Power Systems

Diagnostics and service aids

IBM

Power Systems

Diagnostics and service aids

IBM

Note

Before using this information and the product it supports, read the information in “Safety notices” on page v, “Notices” on page 33, 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 POWER7 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:

- **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.**
- **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.**
- **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.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **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. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **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. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**

  (D005)

DANGER

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

- **Heavy equipment–personal injury or equipment damage might result if mishandled.**
- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices.**
- **Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet 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.**

CAUTION

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

(R001)

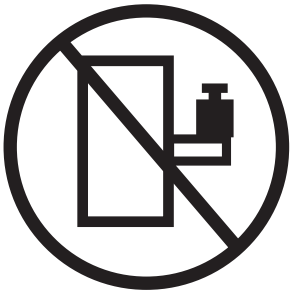
CAUTION:
Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building:

- **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 no empty U-levels between devices installed in the rack cabinet below the 32U level.**
- **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
- **Inspect the route that you plan to take to eliminate potential hazards.**
- **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.**
- **Verify that all door openings are at least 760 x 230 mm (30 x 80 in.).**
- **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
- **Ensure that the four leveling pads are raised to their highest position.**
- **Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.**
- **Do not use a ramp inclined at more than 10 degrees.**
- **When the rack cabinet is in the new location, complete the following steps:**
  - **Lower the four leveling pads.**
  - **Install stabilizer brackets on the rack cabinet.**
  - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**
- **If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.**

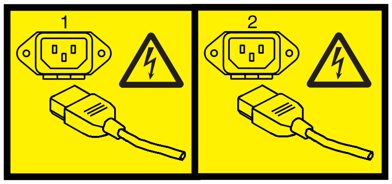
(R002)

(L001)

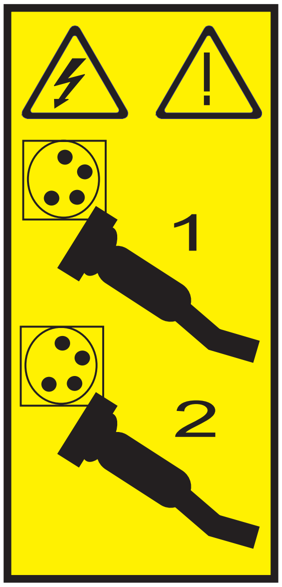
(L002)



(L003)



or



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

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

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

(C026)

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

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

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

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

Do Not:

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

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

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.

Diagnostics and service aids

For systems running the Linux operating system, the diagnostics and service aids are available on a CD that is included with the system unit hardware. These hardware diagnostics are known as stand-alone diagnostics. The stand-alone diagnostics can be booted from the CD or if there is no CD drive available, the diagnostics also can be loaded from a Network Installation Management (NIM) server.

General diagnostic information

Use the general diagnostic information to view logs, to run tests, and to use diagnostic service utilities that can help a service provider.

For more information about working with Linux, see the Linux Information Center.

Firmware and microcode

There are several types of firmware that are used by the system:
- Power subsystem firmware (if applicable)
- Service power control network (SPCN) firmware (if applicable)
- Service processor firmware (if applicable)
- System firmware

The following types of microcode are used by the system:
- Adapter microcode
- Device microcode

If a management console is attached to the server, the management console must be used to manage the firmware and microcode levels on the server.

If a management console is not attached to the server, diagnostic tasks can be used to display device and adapter microcode levels. The tasks can also be used to update device and adapter microcode. Diagnostic tasks also provide the capability to update firmware.

To determine the level of server firmware, and device and adapter microcode, use the Display Microcode Level task in diagnostic service aids. This task presents a list of resources that are currently installed and supported by this task. You then select the resource whose microcode level you with to check. For more information, see Display Microcode Level. For adapters and devices not supported by this task, refer to the instructions provided by the manufacturer to determine the microcode levels.

Use the Update and manage system flash task to update firmware on the server. When the flash update is complete, the server automatically reboots. See “Updates” on page 4 for detailed scenarios that explain how to use the update and manage system flash task.

If your system is running the Linux operating system, you can use the service aids in the stand-alone diagnostics to update most system flash, adapter, and device microcode.

CEREADME file

A CEREADME (CE readme file) is available on all diagnostic media. This file might contain information such as:

- Errata information for the service information
- Service hints for problems

- Diagnostic information that might not be included in service information
- Other pertinent (release-specific) information

The CEREADME file is helpful in describing differences in diagnostics between the current version and the preceding version.

You can view the CEREADME file by using the Service Hints service aid after the diagnostics are loaded. Also, you can read the file directly from the disk using the **pg** command to display `/usr/lpp/diagnostics/CEREADME`. The CEREADME file can be copied or printed using the normal commands. For information about using the service hints, see Display Service Hints.

Print the CEREADME file from disk

You can print the CEREADME file from disk using the **cat** command. The path to this file is as follows: `/usr/lpp/diagnostics/CEREADME`

A copy of this file should be printed and stored with the Service Information. **lp0** is normally the printer attached to the parallel port. If a printer is attached to the parallel port and is considered as **lp0**, the command for printing the file is as follows:

```
cat /usr/lpp/diagnostics/CEREADME > /dev/lp0
```

Print the CEREADME file from a source other than disk

The CEREADME file cannot be printed while diagnostics are being run from a source other than from the disk. The file can be printed on a system when the operating system is running in a normal user environment. The procedure involves copying the file from the diagnostic media to a temporary file on disk, printing the file, and then deleting the file from disk. Check for directory `/tmp/diag`. To determine whether this directory exists, enter:

```
cd /tmp/diag
```

If the directory does not exist, the message `/tmp/diag: not found` displays. *Do not* attempt to print the CEREADME file if this message is not displayed. To print the CEREADME file, choose the appropriate section below and follow the steps listed.

Print the CEREADME file from CD-ROM

Insert the diagnostic CD-ROM disc into the CD-ROM drive, and then enter the following commands:

```
mkdir /tmp/diag
mount -o ro -v cdrfs /dev/cd0  /tmp/diag
cd /tmp/diag/usr/lpp/diagnostics
cat CEREADME > /dev/lp0
cd /tmp
unmount /dev/cd0
```

The CEREADME file prints on **lp0**, which is the printer normally attached to the parallel port. If this file is not the same as the CEREADME file on the disk, a copy of this file should be printed and stored with the Service Information.

CE login

CE login enables a user to perform operating system commands that are required to service the system without being logged in as a root user. CE login must have a role of **`RunDiagnostics`** and a primary group of **`system`**. This command enables the user to:

- Run the diagnostics including the service aids, such as hot plug tasks, certify, and format.
- Run all the operating system commands run by **system** group users.

- Configure and unconfigure devices that are not busy.

In addition, CE login can have **shutdown** group enabled to allow:
- Use of the Update System Microcode service aid.
- Use of shutdown and reboot operations.

To use CE login, ask the customer to create a unique user name and configure these characteristics for that name. After the user name is set up, you will need to obtain the user name and password from the customer to log in with these capabilities. The recommended CE login user name is **qserv**.

Diagnostic programs

This section provides overview of the various diagnostic programs.

Error log analysis

If you are running the stand-alone diagnostics, error log analysis occurs on errors logged while booting the stand-alone diagnostics CD, or while running the stand-alone diagnostics.

Enhanced FRU isolation

The diagnostics provide enhanced field replaceable unit (FRU) isolation by automatically selecting associated resources. The typical way in which diagnostics select a resource is to present a list of system resources, and you are then asked to select one. Diagnostics begin with that same type of selection.

If the diagnostic application for the selected resource detects a problem with that resource, the diagnostic controller checks for an associated resource. For example, if the test of a disk drive detects a problem, the diagnostic controller tests a sibling device on the same controller. This test determines whether the drive or the controller is failing. This extra FRU isolation is apparent when you test a resource and notice that the diagnostic controller continues to test another resource that you did not select.

Advanced diagnostics function

The advanced diagnostics function are normally used by a service representative. These diagnostics might ask you to disconnect a cable and install a wrap plug.

The advanced diagnostics run in the same modes as the diagnostics used for normal hardware problem determination. The advanced diagnostics provide additional testing by allowing the service representative to do the following tasks:
- Use wrap plugs for testing.
- Loop on a test (not available in concurrent mode) and display the results of the testing.

Task and service aid functions

If a device does not show in the test list, or a diagnostic package is not loaded for a device, check it by using the display configuration and resource list task. If the device you want to test has a plus (+) sign or a minus (-) sign preceding its name, the diagnostic package is loaded. If the device has an asterisk (*) preceding its name, the diagnostic package for the device is not loaded or is not available.

Tasks and service aids provide a means to display data, check media, and check functions without being directed by the hardware problem determination procedure. For more information about tasks and service aids, see “Tasks and service aids” on page 13.

System checkout

The system checkout program uses the configuration list generated by the configuration procedure to determine which devices and features to test. These tests run without interaction. To use system checkout, select **All Resources** on the resource selection menu.

Missing resource description

In diagnostics version earlier than 5.2.0, missing devices are presented on a missing resource screen. This happens as a result or running **diag -a** or by booting online diagnostics in service mode.

In diagnostics version 5.2.0 and later, missing devices are identified on the diagnostic selection screen by an uppercase M preceding the name of the device that is missing. The diagnostic selection menu is displayed anytime you run the diagnostic routines or the advanced diagnostics routines. The diagnostic selection menu can also be entered by running **diag -a** when there are missing devices or missing paths to a device.

When a missing device is selected for processing, the missing resource menu checks several items. It checks whether the device is turned off, removed from the system, moved to a different physical location, or if it is still present.

When a single device is missing, the fault is probably with that device. When multiple devices with a common parent are missing, the fault is most likely related to a problem with the parent device.

The diagnostic procedure might include testing the parent of the device, analyzing which devices are missing, and any manual procedures that are required to isolate the problem.

Missing path resolution for MPIO resources

Diagnostics also identifies a multipath I/O device that has multiple configured paths, all of which are missing as a missing device. If some, but not all, paths to a multipath I/O device are missing, then diagnostics identifies those paths as missing. In such an instance, an uppercase P displays in front of the multipath I/O device.

When a device with missing paths is selected from the **diagnostic selection** menu, the **missing path selection** menu displays showing the missing paths for the device. The menu requests the user to select a missing path for processing. If the device has only one missing path, then the selection menu is bypassed. In either case, a menu is displayed showing the selected missing path and other available paths to the device (which might be missing or available). Use the menu to check whether the missing path has been removed, has not been removed, or should be ignored. The procedures are as follows:

- If the **Path Has Been Removed** option is selected, diagnostics removes the path from the data base.
- If the **Path Has Not Been Removed** option is selected, diagnostics determines why the path is missing.
- If the **Run Diagnostics on the Selected Device** option is selected, diagnostics runs on the device and does not change the system configuration.

Updates

Learn about obtaining machine code updates for your management console, server firmware, I/O adapter and device, as well as operating system updates.

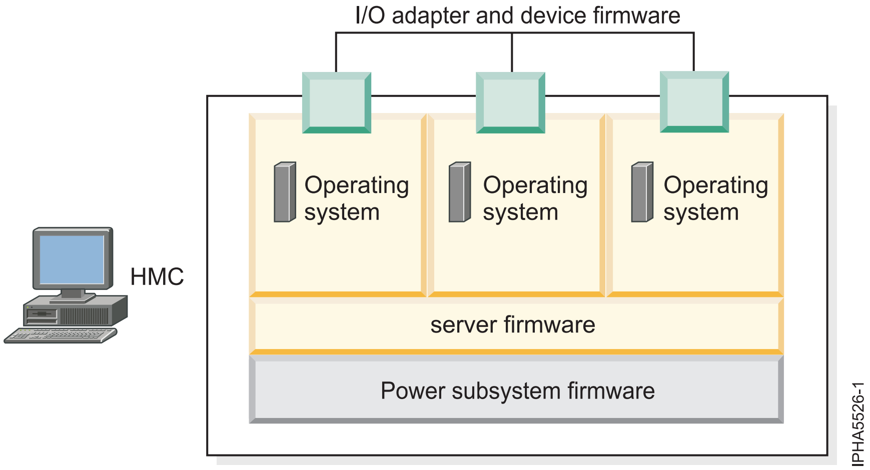
Updates provide changes to your software, Licensed Internal Code, or machine code that fix known problems, add new function, and keep your server or management console operating efficiently. For example, you might install updates for your operating system in the form of a program temporary fix (PTF). Or, you might install a server firmware update with code changes that are needed to support new hardware or new functions of the existing hardware.

A good update strategy is an important part of maintaining and managing your server. If you have a dynamic environment that changes frequently, install updates on a regular basis. If you have a stable environment, you do not have to install updates as frequently. However, you should consider installing updates whenever you make any major software or hardware changes in your environment.

You can get updates using various methods, depending on your service environment. For example, if you use an HMC to manage your server, you can use the HMC interface to download, install, and manage your HMC and firmware updates. If you do not use an HMC to manage your server, you can use the functions specific to your operating system to get your updates. In addition, you can download or order many updates through Internet websites.

You must manage several types of updates to maintain your hardware. The following figure shows the different types of hardware and software that might require updates.

Figure 1. This diagram shows the hardware and software that might require updates.



HMC user interface

Learn about the Hardware Management Console (HMC) graphical user interface.

The HMC provides a menu (also called the *context* menu) for quick access to menu choices. The menu lists the actions found in the Selected and Object menus for the current object or objects.

The user interface provided with the Hardware Management Console (HMC) uses navigation that provides hierarchical views of system resources and tasks. This user interface is made up of several major components: the banner, the navigation pane, the work pane, the task bar, and the status bar. The following sections describe each of these components.

System fault indicator and system identify indicator

Some systems support the system identify indicator and, or the system fault indicator.

The system identify indicator is used to help physically identify a particular system in a room. The system fault indicator is used to help physically identify a particular system that has a fault condition.

On a system that supports system fault indicator, the indicator is set to fault condition when a fault is detected. After the problem with the system is fixed, the system fault indicator must be set back to normal. This is done by using the log repair action task.

Note: This action keeps the system fault indicator from being set to the fault state due to a previous error, that has already been serviced, in the error log.

Both of these indicator functions can be managed by using the system identify indicator and system fault indicator tasks. For more information, see System Fault Indicator or System Identify Indicator.

Array bit steering

An advanced feature of many systems is array bit steering. The processors in these systems have internal cache arrays with extra memory capacity that can be configured to correct certain types of array faults.

This reconfiguration can be used to correct arrays for faults detected at IPL or run time. If a fault is detected during run time, the recoverable fault is reported with a `Repair Disposition Pending Reboot` indicator set. This setting allows diagnostics to callout a service request number that identifies the array and directs the service representative to a MAP for problem resolution that uses array bit steering. If the array bit steering cannot be used for the reported fault, then the FRU with that array is replaced.

Enhanced I/O error handling

Enhanced I/O Error Handling (EEH) is an error recovery strategy for errors that can occur during I/O operations on the PCI bus. Not all systems support EEH; if you get an SRN involving an EEH error, follow the action listed.

Preparing to run the stand-alone hardware diagnostics

Use these tools to diagnose hardware problems on your system that is running the Linux operating system.

Use these diagnostics only if you are directed from another procedure or directed by your next level of support or your hardware service provider.

Diagnostic service aids are available for systems that are running the Linux operating system which can help you perform hardware analysis. If a problem is found, you might receive a service request number (SRN) that can help you pinpoint the problem and determine a corrective action.

You can run stand-alone hardware diagnostics from CD or from a NIM server. Additionally, various service aids in the diagnostics can help you with service tasks.

You can also verify a repair by using the diagnostics. To verify a repair in Linux, see Verify a repair in Linux.

Running the stand-alone hardware diagnostics

The stand-alone hardware diagnostics can be run from CD or a NIM server. Use this procedure when directed from another procedure or by your next level of support.

Running stand-alone diagnostics from CD on a server without a management console attached

Learn how to run the stand-alone diagnostics on a system that does not have a management console attached.

When preparing to run the stand-alone diagnostics from a CD perform the following procedure:

1. Choose from the following options:
   - If the system is powered on, continue with step 2 on page 7.
   - If the system is powered off, continue with step 3 on page 7.

2. If the system is powered on, perform these steps:
   a. Let the system administrator and system users know that the system unit will be shut down.
   b. Stop all programs including the operating system. For details, see Powering on and powering off a system.
   c. Continue with step 4.
3. If the system is powered off, perform the following steps:
   a. Start the server so you can insert the diagnostic CD into the CD drive during the next step.
   b. Continue with step 4.
4. Insert the diagnostic CD in the CD drive.
5. Restart the server.
6. Continue with "Selecting testing options when running stand-alone diagnostics without an HMC attached."

Selecting testing options when running stand-alone diagnostics without an HMC attached:

This topic contains an overview of the testing options available when using the stand-alone diagnostics CD. This overview applies to a system that is *not* connected to a hardware management console (HMC).

To view the available testing options perform the following steps in the order listed:

1. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the **5** key. The **5** key is available on the attached keyboard or the ASCII keyboard. This action initiates a service mode boot using the default service mode boot list.
2. When the Welcome screen is shown, define the following items:
   - System console
   - Language to be used
   - Type of terminal

   Note: Depending on the terminal emulator selected, the function keys (Fn) might not function. In this case, use the ESC and the number in the screen menus. For example, F3 = ESC key and the #3.
3. When the Diagnostics Operating Instructions appear, press Enter.

   Note: If you are unable to load the diagnostics to the point where the "Diagnostic Operating Instructions" display is shown, contact your next level of support or your hardware service provider.
4. From the Function Select screen, select one of the following options:
   - If you want to run diagnostics in Problem Determination mode, continue with the next step.
   - If you want to run diagnostics in Task Selection (Service Aids) mode, go to step 11 on page 8.
5. Select **Problem determination** and press Enter.
6. Check the list of resources that is displayed. Does the list of resources match what you know to be installed in your system or partition?
   - **Yes:** Continue with the next step.
   - **No:** Record any information you have about the missing resource and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary). To test the available resources, continue with the next step.
7. Select **All Resources**, or the specific resource or resources to be tested, and press the P7 (commit) key.
8. Record any error information you receive during the diagnostics, including service request numbers (SRNs) or SRCs, to report to your service provider.

9. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
10. Choose from the following options:
    - To continue testing, return to step 7 on page 7.
    - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with step 18.
11. Select **Task Selection list** and press Enter.
12. To perform one of these tasks, select the **Task Selection** option from the **Function Selection** menu. After a task is selected, a resource menu might be presented showing all resources supported by the task.
13. From the Task selection list, select the service aid task you want to perform. For example, Update and manage system flash.
14. Follow the instructions for the task selected on each menu or panel.
15. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider.
16. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
17. Choose from the following options:
    - To continue testing, return to step 13.
    - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with the next step.
18. Remove the CD from the drive.
19. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs) and any missing resources. **This ends the procedure.**

Running stand-alone diagnostics from CD on a server with a management console attached

Learn to run the stand-alone diagnostics on a system that has a management console attached.

If you have logical partitions, note the following considerations:

- When running diagnostics in a logically partitioned system, you must run diagnostics in the logical partition containing the resource or resources that you want to test.
- The device from which you are loading stand-alone diagnostics must be made available to the logical partition on which you want to run diagnostics. This action might require moving the device to the logical partition on which you want to run diagnostics. For example, the CD drive or the network adapter connected to the Network Installation Management (NIM) server.

When preparing to run the stand-alone diagnostics from a CD with a management console attached perform the following steps from the management console:

Note: If you need help with any of these steps, contact your system operator.

1. Remove all tapes, diskettes, CDs, or DVDs, and insert the diagnostic CD into the CD drive on the managed system (not the CD drive on the management console).
2. Shut down the operating system from the management console by performing the following steps:

   For HMC:

   a. In the navigation area, select **Systems Management** > **Servers**.
   b. In the contents pane, expand the server that contains the partition you want to test and use the check box to select a server on the right pane.
   c. From the tasks menu, select **Console Window** > **Open Terminal Window**.
   d. In the VTerm window, log in as root user and enter any requested passwords.
   e. Shut down the operating system using one of the following commands:

- If Linux is running, type the `shutdown -h now` command

f. Close the VTerm window.

For SDMC:

a. Go to the **Resources** tab and click **Hosts**.

b. In the contents pane, expand the server that contains the partition you want to test and use the check box to select a server on the right pane.

c. From the **Actions** menu, select **Operations** > **Console Window** > **Open Terminal Window**.

d. In the VTerm window, log in as root user and enter any requested passwords.

e. Shut down the operating system using one of the following commands:

- If Linux is running, type the `shutdown -h now` command

f. Close the VTerm window.

3. Activate the server partition.

   For HMC: From the **Tasks** menu, select **Operations** > **Activate**.

   For SDMC: From the **Actions** menu, select **Operations** > **Activate** > **Current configuration** or **Profile**.
4. Ensure the **Open a terminal window or console session box** is selected and click **OK**.
5. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the **5** key. The **5** key is available on the attached keyboard or the ASCII keyboard. This action initiates a service mode boot using the default service mode boot list.
6. Continue with “Selecting testing options when running stand-alone diagnostics with an HMC attached.”

Selecting testing options when running stand-alone diagnostics with an HMC attached:

Contains an overview of the testing options available when using the stand-alone diagnostics CD on a system that is connected to a Hardware Management Console (HMC).

To view the available testing options perform the following steps in the order listed:

1. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the **5** key. The **5** key is available on the attached keyboard or the ASCII keyboard. This action initiates a service mode boot using the default service mode boot list.
2. When the Welcome screen is shown, define the following items:
   - System console
   - Language to be used
   - Type of terminal

     Note: Depending on the terminal emulator selected, the function keys (Fn) might not function. In this case, use the ESC and the number in the screen menus. For example, F3 = ESC key and the #3.
3. When the Diagnostics Operating Instructions appear, press Enter.

   Note: If you are unable to load the diagnostics to the point where the "Diagnostic Operating Instructions" display is shown, contact your next level of support or your hardware service provider.
4. From the Function Select screen, select one of the following options:
   - If you want to run diagnostics in Problem Determination mode, continue with the next step.
   - If you want to run diagnostics in Task Selection (Service Aids) mode, go to step 11 on page 10.
5. Select **Problem determination** and press Enter.
6. Check the list of resources that is displayed. Does the list of resources match what you know to be installed in your system or partition?

- **Yes:** Continue with the next step.
- **No:** Record any information you have about the missing resource and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary). To test the available resources, continue with the next step.

7. Select **All Resources**, or the specific resource or resources to be tested, and press the P7 (commit) key.
8. Record any error information you receive during the diagnostics, including service request numbers (SRNs) or SRCs, to report to your service provider.
9. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
10. Choose from the following options:
    - To continue testing, return to step 7.
    - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with step 18.
11. Select **Task Selection list** and press Enter.
12. To perform one of these tasks, select the **Task Selection** option from the **Function Selection** menu. After a task is selected, a resource menu might be presented showing all resources supported by the task.
13. From the Task selection list, select the service aid task you want to perform. For example, Update and manage system flash.
14. Follow the instructions for the task selected on each menu or panel.
15. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider.
16. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
17. Choose from the following options:
    - To continue testing, return to step 13.
    - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with the next step.
18. Remove the CD from the drive.
19. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs) and any missing resources. **This ends the procedure.**

Running stand-alone diagnostics from a Network Installation Management server

Learn how to run the stand-alone diagnostics from a Network Installation Manager (NIM) server.

The stand-alone diagnostics can help you perform hardware analysis. If a problem is found, you will receive a service request number (SRN) that can help pinpoint the problem and determine a corrective action.

A client system connected to a network with a NIM server can boot stand-alone diagnostics from the NIM server if the client-specific settings on both the NIM server and client are correctly configured.

Notes:

1. For NIM clients that have adapters that would normally require that supplemental media be installed when stand-alone diagnostics are run from CD, the support code for these adapters must be installed into the directory pointed to by the NIM SPOT from which you want to boot that client. Before running stand-alone diagnostics on these clients from the NIM server, the NIM server system administrator must ensure that any needed support for these devices is installed on the server.
2. All operations to configure the NIM server require root user authority.

3. If you replace the network adapter in the client, the network adapter hardware address settings for the client must be updated on the NIM server.
4. The **Cstate** for each stand-alone diagnostics client on the NIM server should be kept in the *diagnostic boot has been enabled* state.
5. On the client system, the NIM server network adapter should be put in the bootlist after the boot disk drive. This allows the system to boot in stand-alone diagnostics from the NIM server if there is a problem booting from the disk drive. See the Multiboot section under SMS in the client system's service information about setting the bootlist.

Configuring the NIM server

See the "Advanced NIM configuration tasks" chapter of the *AIX® Installation Guide and Reference* for information about performing the following tasks:

- Registering a client on the NIM server
- Enabling a client to run diagnostics from the NIM server

To verify that the client system is registered on the NIM server and the diagnostic boot is enabled, run the command from the command line on the NIM server:

```
Isnim -a Cstate -z ClientName
```

Note: The ClientName is the name of the system on which you want to run stand-alone diagnostics.

Refer to the following table for system responses.

System response	Client status
#name:Cstate:ClientName:diagnostic boot has been enabled:	The client system is registered on the NIM server and enabled to run diagnostics from the NIM server.
#name:Cstate:ClientName:ready for a NIM operation:or #name:Cstate:ClientName:B0S installation has been enabled:	The client is registered on the NIM server but not enabled to run diagnostics from the NIM server. **Note:** If the client system is registered on the NIM server but Cstate has not been set, no data will be returned.
0042–053 Isnim: there is no NIM object named "ClientName"	The client is not registered on the NIM server.

Configuring the client and running the stand-alone diagnostics from a NIM server

Perform the following steps to run stand-alone diagnostics on a client from the NIM server:

1. Let the system administrator and system users know that the system unit might be shut down.
2. Stop all programs including the Linux operating system. For details, see Powering on and powering off the system. If you need help, contact the system administrator.
3. Remove all tapes, diskettes, and CDs.
4. Choose from the following options:
   - If you are running stand-alone diagnostics in a full system partition profile, verify with the system administrator and system users that the system unit can shut down using the shutdown command. Then power down the system.
   - If you are running on a logically partitioned system, make sure that the CD drive is available to the partition used to run stand-alone diagnostics. Verify with the system administrator and system users using that partition that all applications on that partition must be stopped, and that the partition will be restarted. Stop all programs on that partition, including the operating system.
5. Choose from the following options:
   - If you are in a full system partition, power on the system unit to run stand-alone diagnostics.

- If you are in a logically partitioned system, restart the partition to run stand-alone diagnostics.

6. When the keyboard indicator is displayed (the word *keyboard* on a management console virtual terminal window or the keyboard icon on a graphical display) press the number 1 key on the keyboard to display the SMS menu.
7. Enter any requested passwords.
8. Select **Set Up Remote IPL** (Initial Program Load).
9. Enter the client address, server address, gateway address, if applicable, and subnet mask. If there is no gateway between the NIM server and the client, set the gateway address to 0.0.0.0.

   To determine whether there is a gateway, either ask the system network administrator or compare the first three octets of the NIM server address and the client address. If they are the same, (for example, if the NIM server address is 9.3.126.16 and the client address is 9.3.126.42, the first three octets (9.3.126) are the same), then set the gateway address in the RIPL field to 0.0.0.0.

   Note: The RIPL is located under the Utility menu in system management services (SMS). Refer to it for information about setting these parameters.
10. If the NIM server is set up to allow pinging from the client system, use the ping utility in the RIPL utility to verify that the client system can ping the NIM server.
11. Under the ping utility, choose the network adapter that provides the attachment to the NIM server to do the ping operation. If the ping returns with an OK prompt, the client is prepared to boot from the NIM server. If ping returns with a FAILED prompt, the client cannot proceed with the NIM boot.

    Note: If the ping fails, see the Boot problems and concerns information. Then follow the steps for network boot problems.
12. Exit the SMS Main screen.
13. Select **Select Boot Options** > **Install or Boot a Device** > **Network**.
14. Record the current bootlist settings. You will need to set the bootlist back to the original settings after running diagnostics from the NIM server.
15. Change the bootlist so the network adapter attached to the NIM is first in the bootlist.
16. Set the network parameters for the adapter from which you want to boot.
17. Exit completely from SMS. The system will start loading packets while doing a bootp from the network.
18. Follow the on-screen instructions.
    - If Diagnostic Operating Instructions Version x.x.x displays, stand-alone diagnostics have installed successfully.
    - If the operating system login prompt displays, stand-alone diagnostics did not load. Continue with step 19.
19. If the diagnostics did not load, check the following items:
    - The bootlist on the client might be incorrect.
    - Cstate on the NIM server might be incorrect.
    - Network problems might be preventing you from connecting to the NIM server.
    - Verify the settings and the status of the network. If you continue to have problems, see the Boot problems/concerns section for the system unit. Then follow the steps for network boot problems.
20. After running diagnostics, restart the system and use SMS to change the IP settings and bootlist sequence back to the original settings.

Tasks and service aids

The diagnostic package contains programs called *tasks and service aids*. Tasks and service aids are used to have the diagnostics perform specific functions on resources contained in a system.

Notes:

1. The specific tasks available depend on the hardware attributes or capabilities of the system you are servicing. Not all service aids nor tasks are available on all systems.
2. If the system is running on a logically partitioned system, the following tasks can be run only in a partition with service authority:
   - Configure scan dump policy
   - Enable platform automatic power restart
   - Configure platform processor diagnostics

For more information about Linux tasks and service aids, see the Service Aids topic in the Linux Information Center.

To perform these tasks, use the **Task Selection** option from the FUNCTION SELECTION menu.

After a task is selected, a resource menu might be displayed showing all resources supported by the task.

Add resources to the resource list

Use this task to add resources back to the resource list.

Note: Only resources that were previously detected by the diagnostics and deleted from the diagnostic test list are listed. If no resources are available to be added, then none are listed.

Back up and restore media

This service aid allows verification of backup media and devices. It presents a menu of tape and diskette devices available for testing and prompts for selecting the wanted device. It then presents a menu of available backup formats and prompts for selecting the wanted format. The supported formats are **tar**, **backup**, and **cpio**. After the device and format are selected, the service aid backs up a known file to the selected device, restores that file to `/tmp`, and compares the original file to the restored file. The restored file remains in `/tmp` to allow for visual comparison. All errors are reported.

Certify media

This task allows the selection of diskette, DVD-RAM media, or hard files to be certified. Normally, this task is done under the following conditions:

- To determine the condition of the drive and media
- To verify that the media is error-free after a format service aid is run on the media

Normally, run Certify if after running diagnostics on a drive and its media, no problem is found, but you suspect that a problem still exists.

Hard files can be connected either to a SCSI adapter (non-RAID) or a PCI SCSI RAID adapter. The usage and criteria for a hard file connected to a non-RAID SCSI adapter are different from the usage and criteria for a hard file connected to a PCI SCSI RAID adapter.

Certify media can be used with the following options:

Certify Diskette

Use this selection to verify the data written on a diskette. When you select this service aid, the menu prompts you for a diskette type that you want to verify. The program then reads all of the ID and data fields on the diskette one time and displays the total number of bad sectors found.

Certify DVD-RAM media

This selection reads all of the ID and data fields. It checks for bad data and counts all errors encountered. If an unrecovered data error occurs, the data on the media must be transferred to another media and the original media must be discarded. If an unrecovered equipment error occurs or recovered errors exceed the threshold value, the original media must be discarded.

The certify service aid displays the following information:

- Capacity in bytes
- Number of data errors recovered
- Number of data errors not recovered
- Number of equipment check errors
- Number of equipment checks not recovered

If the drive is reset during a certify operation, the operation is restarted.

If the drive is reset again, the certify operation is terminated, and you are asked to run diagnostics on the drive.

Certify Hard file Attached to a Non-RAID and PCI-X RAID SCSI adapter

For pdisks and hdisks, this selection reads all of the ID and data fields on the hard file. If bad-data errors are encountered, the certify operation counts the errors.

If there are non-recovered data errors that do not exceed the threshold value, do one of the following tasks:

For hdisk hard files, format the hard file and certify again.

For pdisk hard files, run diagnostics on the parent adapter.

If the non-recovered data errors, recovered data errors, recovered and non-recovered equipment errors exceed the threshold values, the hard file must be replaced.

After the read certify of the disk surface completes for hdisk hard files, the certify operation performs 2000 random-seek operations. Errors are also counted during the random-seek operations. If a disk timeout occurs before the random seeks are finished, the disk needs to be replaced.

The Certify service aid displays the following information:

- For hdisks:
  - Drive capacity in megabytes.
  - Number of data errors recovered.
  - Number of data errors not recovered.
  - Number of equipment checks recovered.
  - Number of equipment checks not recovered.
- For pdisks:
  - Drive capacity in megabytes.
  - Number of data errors not recovered.
  - Number of LBA reassignments
  - Number of equipment checks not recovered.

Certify Hard File Attached to a PCI SCSI RAID adapter

This selection is used to certify physical disks attached to a PCI SCSI RAID adapter. Certify reads the entire disk and checks for recovered errors, unrecovered errors, and reassigned errors. If these errors exceed the threshold values, you are prompted to replace the physical disk.

Change hardware vital product data

Use this service aid to display the display/alter VPD selection menu. The menu lists all resources installed on the system. When a resource is selected, a menu displays that lists all the VPD for that resource.

Note: The user cannot alter the VPD for a specific resource unless the VPD is not machine readable.

Configure reboot policy (CHRP)

This service aid controls how the system tries to recover when power is restored after a power outage.

Use this service aid to display and change the following settings for the reboot policy.

Configure scan dump policy

Configure scan dump policy allows the user to set or view the scan dump policy (scan dump control and size) in NVRAM. Scan dump data is a set of chip data that the service processor gathers after a system malfunction. It consists of chip scan rings, chip trace arrays, and scan COM (SCOM) registers. This data is stored in the scan-log partition in the nonvolatile random access memory (NVRAM) on the system.

Use this service aid to display and change the following settings for the scan dump policy at run time:

- Scan Dump Control (how often the dump is taken)
- Scan Dump Size (size and content of the dump)

The Scan Dump Control (SDC) settings include the following options:

As needed
This setting allows the platform firmware to determine whether a scan dump is performed. This setting is the default setting for the dump policy.

Always
This setting overrides the firmware recommendations and always performs a dump after a system failure.

The Scan Dump Size (SDS) settings include the following options:

As Requested
Dump content is determined by the platform firmware.

Minimum
Dump content collected provides the minimum debug information, enabling the platform to reboot as quickly as possible.

Optimum
Dump content collected provides a moderate amount of debug information.

Complete
Dump data provides the most complete error coverage at the expense of reboot speed.

Delete resource from resource list

Use this task to delete resources from the resource list.

Note: Only resources that were previously detected by the diagnostics and were not deleted from the diagnostic test list are listed. If no resources are available to be deleted, then none are listed.

Disk maintenance

This service aid provides the following options for the hard disk maintenance:
- Disk to Disk Copy
- Display/Alter Sector

Disk-to disk-copy

Notes:
1. This service aid cannot be used to update a drive of a different size. The service aid only supports copying from a SCSI drive to another SCSI drive of the same size.
2. Use the **migratepv** command when copying the contents to other disk drive types. This command also works when copying SCSI disk drives or when copying to a SCSI disk drive that is not the same size.

Use this selection to recover data from an old drive when replacing it with a new drive. The service aid recovers all logical volume manager (LVM) software-reassigned blocks. To prevent corrupted data from being copied to the new drive, the service aid stops if an unrecoverable read error is detected. To help prevent possible problems with the new drive, the service aid stops if the number of bad blocks to be reassigned reaches a threshold.

To use this service aid, both the old and new disks must be installed in, or attached to the system with unique SCSI addresses. The new disk drives SCSI address must be set to an address that is not currently in use, and the drive must be installed in an empty location. If there are no empty locations, then one of the other drives must be removed. When the copy is complete, only one drive can remain installed. Either remove the target drive to return to the original configuration, or perform the following procedure to complete the replacement of the old drive with the new drive:
1. Remove both drives.
2. Set the SCSI address of the new drive to the SCSI address of the old drive.
3. Install the new drive in the location of the old drive.
4. Install any other drives (that were removed) into their original location.

To prevent problems that can occur when running this service aid from disk, run this service aid from the diagnostics that are loaded from removable media when possible.

Display/alter sector

Attention: Use caution when you use this service aid. Inappropriate modification to some disk sectors can result in the total loss of all data on the disk.

This selection allows the user to display and alter information about a disk sector. Sectors are addressed by their decimal sector number. Data is displayed both in hex and in ASCII. To prevent corrupted data from being incorrectly corrected, the service aid does not display information that cannot be read correctly.

Display configuration and resource list

If a device is not included in the test list or if you think a diagnostic package for a device is not loaded, check by using the display configuration and resource list task. If the device you want to test has a plus (+) sign or a minus (-) sign preceding its name, the diagnostic package is loaded. If the device has an asterisk (*) preceding its name, the diagnostic package for the device is not loaded or is not available.

This service aid displays the item header only for all installed resources. Use this service aid when there is no need to see the vital product data (VPD). (No VPD is displayed.)

Display firmware device node information

This task displays the firmware device node information. This service aid is intended to gather more information about individual or particular devices on the system. The format of the output data might differ depending on which level of the operating system is installed.

Display hardware error report

This service aid uses the **`errpt`** command to view the hardware error log.

The display error summary and display error detail selections provide the same type of report as the `errpt` command. The display error analysis summary and display error analysis detail selections provide additional analysis.

Display hardware vital product data

This service aid displays all installed resources, along with any VPD for those resources. Use this service aid when you want to look at the VPD for a specific resource.

Display machine check error log

Note: The display machine check error log service aid is available only on stand-alone diagnostics.

When a machine check occurs, information is collected and logged in an NVRAM error log before the system unit shuts down. This information is logged in the error log and cleared from NVRAM when the system is rebooted from the hard disk, LAN, or stand-alone media. When booting from stand-alone diagnostics, this service aid converts the logged information in to a readable format that can be used to isolate the problem.

Display microcode level

Note: Display microcode level is a subtask that can be accessed after selecting Microcode Tasks, see "Microcode tasks" on page 25.

This task provides a way to display microcode on a device or adapter. When the **sys0** resource is selected, the task displays the levels of both the system firmware and service processor firmware. **sys0** might not be available in all cases.

Display service hints

This service aid reads and displays the information in the CEREADME file from the diagnostics media. This file contains information that is not contained in the publications for this version of the diagnostics. The file also contains information about using this particular version of diagnostics.

Display test patterns

This service aid provides a means of adjusting system display units by providing test patterns that can be displayed. The user uses a series of menus to select the display type and test pattern. After the selections are made, the test pattern displays.

Display USB devices

The following are the main functions of this service aid:

- Display a list of USB controllers on an adapter.
- Display a list of USB devices that are connected to the selected controller.

To run the USB devices service aid, go to the diagnostics TASKS SELECTION menu, and select **Display USB Devices**. From the controller list that displayed on the screen, select one of the items that begins with "OHCDX", where "X" is a number. A list of devices attached to the controller displays.

Download microcode

Note: Download microcode is a subtask that can be accessed after selecting **Microcode Tasks**, see "Microcode tasks" on page 25.

This service aid provides a way to copy microcode to an adapter or device. The service aid presents a list of adapters and devices that use microcode. After the adapter or device is selected, the service aid provides menus to guide you in checking the current level and installing the needed microcode.

Microcode installation to adapters and devices

For many adapters and devices, microcode installation occurs and becomes effective while the adapters and devices are in use. Ensure that a current backup is available and the installation is scheduled during a non-peak production period.

Notes:

1. If the source is `/etc/microcode`, the image must be stored in the `/etc/microcode` directory on the system. If the system is booted from a NIM server, the image must be stored in the `usr/lib/microcode` directory of the SPOT the client is booted from.
2. If the source is CD (cdX), the CD must be in ISO 9660 format. There are no restrictions as to what directory in which to store the image.
3. If the source is diskette (fdX), the diskette must be in backup format and the image stored in the `/etc/microcode` directory.

Microcode installation to an SES device

Notes:

1. If the source is `/etc/microcode`, the image must be stored in the `/etc/microcode` directory on the system. If the system is booted from a NIM server, the image must be stored in the `usr/lib/microcode` directory of the SPOT the client is booted from.
2. If the source is CD (cdX), the CD must be in ISO 9660 format. There are no restrictions as to what directory to store the image.
3. If the source is diskette (fdX), the diskette must be in backup format and the image stored in the `/etc/microcode` directory.

Microcode installation to PCI SCSI RAID adapters

PCI SCSI RAID adapters that support this type of installation are:

- Type 4-H, PCI SCSI-2 Fast/Wide RAID adapter (Feature Code 2493)
- Type 4-T, PCI 3-Channel Ultra2 SCSI RAID adapter (Feature Code 2494)
- Type 4-X, PCI 4-Channel Ultra3 SCSI RAID adapter (Feature Code 2498)

Notes:

1. If the image is on the hard disk drive, it must be stored in the `/etc/microcode` directory on the system. If the system is booted from a NIM server, the image must be stored in the `usr/lib/microcode` directory of the SPOT the client is booted from.
2. If the image is on a diskette, the diskette must be in backup format and the image stored in the `/etc/microcode` directory.

Microcode installation to disk drive attached to PCI SCSI RAID adapters

Microcode for a disk drive attached to a PCI SCSI RAID adapter is installed through the adapter to the drive. PCI SCSI RAID adapters that support this type of installation are:

- Type 4-H, PCI SCSI-2 Fast/Wide RAID adapter (Feature Code 2493)
- Type 4-T, PCI 3-Channel Ultra2 SCSI RAID adapter (Feature Code 2494)
- Type 4-X, PCI 4-Channel Ultra3 SCSI RAID adapter (Feature Code 2498)

Notes:

1. If the image is on the hard disk drive, it must be stored in the `/etc/microcode` directory on the system. If the system is booted from a NIM server, the image must be stored in the usr/lib/microcode directory of the SPOT the client is booted from.
2. If the image is on a diskette, the diskette must be in backup format and the image stored in the `/etc/microcode` directory.

Fibre Channel RAID service aids

The Fibre Channel RAID service aids contain the following functions:

Certify LUN
This selection reads and checks each block of data in the logical unit number (LUN). If excessive errors are encountered, you are notified.

Certify spare physical disk
This selection certifies (check integrity of the data) drives that are designated as spares.

Format physical disk
This selection formats a selected disk drive.

Array controller microcode download
This selection updates the microcode on the Fibre Channel RAID controller when required.

Physical disk microcode download
This selection updates the microcode on any of the disk drives in the array.

Update EEPROM
This selection updates the contents of the electronically erasable programmable read-only memory (EEPROM) on a selected controller.

Replace controller
Use this selection when it is necessary to replace a controller in the array.

Flash drive (USB)

Use this command to update microcode images or boot images for stand-alone diagnostics from a flash memory device.

You must first load an ISO9660 or later image onto a supported USB flash drive. You are prompted to connect a flash drive, select a flash drive from a list of available flash drives, and select a source ISO image. The source image might be on the file system or on removable media.

This service aid is also used to copy the contents of optical media and other flash drives to a flash drive.

Flash SK-NET FDDI firmware

This task allows the flash firmware on the SysKonnect SK-NET FDDI adapter to be updated.

Format media

This task allows the selection of diskettes, hard disks, or optical media to be formatted.

Hard disk attached to SCSI adapter (non-RAID)

This service aid includes the following options:

Hard disk format
Writes all of the disk. The pattern written on the disk is device-dependent; for example some drives might write all zeros, while some might write the hexadecimal number 5F. No bad block reassignment occurs.

Hard disk Format and Certify
Performs the same function as hard disk format. After the format is completed, Certify is run. Certify then reassigns all bad blocks encountered.

Hard disk Erase Disk
This option can be used to overwrite (remove) all data currently stored in user-accessible blocks of the disk. The erase disk option writes one or more patterns to the disk. An additional option allows data in a selectable block to be read and displayed on the system console.

To use the erase disk option, specify the number (0-3) of patterns to be written. The patterns are written serially; that is, the first pattern is written to all blocks. The next pattern is written to all blocks, overlaying the previous pattern. A random pattern is written by selecting the `Write Random Pattern?` option.

Note: The erase disk service aid is not certified as meeting the Department of Defense or any other security organization guidelines.

To overwrite the data on the drive, use the following steps:

1. Select **Erase Disk**.
2. Do a format without certify.
3. Select **Erase Disk** to run it a second time.

For a newly installed drive, you can ensure that all blocks on the drive are overwritten with your pattern by using the following procedure:

1. Format the drive.
2. Check the defect MAP by running the erase disk option.

   Note: If you use the format and certify option, there might be some blocks which get placed into the grown defect MAP.
3. If there are bad blocks in the defect MAP, record the information presented and ensure that this information is kept with the drive. This data is used later when the drive is to be overwritten.
4. Use the drive as you would normally.
5. When the drive is no longer needed and is to be erased, run the same version of the erase disk option which was used in step 2.

   Note: Using the same version of the service aid is only critical if any bad blocks were found in step 3.
6. Compare the bad blocks which were recorded for the drive in step 3 with the bad blocks that now appear in the grown defect MAP.

Note: If there are differences between the saved data and the newly obtained data, all sectors on this drive cannot be overwritten. The new bad blocks are not overwritten.

7. If the bad block list is the same, continue running the service aid to overwrite the disk with the chosen pattern or patterns.

Optical media

Use the following functions to check and verify optical media:

Optical Media Initialize
Formats the media without certifying. This function does not reassign the defective blocks or erase the data on the media. This option provides a quick way of formatting the media and cleaning the disk.

Note: It takes approximately 1 minute to format the media.

Optical Media Format and Certify
Formats and certifies the media. This function reassigns the defective blocks and erases all data on the media.

DVD-RAM media

Initialize
Formats the media without certifying. This function does not reassign the defective blocks or erase the data on the media. This format type can be used only with previously formatted media.

Format and Certify
Formats and certifies the media. This function reassigns the defective blocks and erases the data on the media by writing an initialization pattern to the entire media.

Diskette format

This selection formats a diskette by writing patterns to it.

Generic microcode download

Note: Generic microcode download is a subtask that can be accessed after selecting **Microcode Tasks**, see “Microcode tasks” on page 25.

The generic microcode download service aid provides a means of executing a genucode script from a diskette or tape. The purpose of this generic script is to load microcode to a supported resource.

The genucode program must be downloaded onto diskette or tape in the **tar** format. The microcode image itself goes onto another one in **restore** format. Running the generic microcode download task searches for the genucode script on diskette or tape and runs it. You will be prompted to insert a genucode media into the drive. The service aid moves the genucode script file to the `/tmp` directory and runs the program that downloads the microcode to the adapter or device.

This service aid is supported in stand-alone mode from disk, LAN, or loadable media.

Hot plug task

Attention: Some systems do not support hot pluggable procedures. These systems must be shut down and powered off before replacing any PCI adapter or device. Follow the non-hot pluggable adapter or device procedures when replacing a PCI adapter or device on any of these systems.

The hot plug task provides software function for those devices that support hot plug or hot plug capability. These devices include PCI adapters, SCSI devices, and some RAID devices. This task was previously known as "SCSI Device Identification and Removal" or "Identify and Remove Resource."

Depending on the environment and the software packages installed, selecting this task displays the following subtasks:
- PCI hot plug manager
- SCSI hot plug manager
- RAID hot plug devices

If the missing options resolution procedure runs with no menus or prompts, device configuration is complete. Select the device that has an uppercase `M` in front of it in the resource list so that missing options processing can be done on that resource.

SCSI hot plug manager

This task was previously known as SCSI Device Identification and Removal or Identify and Remove Resources. This task allows you to identify, add, remove, and replace a SCSI device in a system unit that uses a SCSI Enclosure Services (SES) device. The following functions are available:

List the SES Devices
Lists all the SCSI hot plug slots and their contents. Status information about each slot is also available. The status information available includes the slot number, device name, whether the slot is populated and configured, and location.

Identify a Device Attached to an SES Device
Identifies the location of a device attached to an SES device. This function lists all the slots that are occupied or empty which support hot plug. When a slot is selected for identification, the visual indicator for the slot is set to the Identify state.

Attach a Device to an SES Device
Lists all empty hot plug slots that are available for the insertion of a new device. After a slot is selected, the power is removed. If available, the visual indicator for the selected slot is set to the remove state. After the device is added, the visual indicator for the selected slot is set to the normal state, and power is restored.

Replace/Remove a Device Attached to an SES Device
Lists all populated hot plug slots that are available for removal or replacement of the devices. After a slot is selected, the device that is populating that slot is unconfigured; then the power is removed from that slot. If the unconfigure operation fails, it is possible that the device is in use by another application. In this case, the customer or system administrator must be notified to quiesce the device. If the unconfigure operation is successful, the visual indicator for the selected slot is set to the remove state. After the device is removed or replaced, the visual indicator, if available for the selected slot, is set to the normal state, and power is restored.

Note: Before you remove the device, be sure that no other host is using it.

Configure Added/Replaced Devices
Runs the configuration manager on the parent adapters that had child devices added or removed. This function ensures that the devices in the configuration database are configured correctly.

The stand-alone diagnostics have restrictions on using the SCSI hot plug manager. For example:
- Devices being used as replacement devices must be the same type of device as the device that is being replaced.
- New devices cannot be added unless a device of the same FRU part number exists in the system. This rule is because the configuration information for the new device is not known after the stand-alone diagnostics are booted.

SCSI and SCSI RAID hot plug manager

This task was previously called "SCSI hot-swap manager", "SCSI device identification and removal", or "Identify and remove resources". This task allows the user to identify, add, remove, and replace a SCSI device in a system unit that uses a SCSI hot plug enclosure device. This task also performs these functions on a SCSI RAID device attached to a PCI-X RAID controller. The following functions are available:

List the SCSI hot plug enclosure devices
Lists all the SCSI hot plug slots and their contents. Status information about each slot is also available. The status information available includes the slot number, device name, whether the slot is populated and configured, and location.

Identify a device attached to a SCSI hot plug enclosure device
Helps identify the location of a device attached to a SCSI hot plug enclosure device. This function lists all the slots that are occupied or empty which support hot plug. When a slot is selected for identification, the visual indicator for the slot is set to the identify state.

Attach a device to a SCSI hot plug enclosure device
Lists all empty hot plug slots that are available for the insertion of a new device. After a slot is selected, the power is removed. If available, the visual indicator for the selected slot is set to the remove state. After the device is added, the visual indicator for the selected slot is set to the normal state, and power is restored.

Replace/remove a device attached to a SCSI hot plug enclosure device
Lists all populated hot plug slots that are available for removal or replacement of the devices. After a slot is selected, the device that is populating that slot is unconfigured, the power is removed from that slot. If the unconfigure operation fails, it is possible that the device is in use by another application. In this case, the customer or system administrator must be notified to quiesce the device. If the unconfigure operation is successful, the visual indicator for the selected slot is set to the remove state. After the device is removed or replaced, the visual indicator, if available for the selected slot, is set to the normal state, and power is restored.

Note: Before you remove the device, be sure that no other host is using it.

Configure added/replaced devices
Runs the configuration manager on the parent adapters that had child devices added or removed. This function ensures that the devices in the configuration database are configured correctly.

The stand-alone diagnostics have restrictions on using the SCSI hot plug manager. For example:

- Devices being used as replacement devices must be the same type of device as the device that is being replaced
- New devices cannot be added unless a device of the same FRU part number exists in the system. This restriction is because the configuration information for the new device is not known after the stand-alone diagnostics are booted.

-a Specifies the option under the task.

-d Indicates the SCSI device.

-T Specifies the task to run.

RAID hot plug devices

This task allows the user to identify or remove a RAID device in a system unit that uses a SCSI Enclosure Services (SES) device. The following subtasks are available:

- **Normal**
- **Identify**
- **Remove**

The normal subtask is used to return a RAID hot plug device to its normal state. This subtask is used after a device is identified or replaced. This subtask lists all channel/IDs of the RAID and the status of the devices that are connected. A device in its normal state has power and the check light is off.

The identify subtask is used to identify the physical location of a device or an empty position in the RAID enclosure. This subtask lists all channel/IDs of the RAID and the status of the devices that are connected to the RAID enclosure. If a device is attached to the selected channel/ID, the check light on the device will begin to flash. If the channel/ID does not have a device attached, the light associated with the empty position on the enclosure will begin to flash.

The remove subtask is used to put the RAID hot plug device in a state where it can be removed or replaced. This subtask lists all channel/IDs of the RAID adapter that have devices that can be removed. Only devices with a status of `Failed`, `Spare`, `Warning`, or `Non Existent` can be removed. After a device is selected for removal, the check light on the device will begin to flash, indicating that you can physically remove that device.

The stand-alone diagnostics have restrictions on using the RAID hot plug manager:

- Devices being used as replacement devices must be the same type of device as the device that is being replaced.
- New devices cannot be added unless a device of the same FRU part number exists in the system. This rule is because the configuration information for the new device is not known after the stand-alone diagnostics are booted.

Identify indicators

The component and attention LEDs assist in identifying failing components in your server.

Identify and system attention indicators

This task is used to display or set the identify indicators and the single system attention indicator on the systems that support this function.

Some systems might support only the identify indicators or only the attention indicator. The identify indicators are used to help physically identify the system, enclosure, or FRU in a large equipment room. The attention indicator is used to alert a user that the system needs attention and might have a hardware problem. In most cases, when an identify indicator is set to the Identify state, this results in a flashing LED. And, when an attention indicator is set to the Attention state, this results in a solid LED.

When a hardware problem is detected on a system that supports the attention indicator, the indicator is set to an attention state. After the failure is identified, repaired, and a repair action is logged, the attention indicator is reset to the normal state.

-s {normal | identify}
Sets the state of the system identify indicator to either normal or identify.

-l *location code*
Identifies the resource by physical location code.

-d *device name*
Identifies the resource by device name

-t Displays a list of all supported identify indicators by physical location codes.

When this command is used without the **-l** or the **-d** flags, the primary enclosure resource is used.

Use the -l flag only in systems that have more than one identify indicator. Use of the -d flag is preferred over use of the -l flag.

When this command is used without the **-s** flag, the current state of the identify indicator is displayed.

Local area network analyzer

This selection is used to exercise the LAN communications adapters (token ring, Ethernet, and (FDDI) Fiber Distributed Data Interface). The following services are available:

- Connectivity testing between two network stations. Data is transferred between the two stations, requiring the user to provide the IP addresses of both stations.
- Monitoring ring (token ring only). The ring is monitored for a specified time. Soft and hard errors are analyzed.

Microcode tasks

Similar microcode tasks are combined under a single task topic, while providing a way to access the microcode and flashing features. The combined tasks that are included under Microcode tasks are:

- Display microcode level
- Download microcode
- Generic microcode download
- Update system or service processor flash
- Update and manage system flash

PCI RAID physical disk identify

For a description of the PCI RAID physical disk identify task, see SCSI RAID Physical Disk Status and Vital Product Data.

Process supplemental media

Diagnostic supplemental media contains all the necessary diagnostic programs and files required to test a particular resource. The supplemental media is normally released and shipped with the resource as indicated on the diskette label. Diagnostic supplemental media must be used when the device support has not been incorporated into the latest diagnostic CD-ROM.

This task processes the diagnostic supplemental media. Insert the supplemental media when you are prompted; then press Enter. After processing has completed, go to the resource selection list to find the resource to test.

Notes:

1. This task is supported in stand-alone diagnostics only.
2. Process and test one resource at a time. Run diagnostics after each supplemental media is processed. (For example, if you need to process two supplemental media, run diagnostics twice, once after each supplement media is processed.)

Run diagnostics

The run diagnostics task starts the resource selection list menu. When the commit key is pressed, diagnostics are run on all selected resources.

Run error log analysis

The run error log analysis task starts the resource selection list menu. When the commit key is pressed, error log analysis is run on all selected resources.

SCSI bus analyzer

Use this service aid to diagnose a SCSI bus problem in a freelance mode.

To use this service aid, you must understand how a SCSI bus works. Use this service aid when the diagnostics cannot communicate with anything on the SCSI bus and cannot isolate the problem. To find a problem on the SCSI bus with this service aid, start with a single device attached, ensure that it is working, then start adding devices and cables to the bus. After each addition, ensure that each one works. This service aid works with any valid SCSI bus configuration.

The SCSI bus service aid transmits a SCSI inquiry command to a selectable SCSI address. The service aid then waits for a response. If no response is received within a defined amount of time, the service aid displays a timeout message. If an error occurs or a response is received, the service aid then displays one of the following messages:

- `The service aid transmitted a SCSI Inquiry Command and received a valid response back without any errors being detected.`
- `The service aid transmitted a SCSI Inquiry Command and did not receive any response or error status back.`
- `The service aid transmitted a SCSI Inquiry Command and the adapter indicated a SCSI bus error.`
- `The service aid transmitted a SCSI Inquiry Command and an adapter error occurred.`
- `The service aid transmitted a SCSI Inquiry Command and a check condition occur.`

When the SCSI bus service aid is started a description of the service aid displays.

Pressing Enter displays the adapter selection menu. Use this menu to enter the address to transmit the SCSI Inquiry Command.

When the adapter is selected, the SCSI bus address selection menu displays. Use this menu to enter the address to transmit the SCSI inquiry command.

After the address is selected, the SCSI bus test run menu displays. Use this menu to transmit the SCSI inquiry command by pressing Enter. The service aid then indicates the status of the transmission. When the transmission is completed, the results of the transmission displays.

Notes:

1. A check condition can be returned when the bus or device is working correctly.
2. If the device is in use by another process, the command is not sent.

SCSI RAID physical disk status and vital product data

Note: This task was previously known as the PCI RAID physical disk identify task.

Use this service aid when you want to look at the vital product data for a specific disk attached to a RAID adapter. This service aid displays all disks that are recognized by the PCI RAID adapter, along with their status, physical location, microcode level, and other vital product data. The physical location of a disk consists of the channel number of the RAID adapter and the SCSI ID number of the position in the enclosure. The microcode level is listed next to the physical location of the disk.

SCSD tape drive service aid

Use this service aid to obtain the status or maintenance information from an SCSD tape drive. Not all models of SCSD tape drive are supported.

The service aid provides the following options:

Display time since a tape drive was last cleaned.
The time since the drive was last cleaned displays on the screen. Also, a message is shown whether it is recommended to clean the drive.

Copy a trace table for a tape drive.
The trace table of the tape drive is written to diskettes or a file. The diskettes must be formatted for DOS. Writing the trace table might require several diskettes. The actual number of diskettes is determined by the size of the trace table. Label the diskettes as follows:

TRACE*x*.DAT (where *x* is a sequential diskette number). The complete trace table consists of the sequential concatenation of all the diskette data files.

When the trace table is written to a disk file, the service aid prompts for a file name. The default name is: `/tmp/TRACE. x`, where *x* is the name of the SCSD tape drive that is being tested.

Display or copy a log sense information for a tape drive.
The service aid provides options to display the log sense information to the screen, to copy it to a DOS formatted diskette, or to copy it to a file. The file name `LOGSENSE.DAT` is used when the log sense data is written to the diskette. If you selected to have the log sense data be copied to a file, you will be prompted for a file name

Spare sector availability

This selection checks the number of spare sectors available on the optical disk. The spare sectors are used to reassign when defective sectors are encountered during normal usage or during a format and certify operation. Low availability of spare sectors indicates that the disk must be backed up and replaced. Formatting the disk does not improve the availability of spare sectors.

System fault indicator

If a failing component is detected in your system, an amber-colored attention LED on the front of the system unit is turned on solid (not flashing).

System identify indicator

To identify a system from a group of systems, an amber-colored attention LED on the front of the system unit is flashing.

Update system or service processor flash

Notes:

- Update system or service processor flash is a subtask that can be accessed after selecting **Microcode Tasks**, see “Microcode tasks” on page 25.
- This task has been replaced with the Update and manage system flash task, see “Update and manage system flash” on page 28.

Attention: If the system is running on a logically partitioned system, ask the customer or system administrator if a service partition has been designated.

- If a service partition has been designated, ask the customer or system administrator to shut down all of the partitions except the one with service authority. The firmware update can then be done by using the service aid.
- If a service partition has not been designated, the system must be shut down. If the firmware update image is available on backup diskettes or optical media, the firmware update can then be done from the service processor menus as a privileged user. If the firmware update image is in a file on the system, reboot the system in a full system partition and use the following normal firmware update procedures.

If the system is already in a full system partition, use the following normal firmware update procedures.

This selection updates the system or service processor flash. Some systems might have separate images for system and service processor firmware; newer systems have a combined image that contains both in one image.

Look for additional update and recovery instructions with the update kit. You need to know the fully qualified path and file name of the flash update image file provided in the kit. If the update image file is on a diskette or optical media, the service aid can list the files on the diskette or optical media for selection. The diskette must be a valid backup format diskette.

See the update instructions with the kit, or the service information for the system unit to determine the current level of the system unit or service processor flash memory.

When this service aid is run from the stand-alone diagnostics, the flash update image file is copied to the file system from diskette, optical media, or from the Network Installation Management (NIM) server. If you use a diskette, you must provide the image on backup format diskette because you will not have access to remote file systems or any other files that are on the system. Before you can boot diagnostics from the NIM server, you must ensure that the microcode image is copied to the `/usr/lib/microcode` directory on the NIM server. Then point to the NIM SPOT (from which you plan to have the NIM client boot stand-alone diagnostics). Next, a NIM check operation must be run on the SPOT containing the microcode image on the NIM server. After performing the NIM boot of diagnostics, you can use this service aid to update the microcode from the NIM server. Choose the `/usr/lib/microcode` directory when prompted for the source of the microcode that you want to update. If there is not enough space available, an error is reported, stating additional system memory is needed. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue with the update, the system reboots by using the **`reboot -u`** command. You might receive a Caution: some processes would not die message during the reboot process. You can ignore this message. The current flash image is not saved.

Update and manage system flash

Note: Update and manage system flash is a subtask that can be accessed after selecting **Microcode Tasks**, see "Microcode tasks" on page 25.

Attention: If the system is managed by a management console, the firmware update must be done through the management console. If the system is not managed by a management console, the firmware update can be done by using the service aid..

This selection validates a new system firmware flash image and uses it to update the system temporary flash image. This selection can also be used to validate a new system firmware flash image without performing an update, commit the temporary flash image, and reject the temporary flash image.

When this service aid is run from stand-alone diagnostics, the flash update image file is copied to the file system from optical media, or from the NIM server. Before performing the NIM boot of diagnostics, the server firmware image must first be copied onto the NIM server in the `/usr/lib/microcode` directory. Then you must point to the NIM SPOT (from which you plan to have the NIM client boot stand-alone diagnostics). Next, a NIM check operation must be run on the SPOT containing the microcode image on the NIM server. After performing the NIM boot of diagnostics, you can use this service aid to update the microcode from the NIM server. Choose the `/usr/lib/microcode` directory when prompted for the source of the microcode that you want to update. If enough space is not available, an error is reported, stating additional system memory is needed. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue with the update, the system reboots by using the **`reboot -u`** command. You might receive a message that says: "Caution: some processes would not die" during the reboot process; you can ignore this message. The current flash image is not saved.

Component and attention LEDs

The component and attention light-emitting diodes (LEDs) assist in identifying devices and components in your server when an action is needed or if there is a failure.

If a failing component is detected in your system, an amber attention LED on the front of the system unit is turned on solid (not blinking). You can use the service processor menus in the Advanced System Management Interface to blink the FRU LED for the failing FRU.

Individual LEDs are located on or near the failing field replaceable unit (FRU). The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, CPU). LEDs are either green or amber.

Green LEDs indicate either of the following:

- Electrical power is present.
- Activity is occurring on a link. (The system could be sending or receiving information.)

Amber LEDs indicate a fault or identify condition. If your system or one of the components in your system has an amber LED turned on or blinking, identify the problem and take the appropriate action to restore the system to normal.

The following table identifies the color and status of the component and attention LEDs. Units or FRUs may not have all of the LEDs listed in the table.

Table 1. Component and attention LEDs

Unit (FRU)	LED Function	LED Color	Off	On	Blink
System attention	Attention	Amber	Normal	Fault	Identify
System power	Power	Green	No ac power	System on	Standby
Fan	Identify	Amber	Normal		Identify
	Power	Green	No power	Power on	
Power supply	ac power input good	Green	No Input	Input good	
	Identify	Amber	Normal	Fault	Identify
	dc power output good	Green	All power supply outputs off	All power supply outputs on	Control voltage good
Disk drives	Activity	Green	No disk activity	Disk being accessed	
	Identify	Amber			Identify
PCI slot	Power	Green	No power	Power on	
	Identify	Amber	Normal		Identify
RIO/HSL	Identify	Amber	Normal		Identify
Memory DIMM	Identify	Amber	Normal		Identify
System backplane	Identify	Amber	Normal		Identify
PCI riser card	Power	Green	No power	Power on	
	Identify	Amber	Normal		Identify
Disk drive backplane	Identify	Amber	Normal		Identify

Table 1. Component and attention LEDs (continued)

Unit (FRU)	LED Function	LED Color	Off	On	Blink
Media backplane	Identify	Amber	Normal		Identify
Service processor card	Identify	Amber	Normal		Identify
Voltage regulator module	Identify	Amber	Normal		Identify
RAID adapter card	Identify	Amber	Normal		Identify
HMC port	Link	Green	No link	Link	
	Activity	Green	No activity		Activity
Imbedded Ethernet	Link	Green	No link	Link	
	Activity	Green	No activity		Activity
Node assembly	Power	Green	No power	Power on	
	Identify	Amber	Normal		Identify
Bulk power controller (BPC)	Activity	Green	No power	Power on	
	Identify	Amber	Normal		Identify
Motor drive assembly (MDA)	Power	Green	No power	Power on	
Motor scroll assembly (MSA)	Identify	Amber	Normal		Identify
MCM	Identify	Amber	Normal		Identify
Light strip	Power	Green	No power	Power on	
	Identify	Amber	Normal		Identify

Notices

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

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

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

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

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

Any references in this information to websites not owned by the manufacturer 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 product and use of those websites is at your own risk.

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

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

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

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

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

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

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

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

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

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

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

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.

Trademarks

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER7® processor and its features unless designated as electromagnetic compatibility (EMC) Class B in the feature information.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Community Compliance Statement

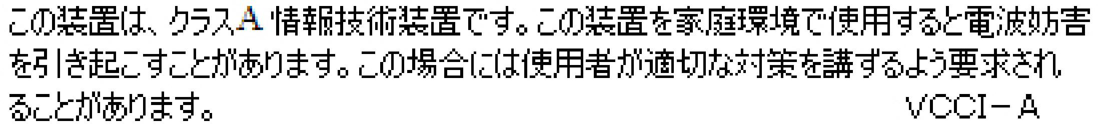
This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

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

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
email: lugi@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan



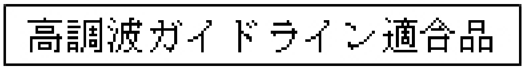
この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI－A

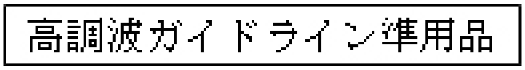
The following is a summary of the VCCI Japanese statement in the box above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

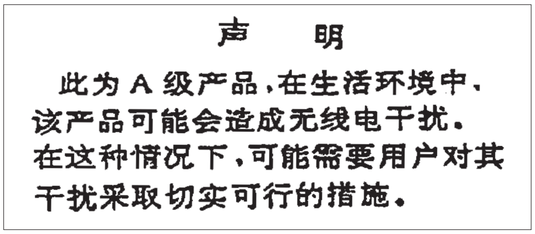
Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)


高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)


高調波ガイドライン準用品

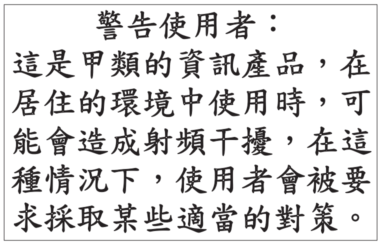
Electromagnetic Interference (EMI) Statement - People's Republic of China


声　明

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

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan


警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

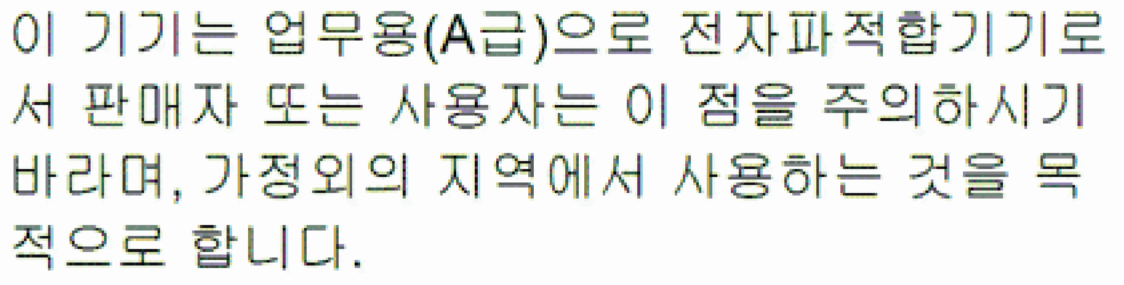
The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

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

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

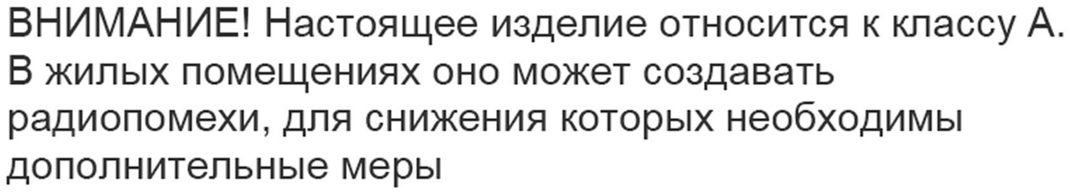
Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15 2941
email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia



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

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC) Class B in the feature installation information.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

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

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
email: lugi@de.ibm.com

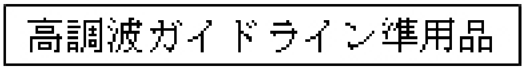
VCCI Statement - Japan

この装置は，クラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　　　　　ＶＣＣＩ－Ｂ

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)

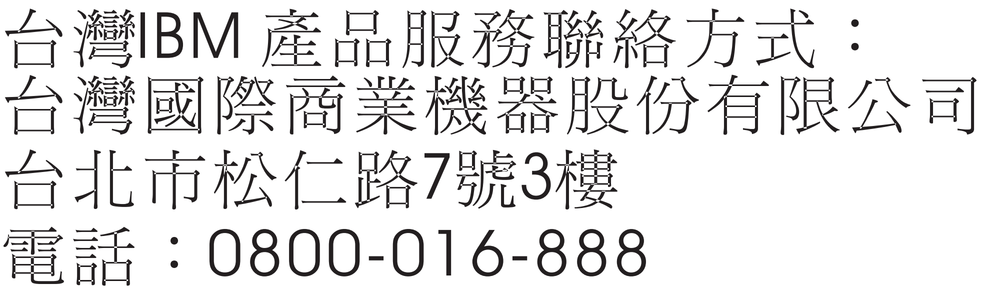
高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)



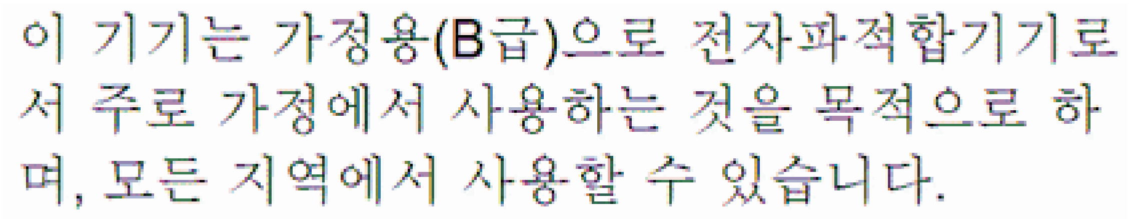
高調波ガイドライン準用品

IBM Taiwan Contact Information



台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



이 기기는 가정용(B급)으로 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse 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 Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15 2941
email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

Terms and conditions

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

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

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

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

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

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

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

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

Printed in USA