Power Systems

Diagnostics and service aids

Power Systems

Diagnostics and service aids

Note

Before using this information and the product it supports, read the information in "Safety notices" on page v, "Notices" on page 53, 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 POWER8 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.**

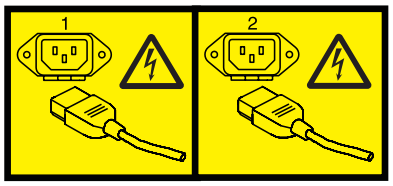
(R002)

(L001)

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

(L002)

(L003)



or

or

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

(L008)

CAUTION: Hazardous moving parts nearby. (L008)

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

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

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

(C026)

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (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 AIX® operating system, the diagnostics and service aids are available as part of the operating system. For AIX partitions that cannot be started, or 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 online diagnostics. The online diagnostics are always available in a partition, and they have the advantage of keeping error log files as long as the operating system is running. This enables the online diagnostics to analyze the error logs to help pinpoint any hardware problems without shutting down the partition. With concurrent maintenance capabilities of the hardware, many repairs can be made concurrently and system users can continue their work without interruption. 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 Knowledge Center.

AIX operating system message files

English is the default language displayed by the diagnostic programs when run from disk. If you want to run the diagnostic programs in a language other than English, you must install the AIX message locale file for the wanted language to the system.

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. If you are using the AIX operating system and using online diagnostics, the **lsmcode** command and the **diag** command can also be used to display the firmware and microcode levels of individual entities in the

system from the command line. 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 8 for detailed scenarios that explain how to use the update and manage system flash task.

Use the Download microcode service aid on systems running AIX 5.2.0.30 or later to update the microcode on adapters and devices. For details on updating adapter and device microcode, see "Updates" on page 8.

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**.

Automatic diagnostic tests

All automatic diagnostic tests run after the system unit is turned on and before the AIX operating system is loaded.

The automatic diagnostic tests display progress indicators (or checkpoints) to track test progress. If a test stops or hangs, the checkpoint for that test remains in the display to identify the unsuccessful test. The descriptions of these tests are contained in Reference code finder.

Power-on self-test

Power-On Self-Test (POST) programs check the devices needed to accomplish an initial program load. The POST also checks the memory, and portions of the central electronics complex, common interrupt handler, and the direct memory access (DMA) handler.

Configuration program

The configuration program determines which features, adapters, and devices are present on the system. The configuration program, which is part of the AIX operating system, builds a configuration list that is used by the diagnostic programs. This list is used to control which tests are run during system checkout.

On systems running AIX, the configuration program displays numbers between 2E6 through 9FF and 2300 through 27FF in the operator panel display (if present). See Reference code finder for a listing of program actions associated with displayed numbers. On systems running logical partitions, LPAR displays in the

operator panel (if present) after the hypervisor (the system firmware that controls the allocation of resources) is loaded. When a partition runningAIX is then booted, the configuration codes display on the Reference code column in the management console Contents area.

Devices attached to serial and parallel ports are not configured. The Dials and Lighted Program Function Keys (LPFKs) can be tested from online diagnostics after they are manually configured. No other device attached to the serial and parallel ports is supported by the diagnostics.

CPU and memory testing and error log analysis

Except for the floating-point tests, all CPU, and memory testing on the system units are done by POST and BIST. Memory is tested entirely by the POST. The POST provides an error-free memory MAP. If POST cannot find enough good memory to boot, it halts and displays an error message. If POST finds enough good memory, the memory problems are logged and the system continues to boot.

If any memory errors were logged, they are reported by the base system or memory diagnostics, which must be run to analyze the POST results.

The CPU and memory cannot be tested after the diagnostics are loaded; however, they are monitored for correct operation by various checkers such as processor runtime diagnostics.

Single-bit memory errors are corrected by ECC (Error Checking and Correction) on systems equipped with ECC memory.

Diagnostic programs

This section provides overview of the various diagnostic programs.

Diagnostic controller

The diagnostic controller runs as an application program on the AIX operating system. The diagnostic controller carries out the following functions:

- Displays diagnostic menus
- Checks availability of needed resources
- Checks error log entries under certain conditions
- Loads diagnostic application programs
- Loads task and service aid programs
- Displays test results

To test an adapter or device, select the device or adapter from the diagnostic selection menu. The diagnostic controller then loads the diagnostic application program for the selected device or adapter.

The diagnostic application program loads and runs test units to check the functions of the device or adapter.

The diagnostic controller checks the results of the tests done by the diagnostic application and determines the action needed to continue the testing.

The amount of testing that the diagnostic application does depends on the mode (service, maintenance, or concurrent) under which the diagnostic programs are running.

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.

When you select the **diagnostics** or **advanced diagnostics** option, the **diagnostic selection** menu is displayed (other menus might be shown before this menu). You can select the purpose for running diagnostics by using this menu.

When you select the **problem determination** option, the diagnostic programs read and analyze the contents of the error log.

Note: Most hardware errors in the operating system error log contain *sysplanar0* as the resource name. The resource name identifies the resource that detected the error; it does not indicate that the resource is faulty or should be replaced. Use the resource name to determine the appropriate diagnostic to analyze the error.

If the error log contains recent errors (approximately the last seven days), the diagnostic programs automatically select the diagnostic application program to test the adapter or device that the error was logged against.

If there are no recent errors logged or the diagnostic application program runs without detecting an error, the diagnostic selection menu is displayed. You can select a resource for testing by using this menu.

If an error is detected while the diagnostic application program is running, the A PROBLEM WAS DETECTED screen displays a service request number (SRN).

Note: After a FRU is replaced based on an error log analysis program, the error log entries for the problem device must be removed or the program might continue to indicate a problem with the device. To accomplish this task, run the **errclear** command from the command line. Alternatively, you can use the System Management Interface Tool (SMIT) to select **Problem Determination/Error Log/Clear the Error Log**. Fill out the appropriate menu items.

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 19.

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.

Automatic error log analysis (diagela)

Automatic error log analysis (**diagela**) is only supported when running the online diagnostics. The **diagela** command provides the capability to perform error log analysis when a permanent hardware error is logged, by enabling the **diagela** program on all platforms.

Note: If you are using the Linux operating system, the ppc64-diag service aid is used for error log analysis. See Obtaining service and productivity tools for Linux.

The **diagela** program determines whether the error should be analyzed by the diagnostics. If the error should be analyzed, a diagnostic application is invoked and the error is analyzed. No testing is done if the diagnostics determine that the error requires a service action. Instead it sends a message to your console, and either the Service Management applications for systems with a management console, or to all system groups. The message contains the SRN.

Running diagnostics in this mode is similar to using the **diag -c -e -d** *Device* command.

Notification can also be customized by adding a stanza to the **PDiagAtt** object class. The following example illustrates how a program can be invoked in place of the normal mail message. The example also shows that you can send the message to the Service Management application when there is no HMC.

```
PDiagAtt:
     DClass = " "
     DSClass = " "
     DType = " "
     attribute = "diag_notify"
     value = "/usr/bin/customer_notify_ program $1 $2 $3 $4 $5"
     rep = "s"
```

If DClass, DSClass, and DType are blank, then the `customer_notify_program` applies for *all* devices. If you enter specifics in the DClass, DSClass, and DType the `customer_notify_program` is invoked only for that device type.

After the above stanza is added to the ODM data base, problems are displayed on the system console. Then, the program specified in the value field of the `diag_notify` predefined attribute is invoked. The following keyword is expanded automatically as arguments to the notify program:

- $1 the keyword `diag_notify`
- $2 the resource name that reported the problem
- $3 the Service Request Number
- $4 the device type
- $5 the error label from the error log entry

If no diagnostic program is found to analyze the error log entry, or analysis is done but no error was reported, a separate program can be specified to be invoked. This is accomplished by adding a stanza to the **PDiagAtt** object class with an attribute = **diag_analyze**. The following example illustrates how a customer's program can be invoked for this condition:

```
PDiagAtt:
     DClass = " "
     DSClass = " "
     DType= " "
     attribute = "diag_anaylze"
     value = "/usr/bin/customer_analyzer_program $1 $2 $3 $4 $5"
     rep = "s"
```

If DClass, DSClass, and DType are blank, then the `customer_analyzer_program` applies for all devices. Specifying the DClass, DSClass, and DType with details causes the `customer_analyzer_program` to be invoked only for that device type.

After the above stanza is added to the ODM data base, the program specified is invoked if there is no diagnostic program specified for the error, or if analysis was done, but no error found. The following keywords expand automatically as arguments to the analyzer program:

- $1 the keyword **diag_analyze**
- $2 the resource name that reported the problem
- $3 the error label from the error log entry if from ELA, the keyword PERIODIC if from Periodic Diagnostics, or the keyword REMINDER if from a Diagnostic Reminder.
- $4 the device type
- $5 the keywords:
  - **no_trouble_found** if the analyzer was run, but no trouble was found.
  - **no_analyzer** if the analyzer is not available.

To activate the automatic error log analysis feature, log in as root user (or use the CE login) and type the following command:

```
/usr/lpp/diagnostics/bin/diagela ENABLE
```

To disable the automatic error log analysis feature, log in as root user (or use the CE login) and type the following command:

```
/usr/lpp/diagnostics/bin/diagela DISABLE
```

The **diagela** program can also be enabled and disabled using the periodic diagnostic service aid.

Log repair action

Note: The log repair action is only supported when using online diagnostics.

The diagnostics perform error log analysis on most resources. The default time for error log analysis is seven days; however, this time can be changed from 1 to 60 days by using the **display or change diagnostic run time options** task. To prevent false problems from being reported when error log analysis is run, repair actions need to be logged whenever a FRU is replaced. A repair action can be logged by using the **log repair action** task or by running advanced diagnostics in system verification mode.

The log repair action task lists all resources. Replaced resources can be selected from the list, and when **commit** (F7 key) is selected, a repair action is logged for each selected resource.

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.

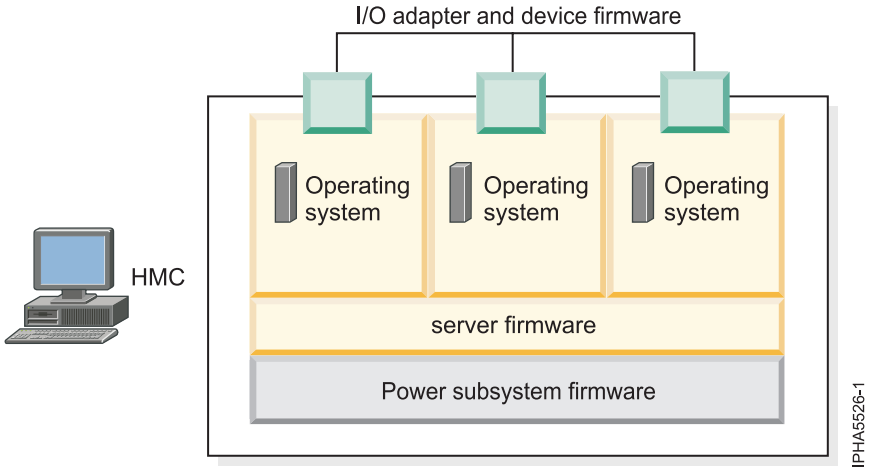
A good update strategy is an important part of maintaining and managing your server. If you have a dynamic environment that changes frequently, install updates on a regular basis. If you have a stable environment, you do not have to install updates as frequently. However, you should consider installing 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. For more information, see Log repair action.

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 online and stand-alone hardware diagnostics

Use these tools to diagnose hardware problems on your system that is running the AIX or 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 AIX or 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.

If you have the AIX operating system installed and it is running, you can perform online hardware diagnostics. However, if the installed AIX operating system cannot be started, or you have the Linux operating system installed, you will need to run the 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. To verify the repair in AIX, see Verify a repair in AIX.

Running the online diagnostics

If you have AIX installed and it can be started, use this procedure to perform diagnostic procedures when directed from another procedure or by your next level of support.

When you run online diagnostics, keep the following in mind:

- When AIX is installed, the support for some devices might not be automatically installed. If this happens, that device will not display in the test list when online diagnostics run.
- 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.

Three modes are available for running the online diagnostics:

- **Service mode** provides the most complete check of the system resources, but requires that no other programs are running on the system. When possible, run the diagnostics in service mode.
- **Maintenance mode** allows you to check most of the available resources, with the exception of SCSI adapters, memory, processor, and the disk drive used for paging.
- **Concurrent mode** allows you to run online diagnostics on some of the system resources while the system is running normal activity.

Running online diagnostics in concurrent mode

Use this procedure to run the online diagnostics in concurrent mode.

Use concurrent mode to run online diagnostics on some of the system resources while the system is running normal activity.

Because the system is running in normal operation, the following resources cannot be tested in concurrent mode:

- SCSI adapters connected to paging devices
- Disk drive used for paging
- Some display adapters and graphics related devices

The following levels of testing exist in concurrent mode:

Share-test level
This level tests a resource while the resource is being shared by programs running in the normal operation. This testing is mostly limited to normal commands that test for the presence of a device or adapter.

Sub-test level
This level tests a portion of a resource while the remaining part of the resource is being used in normal operation. For example, you could test one port of a multiport device while the other ports are being used in normal operation.

Full-test level
This level requires the device to not be assigned or used by any other operation. This level of testing on a disk drive might require the use of the vary off command. Use the diagnostics display menus to allow you to vary off the needed resource.

Perform the following steps to run online diagnostics in concurrent mode:

1. Log in to the AIX operating system as root user, or use CE login. If you need help, contact the system administrator.
2. Enter the `diag` command to load the diagnostic controller, and display the online diagnostic menus.
3. If requested, enter a password.
4. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

   Note: If you do not receive the Diagnostic Operating Instructions display, try to run the stand-alone diagnostics. For details, see "Running the stand-alone hardware diagnostics" on page 13.
5. When testing is complete, press F3 to return to the Diagnostic Operating Instructions display.
6. Press F3 again to return to the AIX operating system prompt.
7. Vary on any resources that you varied off.
8. Press Ctrl+D to log off from root user or CE login.
9. 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).

Running online diagnostics in maintenance mode

Use this procedure to run the online diagnostics in maintenance mode.

Maintenance mode requires that all activity on the logical partition running the AIX operating system be stopped so that the online diagnostics have most of the resources available. All of the system resources, except the SCSI adapters, memory, processor, and the disk drive used for paging can be checked.

Perform the following steps to run the online diagnostics in maintenance mode:

1. Stop all programs running on the logical partition except the AIX operating system.
2. Log in to the AIX operating system as root user or use CE login.
3. Type the `shutdown -m` command to stop all activity on the AIX operating system and put it into maintenance mode.
4. When a message indicates that the system is in maintenance mode, enter the `diag` command to invoke the diagnostic controller so you can run the diagnostics.

   Note: It might be necessary to set TERM type again.
5. Enter any passwords, if requested.
6. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

   Note: If you do not receive the Diagnostic Operating Instructions display, try to run the stand-alone diagnostics. For details, see "Running the stand-alone hardware diagnostics" on page 13.
7. When finished, press Ctrl+D to log off from root user or CE login.
8. Contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs). **This ends the procedure.**

Running online diagnostics in service mode

Use this procedure to run online diagnostics in service mode.

Using service mode will check everything except the SCSI adapter and the disk drives used for paging. However, memory and processor are only tested during POST. Running in service mode ensures that the error state of the system that has been captured in NVRAM is available for your use in analyzing the problem.

Running online diagnostics in service mode with a management console attached:

Use this procedure to run online diagnostics in service mode with an management console attached.

Perform the following steps:

1. Stop all programs including the AIX operating system. For details, see Powering on and powering off the system .
2. From the Hardware Management Console (HMC), complete the following steps:
   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 checkbox to select a server on the right pane.
   c. From the tasks menu, select **Console Window** > **Open Terminal Window**.
3. From the Service Processor Menu on the VTERM, select option 2 (System Power Control).
4. Select option 6.
5. Verify that the state changes to `currently disabled`. Disabling fast system boot automatically enables slow boot.
6. Select option 98 to exit the system power control menu.
7. From the management console, start the managed system in a full system partition.
8. Select **Power on Diagnostic Stored Boot list**.
9. Make sure that there is no media in the devices in the media subsystem.
10. Enter any passwords, if requested.
11. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

Note: If you do not receive the Diagnostic Operating Instructions display, try to run the stand-alone diagnostics. For details, see "Running the stand-alone hardware diagnostics."

12. 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).

Running online diagnostics in service mode without a management console attached:

Use this procedure to run online diagnostics in service mode *without* a management console attached.

Perform the following steps:

1. Stop all programs including the AIX operating system. For details, see Powering on and powering off the system .
2. Remove all tapes, diskettes, and CDs.
3. Turn off the system unit power.
4. Turn on the system unit power.
5. After the keyboard POST indicator displays on the firmware console, and before the last POST indicator (speaker) displays, press 6 on the keyboard or ASCII terminal to indicate that a service mode boot should be initiated using the customized service mode boot list.
6. Enter any passwords, if requested.
7. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

   Note: If you do not receive the Diagnostic Operating Instructions display, try to run the stand-alone diagnostics. For details, see "Running the stand-alone hardware diagnostics."
8. 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).

Running the stand-alone hardware diagnostics

If the system that you want to run hardware diagnostics on has the AIX operating system installed but it cannot be started, or you have the Linux operating system installed, use this procedure to perform hardware diagnostic procedures. 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.
   - If the system is powered off, continue with step 3.
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.
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 on page 15.
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.
3. From the Hardware Management Console (HMC), complete the following steps:
    a. In the navigation area, select **Systems Management** > **Servers**.
    b. In the navigation 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 AIX is running, type the **shutdown -F** command.
        - If Linux is running, type the **shutdown -h now** command
    f. Close the VTerm window.
4. From the **Tasks** menu, select **Operations** > **Activate**. This activates the server partition
5. Ensure the **Open a terminal window or console session box** is selected and click **OK**.
6. 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.

7. 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.
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 on page 17.
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 on page 16.
    - 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

For information about performing the following tasks, see the *Advanced NIM configuration tasks* chapter of the *AIX Installation Guide and Reference*:

- 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 AIX or 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. Many of these programs work on all system model architectures. Some programs are only accessible from online diagnostics in service or concurrent mode, while others might be accessible only from stand-alone diagnostics.
2. 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.
3. 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 Knowledge 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.

You can use a fast path method to perform a task by using the **diag** command with the **-T** flag. By using the fast path method, you can bypass most of the introductory menus to access a particular task. You are presented with a list of resources available to support the specified task. The fast path tasks include the following options:

certify Certifies media

chkspares
Checks for the availability of spare sectors

download
Downloads microcode to an adapter or device

disp_mcode
Displays current level of microcode

format
Formats media

identify
Identifies the PCI RAID physical disks

identifyRemove
Identifies and removes devices (hot plug)

To run these tasks directly from the command line, specify the resource and other task-unique flags. Use the descriptions in this topic to understand which flags are needed for each 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.

Shell prompt

Note: Use this service aid in online service mode only.

This service aid allows access to the AIX command line. To use this service aid, you must know the root password (if a root password is set).

Note: Do not use this task to install code or to change the configuration of the system. This task is intended to view files, configuration records, and data. Using this service aid to change the system configuration or install code can produce unexplained system problems after exiting the diagnostics.

Analyze the adapter internal log

Note: Use this service aid in online mode only.

The PCI RAID adapter has an internal log that logs information about the adapter and the disk drives attached to the adapter. Whenever data is logged in the internal log, the device driver copies the entries to the system error log and clears the internal log.

The analyze adapter internal log service aid analyzes these entries in the system error log. The service aid displays the errors and the associated service actions. Entries that do not require any service actions are ignored.

When running this service aid, a menu is presented to enter the start time, the end time, and the file name. The start time and end time have the following format: [*mmddHHMMyy*]. The *mm* is the month (1-12), *dd* is the date (1-31) *HH* is the hour (00-23) *MM* is the minute (00-59), and *yy* is the last two digits of the year (00-99). The file name is the location where you want to store the output data.

To start the service aid task from the command line, type:

`diag -c -d devicename -T "adapela [-s start date -e end date]`

Flag **Description**

-c Specifies not console mode.

-d *device name*
Specifies the device whose internal log you want to analyze (for example, `SCRAID0`)

-s *start date*
Specifies all errors after this date are analyzed.

-e *end date*
Specifies all errors before this date are analyzed.

-T Specifies the Analyze Adapter Internal Log task

Note: To specify a file name from the command line, use the redirection operator at the end of the command to specify where the output of the command is to be sent. For example `> filename` (where *filename* is the name and location where the user wants to store the output data (for example, `/tmp/adaptlog`).

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

If you are running the AIX operating system in online diagnostic mode, this task can be run directly from the command line. The command-line syntax is: `diag -c -d -T certify`

The following flags can be used:

Flag	Description
-c	No console mode
-d	Specifies a device
-T	Specifies the certify task

Certify Hard disk 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 disk 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 disk files, format the hard diskfile and certify again.

For pdisk hard disk 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 disk file must be replaced.

After the read certify of the disk surface completes for hdisk hard disk 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.

If you are running the AIX operating system in online diagnostic mode, this task can be run directly from the command line. The command-line syntax is: `diag -c -d` *deviceName* `-T "certify"`

Flag	Description
-c	No console mode
-d	Specifies a device
-T	Specifies the certify task

Certify Hard Disk 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.

If you are running the AIX operating system in online diagnostic mode, this task can be run directly from the command line. The command-line syntax is: `diag -c -d` *RAIDadapterName* `-T "certify {-l` *chID* `| -A}"`

Flag	Description
-c	No console mode
-d	Specifies the RAID adapter to which the disk is attached
-T	Specifies the certify task and its parameters
-I	Specifies physical disk channel/ID (for example: -l 27)
-A	All disks

Change hardware vital product data

Use this service aid to view the alter or display the vital product data (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 dials and LPF keys

Note: The dials and LPF keys service aid is not supported in stand-alone mode (CD-ROM and NIM) on systems with 32 MB or less memory. If you have problems in stand-alone mode, use the hard disk-based diagnostics.

This service aid provides a tool for configuring and removing dials and LPF keys to the asynchronous system ports.

This selection starts the System Management Interface Tool (SMIT), which allows dial and LPF key configuration. A TTY must be in the available state on the async port before the dials and LPF keys can be configured on the port. The task allows an async adapter to be configured, then a TTY port defined on the adapter. Dials and LPF keys can then be defined on the port.

Before configuring dials or LPF keys on a system port, you must remove all defined TTYs. To determine whether there are any defined TTYs, select **List All Defined TTYs**. After all defined TTYs are removed, then add a TTY and configure the dials or LPF keys.

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.

Enable platform automatic power restart

When enabled, **Platform auto power** restart allows the platform firmware to restart a system after power is restored following a power outage. If the system is partitioned, each partition that was running when the power outage occurred is restarted as indicated by the SMIT option: `Automatically reboot operating system after a crash`. This setting must be set for each partition.

This service aid can be accessed directly from the command line, by entering:

```
/usr/lpp/diagnostics/bin/uspchrp -b
```

The parameter setting might be read and set directly from the command line. To read the parameter, use the command:

```
/usr/lpp/diagnostics/bin/uspchrp -q platform-auto-power-restart
```

To set the parameter, use the command:

```
/usr/lpp/diagnostics/bin/uspchrp -e platform-auto-power-restart=[0|1]
```

where:

1 = Enable Platform Automatic Power Restart
0 = Disables Platform Automatic Power Restart

The Platform Boot Speed system parameter can be read or set from the command line only. To read the Platform Boot Speed system parameter, use the command: `/usr/lpp/diagnostics/bin/uspchrp -q PlatformBootSpeed`

To set the Platform Boot Speed system parameter, use the command:

```
/usr/lpp/diagnostics/bin/uspchrp -e PlatformBootSpeed=[fast|slow]
```

With a fast platform speed, the platform firmware performs a minimal set of hardware tests before loading the operating system. With a slow platform speed, the platform firmware performs a comprehensive set of hardware tests before loading the operating system.

For the command:

```
/usr/lpp/diagnostics/bin/uspchrp -q <variable name> | -e <variable name>=value
```

The return codes are:
0 = command successful
1 = command not successful

Configure platform processor diagnostics

This service aid provides the user-interface to specify a system parameter platform processor diagnostics used by the firmware. The firmware uses the parameter setting to determine when a series of processor diagnostics tests are run. Errors from the processor diagnostics tests are logged in to the error log and are analyzed by the sysplanar0 diagnostics. Otherwise, there is no notification to the operating system when the tests are run. The possible values of the system parameter and their descriptions are as follow:

disabled
No processor diagnostics.

staggered
Processor diagnostics are run periodically. All processors are tested but are not scheduled at the same time.

immediate
When setting this value, processor diagnostics are run immediately. When querying this value, processor diagnostics are currently running.

periodic
Processor diagnostics are run periodically, all at the same time.

The periodic setting cannot be set by using this service aid, although it can be read. The management console is used to set the periodic setting.

The Configure platform processor diagnostics setting is accessed by using the **diag** command, and then selecting the appropriate topic from the diagnostics task menus.

It also might be accessed directly from the AIX command line, by entering:

```
/usr/lpp/diagnostics/bin/uspchrp -p
```

To query the platform processor diagnostics parameter, enter:

```
/usr/lpp/diagnostics/bin/uspchrp -q PlatformProcessorDiagnostics
```

Note: The output of the query operation might be disabled, staggered, immediate, or periodic.

To set the platform processor diagnostics parameter, enter:

```
/usr/lpp/diagnostics/bin/uspchrp -e PlatformProcessorDiagnostics=[disabled|staggered|immediate]
```

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.

You can access this service aid directly from the AIX command line by typing:
`/usr/lpp/diagnostics/bin/uspchrp -d`

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. When booting from the hard disk or LAN, the information can be viewed from the AIX error log by using the hardware error report service aid. In either case, the information is analyzed when the `sysplanar0` diagnostics are running in problem determination mode.

Display microcode level

Note: Display microcode level is a subtask that can be accessed after selecting Microcode Tasks, see "Microcode tasks" on page 44.

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.

You can display the current level of the microcode on an adapter, the system, or a device by using the **diag** command. See the following command syntax: `diag -c -d device -T "disp_mcode"`

-c No console mode.

-d Used to specify a device.

-T Use the disp_mcode option to display microcode.

The **lsmcode** command serves as a command-line interface to the display microcode level task.

Display MultiPath I/O (MPIO) device configuration

Note: Use this service aid in online mode only.

This service aid displays the status of MPIO devices and their connections to their parent devices.

Use this service aid to send SCSI commands on each available path regardless of the default MPIO path algorithm. Therefore, it is useful for testing the unused path for integrity.

Run this service aid if you suspect a problem with the path between MPIO devices and their parent devices.

Use this service aid for:

- Listing MPIO devices
- Listing the parents of MPIO devices
- Displaying the status and location of specified MPIO devices
- Displaying the hierarchy of MPIO adapters and devices.

If there are no devices with multiple paths, this service aid is not shown on the Task Selection menu.

Access this service aid directly from the command line by typing:

```
/usr/lpp/diagnostics/bin/umpio
```

Display or change bootlist

This service aid allows the bootlist to be displayed, altered, or erased.

The system attempts to perform an IPL from the first device in the list. If the device is not a valid IPL device or if the IPL fails, the system proceeds in turn to the other devices in the list to attempt an IPL.

Display or change diagnostic runtime options

The display or change diagnostic runtime options task allows the diagnostic runtime options to be set.

Note: The runtime options are used only when selecting the run diagnostic task.

The runtime options are:

Display Diagnostic Mode Selection menus
This option allows the user to turn on or off displaying the DIAGNOSTIC MODE SELECTION MENU (the default is on).

Run Tests Multiple Times
This option allows the user to turn on or off, or specify a loop count, for diagnostic loop mode (the default is off).

Note: This option is only displayed when you run the online diagnostics in service mode.

Include Advanced Diagnostics
This option allows the user to turn on or off including the advanced diagnostics (the default is off).

Number of Days Used to Search Error Log
This option allows the user to select the number of days for which to search the AIX error log for errors when running the error log analysis. The default is seven days, but it can be changed from one to 60 days.

Display Progress Indicators
This option allows the user to turn on or off the progress indicators when running the diagnostic applications. The progress indicators, in a box at the bottom of the screen, indicate that the test is being run (the default is on).

Diagnostic Event Logging
This option allows the user to turn on or off logging information to the diagnostic event log (the default is on).

Diagnostic Event Log File Size
This option allows the user to select the maximum size of the diagnostic event log. The default size for the diagnostic event log is 100 KB. The size can be increased in increments of 100 KB to a maximum of 1 MB.

Use the **diaggetrto** command to display one or more diagnostic runtime options. Use the following AIX command syntax:

```
/usr/lpp/diagnostics/bin/diaggetrto [-a] [-d] [-l] [-m] [-n] [-p] [-s]
```

Use the **diagsetrto** command to change one or more diagnostic runtime options. Use the following AIX command syntax:

```
/usr/lpp/diagnostics/bin/diagsetrto [-a on|off] [-d on|off] [-l size]
[-m on|off] [-n days] [-p on|off]
```

Flag descriptions for the **diaggetrto** and **diagsetrto** commands are as follows:

Flag	Description
-a	Displays or changes the value of the advanced diagnostics option.
-d	Displays or changes the value of the diagnostic event that is being logged.
-l	Displays or changes the value of the diagnostic event log file size. Allowable size is between 100K and 1000K in increments of 100K. The size cannot be decreased.
-m	Displays or changes the value of the display diagnostic mode selection menu option.
-n	Displays or changes the value of the number of days used to search the error log option. Allowable values are 1 - 60 days. Seven days is the default.
-p	Displays or changes the value of the display progress indicators option.
-s	Displays all of the diagnostic runtime options.

Display previous diagnostic results

Note: This service aid is not available when using stand-alone diagnostics.

This service aid allows a service representative to display results from a previous diagnostic session. When the display previous diagnostic results option is selected, the user can view up to 25 no trouble found (NTF) and service request number (SRN) results.

This service aid displays diagnostic event log information. You can display the diagnostic event log in a short version or a long version. The diagnostic event log contains information about events logged by a diagnostic session.

This service aid displays the information in reverse chronological order.

This information is not from the operating system error log. This information is stored in the `/var/adm/ras` directory.

You can run the command from the command line by typing:

```
/usr/lpp/diagnostics/bin/diagrpt [[-o] ? [-s mmddyy] ? [-a] ? [-r]]
```

-o Displays the last diagnostic results file stored in the `/etc/lpp/diagnostics/data` directory

-s *mmddyy*
Displays all diagnostic result files logged since the date specified

-a Displays the long version of the diagnostic event log

-r Displays the short version of the diagnostic event log

Display resource attributes

Note: Use this service aid in online mode only.

This task displays the customized device attributes associated with a selected resource. This task is similar to running the `lsattr -E -l resource` command.

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 software product data

This task uses SMIT to display information about the installed software and provides the following functions:

- List Installed Software
- List Applied but Not Committed Software Updates
- Show Software Installation History
- Show Fix (APAR) Installation Status
- List Fileset Requisites
- List Fileset Dependents
- List Files Included in a Fileset
- List File Owner by Fileset

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 **OHCD***X*, 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 44.

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.

This task can be run directly from the AIX command line. Most adapters and devices use a common syntax as identified in the "Microcode installation to adapters and devices" section. Information for adapters and devices that do not use the common syntax can be found following this section.

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.

If you are using the AIX operating system and are using online diagnostics, the following example is the common syntax command: `diag [-c] -d device -T "download [-s {/etc/microcode|source}] [-l {latest|previous}] [-f]"`

-c No console mode. Run without user interaction.

-d *device*
Run the task on the device or adapter specified.

-T download
Install microcode.

-s /etc/microcode
The microcode image is in the `/etc/microcode` directory. This directory is the default.

-s *source*
Microcode image is on specified source. For example, fd0, cd0.

-l latest
Install latest level of microcode. This setting is the default.

-l previous
Install previous level of microcode.

-f Install microcode even if the current level is not on the source.

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.

The following is the common syntax command:

`diag [-c] -d` *`device`* `-T "download [-s {/etc/microcode|`*`source`*`}]"`

-c No console mode. Run without user interaction.

-d *device*
Run the task on the device or adapter specified.

-T download
Install microcode.

-s /etc/microcode
Microcode image is in `/etc/microcode`.

-s *source*
Microcode image is on specified source. For example, fd0, cd0.

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.

Syntax: `diag [-c] -d` *`RAIDadapterName`* `-T "download [-B][-D][-P]"`

-c No console mode. Run without user interaction.

-d *RAIDadapterName*
Run the task on the RAID adapter specified.

-T download
Install microcode.

-B Install boot block microcode. Default is functional microcode.

-D Microcode image is on diskette. Default is /etc/microcode.

-P Install the previous level of microcode. Default is latest level.

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.

Syntax: `diag [-c] -d` *`RAIDadapterName`* `-T "download {-l` *`chID`* `| -A} [-D][-P]"`

-c No console mode. Run without user interaction.

-d RAIDadapterName
Name of the RAID adapter the disk is attached to.

-T download
Install microcode.

-l Physical disk channel/ID of RAID disk drive (example: 27).

-A All disk drives attached to specified RAID adapter.

-D Microcode image is on diskette. Default is `/etc/microcode`.

-P Install the previous level of microcode. Default is the latest level.

Fault indicators

This task is only available through a command-line interface. It is not available from the diagnostic menu or from stand-alone diagnostics.

The fault indicators are used to identify a fault with the system. These indicators might be set automatically by hardware, firmware, or diagnostics when a fault is detected in the system.

The System Attention Indicator is turned off when a Log Repair Action is performed. All other Fault Indicators are turned off when the failing unit is repaired or replaced. After a serviceable event is complete, do a System Verification to verify the fix. Also, do a Log Repair Action if the test on the resource was good, and that resource had an entry in the error log.

For more information about the use of these indicators, see the service information for the system unit you are using.

Note: The AIX command does not allow you to set the fault indicators to the fault state.

Use the following command syntax:

```
/usr/lpp/diagnostics/bin/usysfault [-s normal] [-l location code | -d devicename]
/usr/lpp/diagnostics/bin/usysfault [-t]
```

-s *normal*
Sets the fault indicator to the normal state.

-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 fault indicators by physical location codes.

When the command is used without the -s flag, the current state of the indicator is displayed as normal or fault.

When the command is used without the -l or -d flag, the System Attention Indicator is used.

Use the -l or -d flags only in systems that have more than one fault indicator.

Note: See also the Identify and system attention indicators.

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.

You can run this task from the AIX command line. Use the following AIX fast path command:

```
diag -T "certify"
```

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

You can run this task from the AIXcommand line. Use the following fast path command:

```
diag -T "certify"
```

Format physical disk
This selection formats a selected disk drive.

You can run this task from the AIX command line. Use the following fast path command:

```
diag -T "format"
```

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

You can run this task from the AIX command line. Use the following fast path command:

```
diag -T "download"
```

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

You can run this task from the AIX command line. Use the following fast path command:

```
diag -T "download"
```

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.

Note: There is no command-line interface for this task.

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.

This task can be run directly from the command line. The command syntax is:

```
diag -c -d deviceName -T "format [-s* fmtcert | erase -a {read | write}
         -P {comma separated list of patterns}] [-F]*
```

The following flags are not available for pdisk devices.

Flag **Description**

fmtcert
Formats and certifies the disk.

erase Overwrites the data on the disk.

***** Available in no-console mode only.

-F Forces the disk erasure even if all blocks cannot be erased because of errors when accessing the grown defect map.

-P Comma-separated list of hexadecimal patterns to be written to the drive serially. Up to eight patterns can be specified by using a single command. The patterns must be 1, 2, or 4 bytes long without a leading 0x or 0X. Example of using five patterns: -P ff, a5c0, 00, fdb97531, 02468ace

Note: If no patterns are specified for the erase disk option in command-line mode, then the default pattern of 00 is used.

Hard disk attached to PCI SCSI RAID adapter

This function formats the physical disks attached to a PCI SCSI RAID adapter. This task can be run directly from the AIX command line. The command-line syntax is:

```
diag -c -d RAIDadapterName -T "format {-l chId | -A }"
```

-l Physical disk channel/ID (An example of a physical disk channel/ID is 27, where the channel is 2 and the ID is 7.)

-A All disks

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.

This task can be run directly from the command line. The command-line syntax is:

```
diag -c -d deviceName -T "format [-s {initialize | fmtcert} ]"
```

initialize
Formats media without certifying

fmtcert
Formats and certifies 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.

This task can be run directly from the command line. The command-line syntax is:

```
diag -c -d deviceName -T"format [-s{initialize|fmtcert}]"
```

-c No console mode

-d Used to specify a device

-s initialize
Initialize the media (quick format). This setting is the default.

-s fmtcert
Formats and certifies the media.

-T Used to specify the format task

Diskette format

This selection formats a diskette by writing patterns to it.

Gather system information

If you are using the Linux operating system, the gather system information option does not apply. This service aid uses the **snap** command to collect configuration information about networks, file systems, security, the kernel, the ODM, and other system components. You can also collect SSA adapter and disk drive configuration data, or trace information for software debugging.

The output of the SNAP service aid can be used by field service personnel. The output can also be put on removable media and transferred to remote locations for more extensive analysis.

To use the SNAP task, select **Gather system information** from the task list. You can select which components you want to collect information for, and where to store the data (hard disk or removable media).

Generic microcode download

Note: Generic microcode download is a subtask that can be accessed after selecting **Microcode Tasks**, see "Microcode tasks" on page 44.

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 both concurrent and stand-alone modes 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*.

If you are running the AIX operating system, the hot plug task has a restriction when running in stand-alone or online service mode. New devices cannot be added to the system unless there is already a device with the same FRU part number installed in the system. This restriction is in place because the device software package for the new device cannot be installed in stand-alone or online service mode.

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

To run the hot plug task directly from the AIX command line, type the following command: `diag -T"identifyRemove"`

If you are running the diagnostics in online concurrent mode, run the missing options resolution procedure immediately after removing any device.

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.

PCI hot plug manager

The PCI hot plug manager task is a SMIT menu that enables you to identify, add, remove, or replace PCI adapters that are hot pluggable. The following functions are available under this task:

List PCI hot plug slots
Lists all PCI hot plug slots. Empty slots and populated slots are listed. Populated slot information includes the connected logical device. The slot name consists of the physical location code and the description of the physical characteristics for the slot.

Add a PCI hot plug adapter
Prepares a slot for the addition of a new adapter. The function lists all the empty slots that support hot plug. When a slot is selected, the visual indicator for the slot flashes at the identify rate. After the slot location is confirmed, the visual indicator for the specified PCI slot is set to the action state. This means that the power for the PCI slot is off and the new adapter can be plugged in.

Replace/remove a PCI hot plug adapter
Prepares a slot for adapter exchange. The function lists all the PCI slots that support hot plug and are occupied. The list includes the physical location code of the slot and the device name of the resource installed in the slot. The adapter must be in the defined state before it can be prepared for hot plug removal. When a slot is selected, the visual indicator for the slot is set to the identify state. After the slot location is confirmed, the visual indicator for the specified PCI slot is set to the action state. This means that the power for the PCI slot is off, and the adapter can be removed or replaced.

Identify a PCI hot plug slot
Helps identify the location of a PCI hot plug adapter. The function lists all the PCI slots that are occupied or empty and support hot plug. When a slot is selected for identification, the visual indicator for the slot is set to the identify state.

Unconfigure devices
Attempts to put the selected device, in the PCI hot plug slot, into the defined state. This action must be done before any attempted hot plug function. If the unconfigure function fails, it is possible that the device is still in use by another application. In this case, the customer or system administrator must be notified to quiesce the device.

Configure devices
Allows a newly added adapter to be configured into the system for use. This function must be used when a new adapter is added to the system.

Install/configure devices added after IPL
Attempts to install the necessary software packages for any newly added devices. The software installation media or packages are required for this function.

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

- Adapters that are replaced must be the same FRU part number as the adapter that is being replaced.
- New adapters 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 adapter is not known after the stand-alone diagnostics are booted.
- The following functions are not available from the stand-alone diagnostics and are not displayed in the list:
  - Add a PCI hot plug adapter
  - Configure devices
  - Install/configure devices added after IPL

You can run this task directly from the AIX command line by typing the following command:

```
diag -d device -T"identifyRemove"
```

However, some devices support both the PCI hot plug task and the RAID hot plug devices task. If this is the case for the *device* specified, then the hot plug task displays instead of the PCI hot plug manager menu.

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.

You can run this task directly from the AIX command line. The command-line syntax is:

```
diag -d device-T"identifyRemove"
```

OR

```
diag [-c] -d device -T"identifyRemove -a [identify?remove]"
```

-a Specifies the option under the task.

-c Run the task without displaying menus. Only command-line prompts are used. This flag is only applicable when running an option such as identify or remove.

-d Indicates the SCSI device.

-T Specifies the task to run.

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.

You can run this task directly from the AIX command line. The command syntax is:

```
diag -d device -T"identifyRemove
```

OR

```
diag -d device -T"identifyRemove -a [identify|remove ]
```

-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. The status of a device can be changed with the AIX **`smitty pdam`** command. 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.

You can run this task directly from the AIX command line. The command-line syntax is:

```
diag -c -d devicename -T "identifyRemove -l ChId -s {identify|remove|normal}
```

-c Run the task without displaying menus. Only command-line prompts are used.

-d Raid adapter device name (for example, `scraid0`).

-s Subtask to start, such as identify, remove, or normal.

-l *CHId* is the channel number of the RAID adapter and SCSI ID number of the position in the enclosure concatenated together (for example, 27 for channel 2, device 7).

-T Task to run.

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.

This task can also be run directly from the AIX command line by typing:

```
/usr/lpp/diagnostics/bin/usysident [-s {normal | identify}][-l location code | -d device name]
/usr/lpp/diagnostics/bin/usysident [-t]
```

-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.

Log repair action

The log repair action task logs a repair action in the AIX operating system error log. A repair action log indicates that a FRU has been replaced, and error log analysis should not be done for any errors logged before the repair action. The log repair action task lists all resources. Replaced resources can be selected from the list, and when **commit** (F7 key) is selected, a repair action is logged for each selected resource.

To locate the failing part in a system or partition, do the following steps:

1. Log in as root user.
2. At the command line, enter **diag**.
3. Select the **Diagnostics Routines** option.
4. When the DIAGNOSTIC MODE SELECTION menu displays, select **Problem Determination**.
5. When the ADVANCED DIAGNOSTIC SELECTION menu displays, do one of the following options:
   - To test a single resource, select the resource from the list.
   - To test all the resources available to the operating system, select All Resources.

6. Press Enter, and wait until the diagnostic programs run to completion, responding to any prompts that appear on the console.
7. Use the location information for the failing part to activate the indicator light that identifies the failing part. For instructions, see Activate the indicator light for the failing part.

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.

PCI-X SCSI disk array manager

Restriction:

- If you are using the AIX operating system, note the following restrictions:
  - There are limits to the amount of disk drive capacity allowed in a single RAID array. For example, when using the 32-bit kernel, there is a capacity limitation of 1 TB for each RAID array. When using the 64-bit kernel, there is a capacity limitation of 2 TB for each RAID array. For RAID adapters and RAID enablement cards, this limitation is enforced by the operating system when the RAID arrays are created using the PCI-X SCSI disk array manager.
  - When creating a RAID array of up to 2 TB by using stand-alone diagnostics, ensure version 5.3.0.40 or higher is used. Previous versions of the stand-alone diagnostics have a capacity limitation of 1 TB for each RAID array.

This service aid calls the **smitty pdam** fast path, and is used to manage a RAID array connected to a SCSI RAID adapter. It might also be run from stand-alone diagnostics on systems or logical partitions that are running the AIX operating system. If you are running the Linux operating system, use the iprconfig tool for disk array management.

Some of the tasks performed by using this service aid include:

- Check device status for the disk array on your system.
- Display information of physical drives and disk arrays.
- Run recovery options on the RAID. This action needs to be done at the end of a service call in which you replaced the RAID adapter cache card or changed the RAID configuration)

Other RAID functions are available by using this service aid; they must be used only by the system administrator who is familiar with the RAID configuration. These functions are normally done when booting AIX by running **smitty pdam** from the command line.

Attention: Without knowledge of how the RAID was set up, these functions can cause loss of data stored on the RAID.

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

If you are using the AIX operating system, or by using the stand-alone diagnostics, the run diagnostics task starts the resource selection list menu. When the commit key is pressed, diagnostics are run on all selected resources.

The procedures for running the diagnostics depend on the state of the diagnostics runtime options. See Display or change diagnostic run time options.

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.

If you are running the AIX operating system and are using the online diagnostics, you can run this task directly from the command line. Use the following command syntax:

```
diag -c -d devicename -T "identify"
```

-c Run the task without displaying menus. Only command-line prompts are used.

-d RAID adapter device name (for example, `scraid0`).

-T Task to run.

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

This service aid can be run directly from the AIX command line. See the following command syntax (the path is /usr/lpp/diagnostics/bin/utape):

```
utape [-h | -?] [-d device] [-n | -l | -t]
OR
utape -c -d device [-v] {-n | {-l | -t} { -D | -f [ filename]}}
```

Flag	Description
-c	Run the service aid without displaying menus. The return code indicates success or failure. The output is suppressed except for the usage statement and the numeric value for hours since cleaning (if **-n** and **-D** flags are used).
-D	Copy data to diskette.
-f	Copy data to the file name given after this flag or to a default file name if no name is specified.
-h, -?	Display a usage statement or return code. If the **-c** flag is present, only the return code displays to indicate that the service aid did not run. If the **-c** is not used, a usage statement displays and the service aid exits.
-l	Display or copy log sense information.
-n	Display time since drive was last cleaned.
-t	Copy trace table.
-v	Verbose mode. If the **-c** flag is present, the information displays on the screen. If the **-n** flag is present, the information about tape-head cleaning is printed.

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.

You can run this task directly from the AIX command line. The command syntax is:

```
diag -c -d deviceName -T chkspares
```

SSA service aid

If you are using the Linux operating system, the SSA service aid option does not apply. This service aid provides tools for diagnosing and resolving problems on SSA-attached devices. The following tools are provided:

- Set Service Mode
- Link Verification
- Configuration Verification
- Format and Certify Disk

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 disk-based diagnostics

This service aid allows fixes (APARs) to be applied.

This task starts the SMIT update software by fix (APAR) task. The task allows the input device and APARs to be selected. You can install any APAR by using this task.

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 44.
- This task has been replaced with the Update and manage system flash task, see "Update and manage system flash" on page 49.

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 or the command line in that partition.
- 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 online diagnostics, the flash update image file is copied to the `/var` file system. Put the source of the microcode that you want to download into the `/etc/microcode` directory on the system. If there is not enough space in the `/var` file system for the new flash update image file, an error is reported. If this error occurs, exit the service aid, increase the size of the `/var` file system, and try the service aid again. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue the update flash, the system reboots by using the **`shutdown -u`** command. The system does not return to the diagnostics, and the current flash image is not saved. After the reboot, you can remove the `/var/update_flash_image` file.

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.

You can use the **update_flash** command in place of this service aid. The command is in the `/usr/lpp/diagnostics/bin` directory. The command syntax is as follows:

```
update_flash [-q ]-f file_name
update_flash [-q ]-D device_name -f file_name
update_flash [-q ]-D update_flash [-q ]-D device_name -l
```

Attention: The **update_flash** command reboots the entire system. Do not use this command if more than one user is logged in to the system.

Flag	Description
-D	Specifies that the flash update image file is on diskette. The *device_name* variable specifies the device. The default *device_name* is `/dev/fd0`.
-f	Flash update image file source. The *file_name* variable specifies the fully qualified path of the flash update image file.
-l	Lists the files on a diskette, from which the user can choose a flash update image file.
-q	Forces the **update_flash** command to update the flash EPROM and reboot the system without asking for confirmation.

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 44.

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 or the AIX command line.

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 online diagnostics, the flash update image file is copied to the **/var** file system. If there is not enough space in the **/var** file system for the new flash update image file, an error is reported. If this error occurs, exit the service aid, increase the size of the **/var** file system, and try the service aid again. After the file is copied, a screen requests confirmation before continuing with the flash update. When you continue the update flash, the system reboots by using the **shutdown -u** command. The system does not return to the diagnostics, and the current flash image is not saved. After the reboot, you can remove the `/var/update_flash_image` file.

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.

If you are using online diagnostics, you can use the **update_flash** command in place of this service aid. The command is in the /usr/lpp/diagnostics/bin directory. The command syntax is as follows:

```
update_flash [-q | -v] -f file_name
update_flash [-q | -v] -D device_name -f file_name
update_flash [-q | -v] -D update_flash [-l]
update_flash -c
update_flash -r
```

Attention: The **update_flash** command reboots the entire system. Do not use this command if more than one user is logged in to the system.

Flag	Description
-D	Specifies that the flash update image file is on diskette. The *device_name* variable specifies the device. The default *device_name* is /dev/fd0.
-f	Flash update image file source. The *file_name* variable specifies the fully qualified path of the flash update image file.
-l	Lists the files on a diskette, from which the user can choose a flash update image file.
-q	Forces the **update_flash** command to update the flash EPROM and reboot the system without asking for confirmation.
-v	Validates the flash update image. No update will occur. This flag is not supported on all systems.
-c	Commits the temporary flash image when booted from the temporary image. This action overwrites the permanent image with the temporary image. This flag is not supported on all systems.
-r	Rejects the temporary image when booted from the permanent image. This action overwrites the temporary image with the permanent image. This flag is not supported on all systems.

Examples: Commands

To download the adapter microcode, use this command syntax: `diag -c -d` *deviceName* `-T "download [-B][-D][-P]"`

Flag	Description
-B	Download boot block microcode (default to functional microcode)
-D	Microcode is on diskette (default to /etc/microcode directory)
-P	Download the previous level of microcode (default to latest level)

To download physical disk microcode, use this command syntax: `diag -c -d` *deviceName* `-T "download -l` *ChId* `[-D][-P]"`

Flag	Description
-D	Microcode is on diskette (default to the /etc/microcode directory)

-l Physical disk channel/ID (for example, 27)
-P Download the previous level of microcode (default to latest level)

To format a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "format -l` *ChId*"

Flag	Description
-l	Physical disk channel/ID (for example, 27)

To certify a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "certify -l` *ChId*"

Flag	Description
-l	Physical disk channel/ID (for example, 23)

To identify a physical disk, use this command syntax: `diag -c -d` *deviceName* `-T "identify"`

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 (available from the Advanced System Management Interface) or AIX Service Aid menu to blink the field replaceable unit (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

Table 1. Component and attention LEDs (continued)

Unit (FRU)	LED Function	LED Color	Off	On	Blink
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
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. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some 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. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

IBM may use or distribute any of the information you 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 non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and

cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

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

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

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

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

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

Homologation statement

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

Privacy policy considerations

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

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

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

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information 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 POWER8™ 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 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@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 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@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 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@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

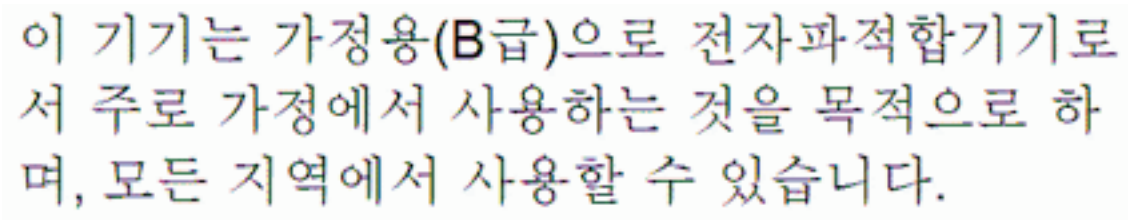
Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)

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



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 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@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