how to initiate the performance dump of the system. You can use the Advanced System Management Interface (ASMI) to initiate a performance dump of the system.

About this task

A performance dump of the system is a collection of data from a service processor after a failure of the system, an external reset of the system, or a manual request. You can initiate the performance dump of the system to collect and store the hardware performance data in the format of a hardware unit dump. The information is stored in a new dump file when the performance dump of the system is initiated. The performance dump of the system can be initiated during the system power-on (service processor runtime) state only.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To initiate a performance dump of the system, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Performance Dump**.
3. Click **Initiate dump** to initiate the performance dump of the system.

Performing a resource dump

Perform a resource dump of the service processor.

About this task

You can dump the hypervisor data that is stored in main storage while all the logical partitions are running. The resource dump option is available when the system is in manual operating mode, and when this function is activated by the operating system.

Note: The resource dump option is not available when the system is in terminate state, while the hypervisor is booting, or when another platform dump is in progress.

To view this information, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To perform a resource dump, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Resource Dump**.

Configuring a system port for call options

Configure a system port for use with the call-home and call-in options.

About this task

You can configure a system port used with the call-home and call-in features. You can also set the baud rate for a system port.

Note: Each system port is disabled when a Hardware Management Console (HMC) is attached to the server and the server is booted beyond the service processor standby state. Therefore, these menus are not present if the system is managed by an HMC or if the system has no ports.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure a system port, complete the following steps:

Procedure

1. In the navigation area, expand **System Service Aids** and click **Serial Port Setup**.

   Once section is displayed. The section is labeled **S1**, which is the system port that is used with the call-home feature.
2. Modify the appropriate fields in the **S1** section.

   Baud rate
   Select the baud rate for this system port. If a terminal is attached to this port, the settings must match. The speeds available are 50, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.

   Character size
   Select the character size for this system port. If a terminal is attached to this port, the settings must match.

   Stop bits
   Select the number of stop bits for this system port. If a terminal is attached to this port, the settings must match.

   Parity
   Select the parity for this system port. If a terminal is attached to this port, the settings must match.
3. Click **Save settings** to save the setting changes.

Configuring your modem

Configure your modem that is connected to the system port.

About this task

Note: Each system port is disabled when a Hardware Management Console (HMC) is attached to the server and the server is booted beyond the service processor standby state.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure the modem, complete the following steps:

Note: If you are attaching a 7852-400 modem to the S1 serial port, you must use the following switch positions on the modem (U=up and D=down): UUDD UUUD UUUD UUUU.

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Modem Configuration**.
4. Modify the fields in the **S1** section.
   - **Modem type**: Select the supported modem type from the selection list.
   - **Modem reset command**: Enter the command to use to reset the modem to the power-on defaults.
   - **Modem initialization command**: This command configures the modem for the required behavior. To ensure proper operation, result codes should be returned (ATQ0), echo should be disabled (ATE0), and result codes should be strings (ATV1). This setting is ignored if the modem type is not Custom.
   - **Modem dial command**: This command is used for dialing a number. For example, ATDT for tone dialing. This setting is ignored if the modem type is not Custom.
   - **Modem auto-answer command**: This command enables the modem to answer incoming calls. For example, ATS0=1. This setting is ignored if the modem type is not Custom.
   - **Modem pager dial command**: Enter the modem pager dial command. This command is used to dial a pager. For example: ATDT%s,,,%s;ATH0.

     Note: Both %s strings are required. This setting is ignored if the modem type is not Custom.
   - **Modem disconnect command**: Enter the modem disconnection command. This command is used to disconnect the call. For example, +++ATH0. This setting is ignored if the modem type is not Custom.
5. Click **Save settings** to save the modem configuration changes.

Configuring the call-home policy

Use this procedure to configure your system to call home (contact your next level of support).

About this task

In the following topic, call-home refers to contacting the IBM service center computer.

Notes:

- The call-home feature is supported only when the service processor (FSP) is in one of the following states: FSP Standby, FSP Termination, or during IPL process when the POWER Hypervisor is not up.
- The call-home option is not available for systems that are managed by the Hardware Management Console (HMC) or on the LC Line of Power Systems servers with BMC service processors.

To complete this operation, your must have one of the following authority levels:

- Administrator
- Authorized service provider

To configure the call-home policy, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Call-home Setup**.
4. Provide the details in the specified fields.
   - **Call-home policy**

     Disabled

     Click **Disabled** to disable the call-home feature.

IBM CC

Click **IBM CC** to forward the call-home request to IBM Service Center.

Note: If your system is behind a firewall, ensure that you allow the following IBM servers for the call-home to reach the service center:

- esupport.ibm.com
- eccgw01.boulder.ibm.com
- eccgw02.rochester.ibm.com
- www-945.ibm.com
- www.ecurep.ibm.com

OEM CC

Click **OEM CC** to forward the call-home request to the customer-specified customer care IP address and port number.

Note: If the system with the specified IP address is behind a firewall, ensure that you add the IP address to the list of allowed addresses.

Legacy CC

This option is only available for an authorized service provider. If the authorized service provider sets the call-home policy as Legacy CC, the administrator can view the details, but will not be able to change it. This option allows the call-home policy to use the configuration that was set up earlier.

- **Telephone numbers**

Service center telephone number

This is the number of the service center computer. The service center usually includes a computer that takes calls from servers with call-out capability. This computer is referred to as the **catcher**. The **catcher** expects messages in a specific format to which the service processor conforms. For more information about the format and **catcher** computers, see the readme file in the AIX **/usr/samples/syscatch** directory. Contact your authorized service provider for the correct service center telephone number to enter. Until you have that number, leave this field unassigned.

Customer administration center telephone number

This is the number of the system administration center computer (catcher) that receives problem calls from servers. Contact your system administrator for the correct telephone number to enter here. Until you have that number, retain this field as unassigned.

Digital pager telephone number

This is the number for a numeric pager carried by the personnel who responds to problem calls from your server. Contact your administration center representative for the correct telephone number to enter.

Pager numeric data

Enter the numeric data to be sent during a pager call.

- **Customer company information**

Provide the complete postal address of the company and the details must be as per boarding pass process.

- **Company name**
- **Street address**
- **City and state**
- **Zip/postal code**
- **Country or region**

- **Customer Data**

Provide any specific data that has to be sent with call-home. The data can be a string up to 64 characters in length.

- **Customer care address**

  This information must be provided only when the call-home policy is set to **OEM CC**.

  - **IP address**
  - **Port number**
- **Call-home setup for Legacy CC**

  This information must be provided only when the call-home policy is set to **Legacy CC**

  - **Call-home serial port**
  - **Call-in serial port**
  - **Call-home dialing policy**
  - **Number of retries**
- **System location**

  This information must be provided only when the call-home policy is set to **Legacy CC**.

  Geography
  Specify the geography where the system is located.

5. Click **Save settings** to save changes.
6. Using the ASMI interface, test the call-home feature. To test the call-home functionality, see "Testing the call-home policy" on page 68.

Testing the call-home policy

You can test the call-home policy configuration after the modem is installed and configured correctly.

About this task

Note: You can test the call-home policy only when it is enabled. See "Configuring the call-home policy" on page 66 for instructions about configuring the call-home policy.

To test the call-home policy, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To test your call-home policy configuration, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Call-Home Test**.
4. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.

Rebooting the service processor

In critical system situations, such as during system hangs, you can reboot the service processor. Complete this task only when directed by your service provider.

About this task

Rebooting the service processor cannot be performed while the service firmware is in the running state.

To complete this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To reboot your service processor, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Reset Service Processor**.
4. Click **Continue** to perform the reboot.

Soft reset of the service processor

In certain situations, you might have to reset the service processor while the service firmware is in the running state. Complete this task only when directed by your service provider.

About this task

During soft reset of the service process, the host partitions are not powered down.

To complete this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To reboot your service processor, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Click **Soft Reset Service Processor**.
4. Click **Continue** to complete the soft reset.

Restoring your server to factory settings

Restore firmware settings, network configuration, and passwords to their factory defaults.

About this task

You can reset all the factory settings on your server to the factory default settings, or you can choose to reset specific settings by using the following options:

- Reset all settings
- Reset the service processor settings
- Reset the server firmware settings
- Reset the PCI bus configuration

If you choose to reset all settings, all three of these actions are performed resulting in the service processor settings, the server firmware settings, and the PCI bus configuration being reset in one operation.

Note: If redundant service processors are installed and enabled, whichever type of reset operation that you perform on the primary service processor will also be performed on the secondary service processor.

⚠ **Attention:** Reset your server settings to the factory default only when directed by your service provider. Before you reset all settings, make sure you have manually recorded all settings that need to be preserved. This operation can be performed only if the identical level of firmware exists on both the permanent firmware boot side, also known as the P side, and the temporary firmware boot side, also known as the T side.

Resetting the service processor settings results in the loss of all system settings (such as the HMC access and ASMI passwords, time of day, network configuration, and hardware deconfiguration policies) that you may have set through user interfaces.

⚠ **Attention:** Resetting the server firmware settings results in the loss of all of the partition data that is stored on the service processor.

Resetting the PCI bus configuration results in the following sequence of events:

- The service processor instructs the server firmware to power on and enter into a standby state.
- When the server firmware has entered into the standby state, the PCI bus configuration settings are cleared.
- The server firmware then powers off and the service processor is in the standby state.

⚠ **Attention:** Resetting all settings results in the loss of system settings as described for each option in the preceding paragraphs. Also, you will lose the system error logs and partition-related information.

To restore factory default settings, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: You can only change the time of day when the system is powered off.

To restore factory default settings, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Factory Configuration**.
4. Select the options that you want to restore to factory settings.
5. Click **Continue**. The service processor reboots after all settings have been reset.

Entering service processor commands

You can enter commands to perform on the service processor. Currently, no syntactical validation is performed on the command string that is entered. As a result, ensure that the command is entered correctly before initiating the action.

About this task

To perform this operation, your authority level must be an authorized service provider.

To enter service processor commands, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Service Processor Command Line**.
4. Enter a valid command that does not exceed 80 characters.

   Note: Entering a command that is not valid might hang the system. If this condition occurs, reset the service processor.

5. Click **Execute** to perform the command on the service processor.

Viewing resources deconfigured using the guard function

View a list of the hardware resources that have been deconfigured by the guard function of the system processor.

About this task

For each deconfigured hardware resource, the type of error that caused the deconfiguration (for example, predictive, diagnostic, uncorrectable) is also displayed. The detailed error log entry can also be viewed.

To view this information, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view a list of the deconfigured resources, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Deconfigured Records** to view a list of deconfigured resources.

   Note: The **Customer Alert** feature, which is available in this view, is enabled by default. This feature periodically alerts you to replace any deconfigured hardware. You can enable or disable the **Customer Alert** feature if the memory or processor has been deconfigured from the system.

Enabling the USB service functions

Learn how to enable an Universal Serial Bus (USB) service functions to save the debug and system configuration data on the removable USB flash device.

About this task

You can use an USB flash device to save the debug and system configuration data and later use the debug and system configuration data to debug the problem. You can save the service processor dump files, system dump files, hardware unit dump files, system settings, network settings, and platform errors or events log on the removable USB flash drive. You can also restore the system settings or network settings from the removable USB flash drive to the service processor.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To enable an USB service functions, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. Change the state of the service processor to **standby** state or termination state.
3. Connect an USB flash drive to the system.
4. In the navigation area, expand **System Service Aids** > **USB-Enabled Service Functions**.
5. From the USB-Enabled Service Functions list, select the required options and click **Continue** to save the dump files or log files to an USB flash drive.

   Note: If you restore network settings from another system, the system is disconnected from the network.

Initiating a service processor failover

You can use the Advanced System Management Interface (ASMI) to initiate a failover from the backup service processor.

About this task

Service processor failover reduces customer outages caused due to service processor hardware failures. If a redundant service processor is supported for the current system configuration, you can initiate a failover from the backup service processor.

To perform this operation, you must have one of the following authority levels:

- Administrator
- Authorized service provider

Note: This task can be initiated only from the backup service processor.

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

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Service Processor Failover**.
3. Click **Continue** to initiate the failover from the backup service processor.

Pending serviceable tasks

You can use the Advanced System Management Interface (ASMI) service aids to view a consolidation of hardware error logs, deconfiguration logs, and other serviceable records in the system.

About this task

To view the pending serviceable tasks, you must have one of the following authority levels:

- Administrator
- Authorized service provider

To view the pending serviceable tasks, complete the following steps:

Procedure

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Pending Serviceable Tasks**.
3. Select one of the following options:
   - **Hardware Serviceable Events**
   - **Deconfigured Hardware**
4. Click **Continue** to view the details.

Validating cables in the 9080-M9S system

You can use the Advanced System Management Interface (ASMI) to validate cables in the system and to identity issues such as unplugged cables, incorrect connection, and incorrect cable length.

About this task

Cable validation occurs automatically during system power on. To validate cables manually:

- If the system is at the FSP standby state, go to "Validating FSP, UPIC, and SMP cables in the 9080-M9S system at the FSP standby state " on page 73.
- If the system firmware level is FW940.00, or later, and if the system power is turned on, go to "Validating UPIC cables in the 9080-M9S system with the system power turned on " on page 73.

To display cable status, go to "Displaying the status of FSP, UPIC, and SMP cables in the 9080-M9S system " on page 74.

Notes:

- The FSP and SMP cables cannot be manually verified with the system power turned on. The cable status that is displayed is the result of the last cable validation that occurred. Cable validation occurs automatically during system power on.
- If the system firmware level is earlier than FW940.00, the UPIC cables cannot be manually verified when the system power is turned on. The cable status that is displayed is the result of the last cable validation that occurred. Cable validation occurs automatically during system power on.

Validating FSP, UPIC, and SMP cables in the 9080-M9S system at the FSP standby state

You can verify whether the flexible service processor (FSP) cables, universal power interconnect (UPIC), and symmetric multiprocessing (SMP) cables are plugged correctly and can be detected.

To validate the cables, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Cable Plugging Validation**. Then click **Validate Cables**. The system verifies that the cables that are connected are present.
3. If your configuration includes two or more nodes, expand **System Service Aids** > **Cable Plugging Validation**. Then, click **Verify Node Position**. If the system is cabled correctly, the blue identify LED on each system node is lit in a sequence, from the top node to the bottom node. If the LEDs are not lit in a sequence, the FSP cables must to be re-installed. Otherwise, if your configuration includes only one node, go to the next step.

   Note: You must follow the step only during the initial system installation process.
4. Expand **System Service Aids > Cable Plugging Validation**. Then, select **All of the above** in the **Display Cable Status** section and click **Continue**. The system validates that the cables are installed in the correct locations. Expand **System Service Aids > Cable Plugging Validation** to display a table with the results. Ensure that the plugging status displays **OK** for each cable in the displayed table. If the status displays **OK**, no further action is required. If the status does not display **OK**, review the error logs, correct the problems, and repeat steps "2" on page 73, "3" on page 73, and "4" on page 73 as needed until the status is **OK** for all cables.

Validating UPIC cables in the 9080-M9S system with the system power turned on

If the system firmware level is FW940.00 or later, you can verify whether the universal power interconnect (UPIC) cables are plugged correctly and can be detected with the system power turned on.

Notes:

- The FSP and SMP cables cannot be manually verified with the system power turned on. The cable status that is displayed is the result of the last cable validation that occurred. Cable validation occurs automatically during system power on.
- If the system firmware level is earlier than FW940.00, the UPIC cables cannot be manually verified when the system power is turned on. The cable status that is displayed is the result of the last cable validation that occurred. Cable validation occurs automatically during system power on.

To validate the cables, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **System Service Aids** > **Cable Plugging Validation**. Then click **Validate Cables**. The system verifies that the UPIC cables are present.
3. Expand **System Service Aids** > **Cable Plugging Validation**. In the **Display Cable Status** section, select **UPIC Cables** and click **Continue**. The system validates that the UPIC cables are installed in the correct locations and displays a table with the results. Ensure that the plugging status displays **OK** for each cable in the displayed table. If the status displays **OK**, no further action is required. If the status does not display **OK**, review the error logs, correct the problems, and repeat steps "2" on page 74 and "3" on page 74 as needed until the status is **OK** for all cables.

Displaying the status of FSP, UPIC, and SMP cables in the 9080-M9S system

You can display the status from the last validation of flexible service processor (FSP) cables, universal power interconnect (UPIC) cables, and symmetric multiprocessing (SMP) cables.

Cable validation occurs automatically during system power on. The cable status that is displayed is the result of the last cable validation that occurred. To display the cable status, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** > **Cable Plugging Validation**.
3. In the **Display Cable Status** section, select one of the following type of cables for which you want to view the details after validation.
   - FSP Cables
   - UPIC Cables
   - SMP Cables
   - All of the above
4. Click **Continue**.
5. Ensure that the plugging status displays **OK** for each cable in the displayed table. If the status displays **OK**, the cable is present and installed in the correct location. No further action is required. If the status does not display **OK** and you want to repair the cable, continue with the next step. If the status does not display **OK** and if you do not want to repair the cable at this time, no further action is required.
6. In the **Indicator state** field, change the indicator state to **Identify** for all cables whose plugging status is not displayed as **OK**. The identify LED for the selected cable starts to flash. Review the error logs, correct the problems, and refer to "Validating FSP, UPIC, and SMP cables in the 9080-M9S system at the FSP standby state " on page 73 or "Validating UPIC cables in the 9080-M9S system with the system power turned on " on page 73 to rerun cable validation. After repairing the cables, you must manually change the indicator state to **OFF**.

Troubleshooting problems in accessing the ASMI

Troubleshoot common problems associated with setting up access to the Advanced System Management Interface (ASMI).

The following table contains information about common problems that might occur while you are trying to access the ASMI through a web browser. The table also provides common resolutions to those problems.

Table 11. Troubleshooting problems when trying to access the ASMI through a web browser

Problem	Resolution
After you enter the server's IP address in the web browser, you receive a security alert.	Usually this means that your PC or notebook does not accept the server as a secure site. To resolve this problem, complete the following steps: 1. In the Client Authentication window, select the certificate you want to use when connecting and click **OK**. 2. If you receive the error that this page cannot be found, your PC or notebook does not trust the server as a secure site. If you have a firewall on your PC or notebook, modify the firewall settings to trust the server IP address. Then, type the IP address in the Address field of your PC's or notebook's Web browser. 3. On the Security Alert window, click **Yes**.
After you enter the server's IP address in the web browser, the browser displays an error message stating that it cannot find the IP address that you entered.	1. Ensure that you entered `https://`*`<IP address of server>`* in the Address field of your web browser. 2. Ensure that you entered the correct IP address for the server. See Table 1 on page 7 for a list of IP addresses for the server. 3. Add a routing entry to the PC or notebook so that the PC or notebook can locate the server on the network. For example, if you are using a PC installed with Windows, open a command line prompt and type: `route add` *`<server IP address>`* `mask 255.255.255.0` *`<PC or Notebook IP address>`* `metric 1`.
You are using Microsoft Internet Explorer 7.0 running on Windows XP, you have correctly cabled the PC or notebook to the server, and you cannot access the ASMI.	Usually this means that the Use TLS 1.0 option in Microsoft Internet Explorer is enabled. To connect to the ASMI, this option must be disabled. To resolve this problem, complete the following steps: 1. From the **Tools** menu in Microsoft Internet Explorer, select **Internet Options**. 2. From the Internet Options window, click the **Advanced** tab. 3. Clear the **Use TLS 1.0** check box (in the Security category) and click **OK**.
You are locked out of the ASMI after you enter the default user ID and password either incorrectly or more than five times.	Reset the default password and network settings to the default settings using one of the following methods: • Request a new login password from your authorized service provider. • Use the service processor reset toggle switches to reset the default password and network settings. This task requires removing the service processor card from the server. For more information, contact your next level of support.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Homologation statement

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

Accessibility features for IBM Power Systems servers

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

Overview

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

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

The IBM Power Systems servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power Systems servers.

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

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the 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.

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

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

Electronic emission notices

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.

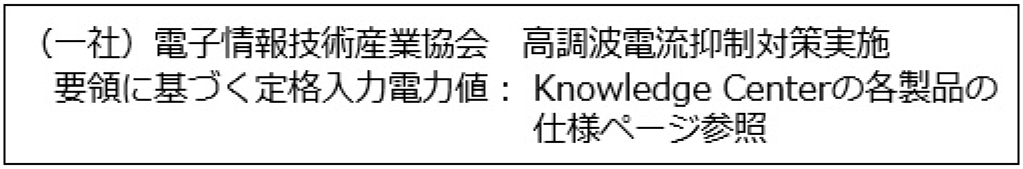
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

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:

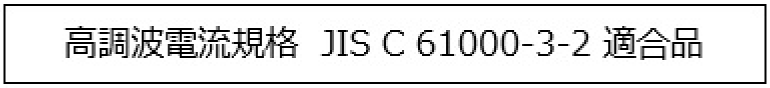
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Japan Electronics and Information Technology Industries Association (JEITA) Notice



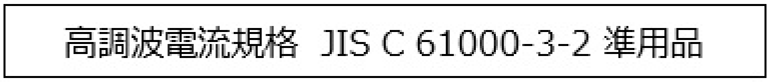
（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

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

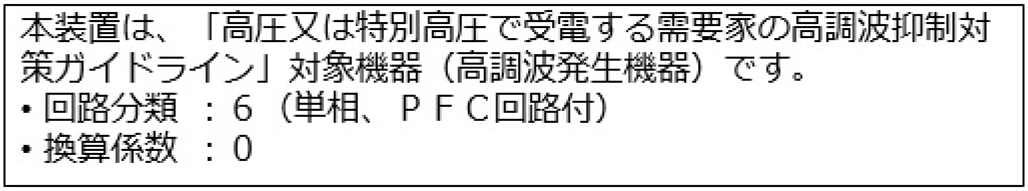


高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.



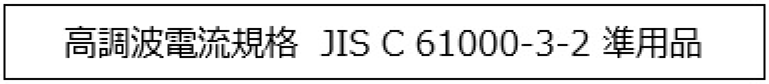
高調波電流規格 JIS C 61000-3-2 準用品



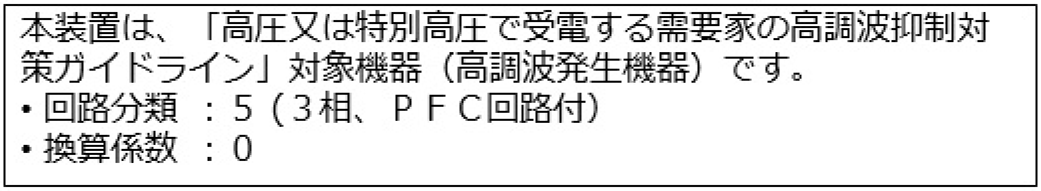
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 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.



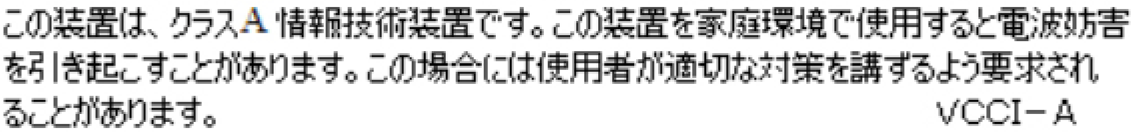
高調波電流規格 JIS C 61000-3-2 準用品



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

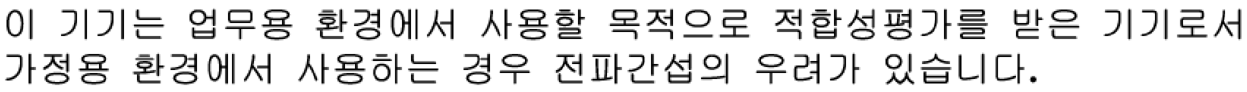
Japan Voluntary Control Council for Interference (VCCI) Notice



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。

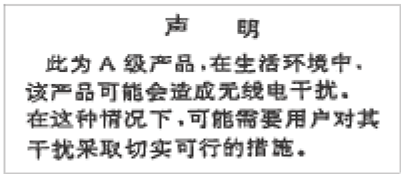
VCCI－A

Korea Notice



이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서
가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

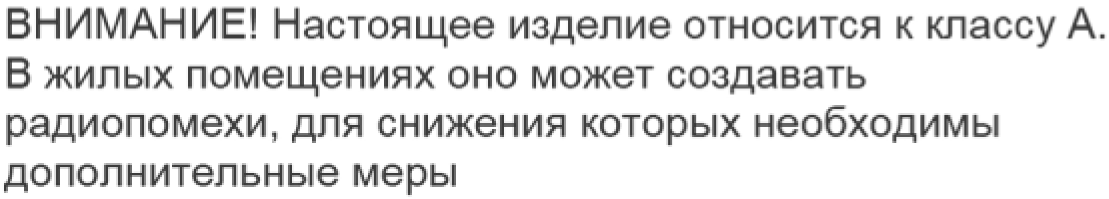
People's Republic of China Notice



声　明

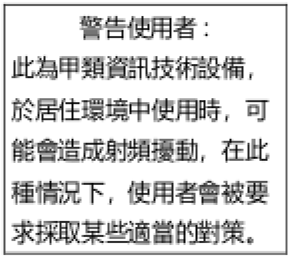
此为 A 级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Russia Notice



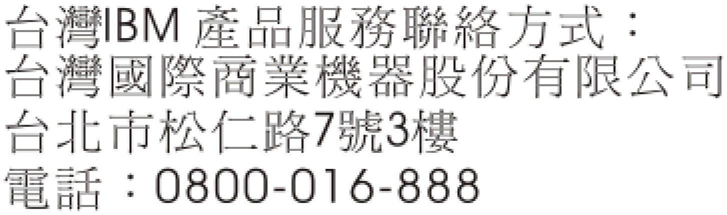
ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

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

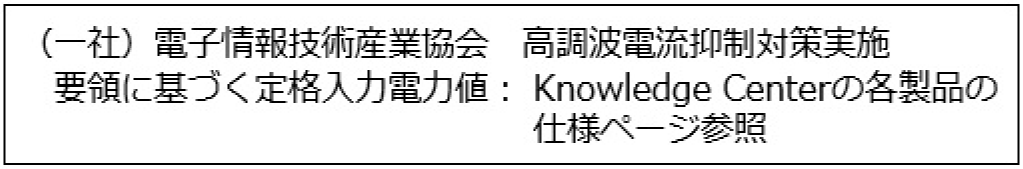
Armonk, New York 10504
Tel: 914-499-1900

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:

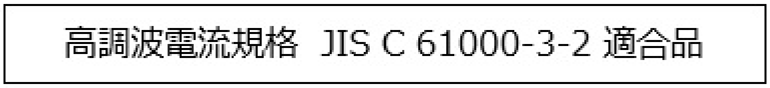
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B

Japan Electronics and Information Technology Industries Association (JEITA) Notice



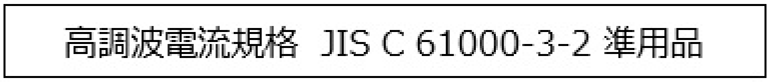
（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

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

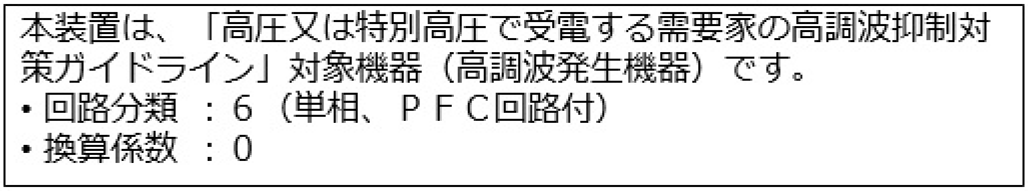


高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.



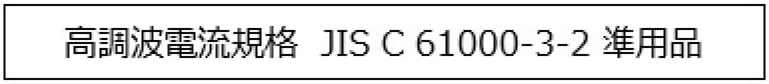
高調波電流規格 JIS C 61000-3-2 準用品



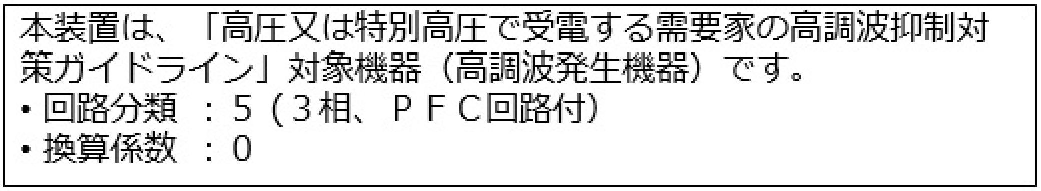
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 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.



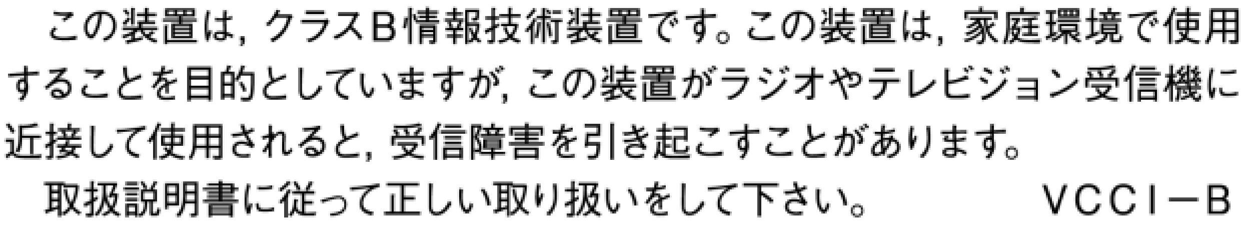
高調波電流規格 JIS C 61000-3-2 準用品



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

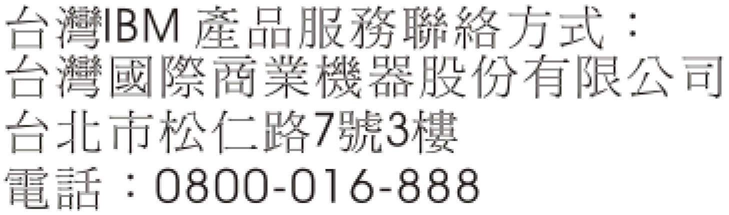
Japan Voluntary Control Council for Interference (VCCI) Notice



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.

IBM®