AIX 5L Version 5.1

System Management Guide: Operating System and Devices

AIX 5L Version 5.1

System Management Guide: Operating System and Devices

Fourth Edition (April 2001)

Before using the information in this book, read the general information in “Appendix. Notices” on page 199

This edition applies to AIX 5L Version 5.1 and to all subsequent releases of this product until otherwise indicated in new editions.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Publications Department, Internal Zip 9561, 11400 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial Internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.
THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. HEWLETT-PACKARD COMPANY, INTERNATIONAL BUSINESS MACHINES CORP., SUN MICROSYSTEMS, INC., AND UNIX SYSTEMS LABORATORIES, INC., MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Contents

About This Book

This book contains information for understanding the tasks that you perform as a system administrator, as well as the tools provided for system management. Use this book along with *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Who Should Use This Book

This book provides system administrators with information for performing system management tasks. The book focuses on procedures, covering such topics as starting and stopping the system and managing processes, users and groups, system security, accounting, and devices.

It is assumed that you are familiar with the information and concepts presented in the following publications:

- *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- *AIX 5L Version 5.1 System User's Guide: Operating System and Devices*
- *AIX 5L Version 5.1 System User's Guide: Communications and Networks*
- *AIX 5L Version 5.1 Installation Guide*

How to Use This Book

This book is organized to help you quickly find the information you need. The tasks of each chapter are arranged in the following order:

- Configuration tasks
- Maintenance tasks
- Troubleshooting

For conceptual information about system management tasks, see the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Highlighting

The following highlighting conventions are used in this book:

Bold — Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.

Italics — Identifies parameters whose actual names or values are to be supplied by the user.

`Monospace` — Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Related Publications

In today's computing environment, it is impossible to create a single book that addresses all the needs and concerns of a system administrator. While this guide cannot address everything, we have tried to structure the rest of our library so that a few key books can provide you with direction on each major aspect of your job.

- *AIX 5L Version 5.1 System Management Guide: Communications and Networks*
- *AIX 5L Version 5.1 Installation Guide*
- *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*
- *AIX 5L Version 5.1 Communications Programming Concepts*
- *AIX 5L Version 5.1 Kernel Extensions and Device Support Programming Concepts*
- *AIX 5L Version 5.1 Files Reference*
- *Performance Toolbox Version 2 and 3 for AIX: Guide and Reference*
- *AIX 5L Version 5.1 Network Installation Management Guide and Reference*
- *Distributed SMIT 2.2 for AIX: Guide and Reference*
- *Common Desktop Environment 1.0: Advanced User's and System Administrator's Guide*

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- AIXwindows
- CICS
- DirectTalk
- HCON
- IBM
- Proprinter
- PS/2
- RS/6000

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be the trademarks or service marks of others.

Chapter 1. Starting and Stopping the System

This chapter deals with system startup activities such as booting, creating boot images or files for starting the system, and setting the system run level. Using the **reboot** and **shutdown** commands is also covered.

The following topics are included in this chapter:

Booting an Uninstalled System

The procedure for booting a new or uninstalled system is part of the installation process. For information on how to boot an uninstalled system, see Start the System in the *AIX 5L Version 5.1 Installation Guide*.

Rebooting a Running System

There are two methods for shutting down and rebooting your system, **shutdown** and **reboot**. Always use the **shutdown** method when multiple users are logged onto the system. Because processes might be running that should be terminated more gracefully than a **reboot** permits, **shutdown** is the preferred method for all systems.

Rebooting a Running System Tasks		
Web-based System Manager	**wsm**, then select **System**	
-OR-		
Task	*SMIT Fast Path*	*Command or File*
Rebooting a Multiuser System	**smit shutdown**	**shutdown -r**
Rebooting a Single-User System	**smit shutdown**	**shutdown -r** or **reboot**

Booting from Hard Disk for Maintenance

Prerequisites

A bootable removable media (tape or CD-ROM) must not be in the drive. Also, refer to the hardware documentation for the specific instructions to enable service mode boot on your particular model.

Procedure

To boot a machine in Service mode from a hard disk:

1. To reboot, either turn the machine off and then power it back on, or press the reset button.
2. The machine will boot to a point where it has a console device configured.

   If there is a system dump that needs to be retrieved, the system dump menu will be displayed on the console.

   > **Note:** If the console fails to configure when there is a dump to be retrieved, the system will hang. The system must be booted from a removable medium to retrieve the dump.
3. If there is no system dump, or if it has been copied, the diagnostic operating instructions will be displayed. Press Enter to continue to the Function Selection menu.
4. From the Function Selection menu, you can select diagnostic or single user mode:

   Single-User Mode: To perform maintenance in a single-user environment, choose this option (option 5). The system continues to boot and enters single-user mode. Maintenance that requires the system to be in a standalone mode can be performed in this mode, and the **bosboot** command can be run, if required.

Booting a System That Crashed

In some instances, you might have to boot a system that has stopped (crashed) without being properly shut down. This procedure covers the basics of how to boot if your system was unable to recover from the crash.

Prerequisites

1. Your system crashed and was not properly shut down due to unusual conditions.
2. Your system is turned off.

Procedure

1. Ensure that all hardware and peripheral devices are correctly connected.
2. Turn on all of the peripheral devices.
3. Watch the screen for information about automatic hardware diagnostics.
   - If any hardware diagnostics tests are unsuccessful, refer to the hardware documentation.
   - If all hardware diagnostics tests are successful, go to the next step.
4. If your machine has a key, then change the key position to correspond to the service mode.
   - If the key was in the Normal position when the system crashed, it reboots automatically when the power is turned on.
   - If the key was in the Secure position, turn it to the Normal position. The key must be in the Normal position in order to perform a complete reboot.

   > **Note**: If your machine does not have a key, please see to the User Guide or documentation that came with the machine for the specific steps to boot from removable media.
5. Turn the system unit on.

Accessing a System That Will Not Boot

If you have a system that will not boot from the hard disk, see the procedure on how to access a system that will not boot in Troubleshooting in the *AIX 5L Version 5.1 Installation Guide*.

This procedure enables you to get a system prompt so that you can attempt to recover data from the system or perform corrective action enabling the system to boot from the hard disk.

Notes:

1. This procedure is intended only for experienced system managers who have knowledge of how to boot or recover data from a system that is unable to boot from the hard disk. Most users should not attempt this procedure, but should contact their service representative.
2. This procedure is not intended for system managers who have just completed a new installation, because in this case the system does not contain data that needs to be recovered. If you are unable to boot from the hard disk after completing a new installation, contact your service representative.

Rebooting a System With Planar Graphics

If the machine has been installed with the planar graphics susbsystem only, and later an additional graphics adapter is added to the system, the following occurs:

1. A new graphics adapter is added to the system, and its associated device driver software is installed.
2. The system is rebooted, and one of the following occurs:
   a. If the system console is defined to be `/dev/lft0` (**lscons** displays this information), the user is asked to select which display is the system console at reboot time. If the user selects a graphics adapter (non-TTY device), it also becomes the new default display. If the user selects a TTY device instead of an LFT device, no system login appears. Reboot again, and the TTY login screen is displayed. It is assumed that if the user adds an additional graphics adapter into the system and the system console is an LFT device, the user will not select the TTY device as the system console.
   b. If the system console is defined to be a TTY, then at reboot time the newly added display adapter becomes the default display.

      Note: Since the TTY is the system console, it remains the system console.
3. If the system console is `/def/lft0`, then after reboot, DPMS is disabled in order to show the system console selection text on the screen for an indefinite period of time. To re-enable DPMS, reboot the system again.

Diagnosing Boot Problems

A variety of factors can cause a system to be unable to boot:

- Hardware problems
- Defective boot tapes or CD-ROMs
- Improperly configured network boot servers
- Damaged file systems
- Errors in scripts such as **/sbin/rc.boot**

For information on accessing a system that will not boot from the disk drive, see “Accessing a System That Will Not Boot”.

Creating Boot Images

To install the base operating system or to access a system that will not boot from the system hard drive, you need a boot image. This procedure describes how to create boot images. The boot image varies for each type of device. The associated RAM disk file system contains device configuration routines for the following devices:

- Disk
- Tape
- CD-ROM
- Network Token-Ring, Ethernet, or FDDI device

Prerequisites

- You must have root user authority to use the **bosboot** command.
- The **/tmp** file system must have at least 20 MB of free space.
- The physical disk must contain the boot logical volume. To determine which disk device to specify, type the following at a command prompt:

  ```
  lsvg -l rootvg
  ```

  The **lsvg -l** command lists the logical volumes on the root volume group (rootvg). From this list you can find the name of the boot logical volume. Then type the following at a command prompt:

  ```
  lsvg -M rootvg
  ```

  The **lsvg -M** command lists the physical disks that contain the various logical volumes.

Creating a Boot Image on a Boot Logical Volume

If the base operating system is being installed (either a new installation or an update), the **bosboot** command is called to place the boot image on the boot logical volume. The boot logical volume is a physically contiguous area on the disk created through the Logical Volume Manager (LVM) during installation.

The **bosboot** command does the following:

1. Checks the file system to see if there is enough room to create the boot image.
2. Creates a RAM file system using the **mkfs** command and a prototype file.
3. Calls the **mkboot** command, which merges the kernel and the RAM file system into a boot image.
4. Writes the boot image to the boot logical volume.

To create a boot image on the default boot logical volume on the fixed disk, type the following at a command prompt:

```
bosboot -a
```

OR:

```
bosboot -ad /dev/ipldevice
```

> **Note:** Do not reboot the machine if the **bosboot** command fails while creating a boot image. Resolve the problem and run the **bosboot** command to successful completion.

You must reboot the system for the new boot image to be available for use.

Creating a Boot Image for a Network Device

To create a boot image for an Ethernet boot, type the following at a command prompt:

```
bosboot -ad /dev/ent
```

For a Token-Ring boot:

```
bosboot -ad /dev/tok
```

Identifying System Run Levels

Before performing maintenance on the operating system or changing the system run level, you might need to examine the various run levels. This procedure describes how to identify the run level at which the system is operating and how to display a history of previous run levels. The **init** command determines the system run level.

Identifying the Current Run Level

At the command line, type `cat /etc/.init.state`. The system displays one digit; that is the current run level. See the **init** command or the **/etc/inittab** file for more information about run levels.

Displaying a History of Previous Run Levels

You can display a history of previous run levels using the **fwtmp** command.

> **Note:** The **bosext2.acct.obj** code must be installed on your system to use this command.

1. Log in as root user.
2. Type the following at a command prompt:

   ```
   /usr/lib/acct/fwtmp </var/adm/wtmp |grep run-level
   ```

   The system displays information similar to the following:

   ```
   run-level 2  0 1 0062 0123 697081013 Sun Feb  2 19:36:53 CST 1992
   run-level 2  0 1 0062 0123 697092441 Sun Feb  2 22:47:21 CST 1992
   run-level 4  0 1 0062 0123 698180044 Sat Feb 15 12:54:04 CST 1992
   run-level 2  0 1 0062 0123 698959131 Sun Feb 16 10:52:11 CST 1992
   run-level 5  0 1 0062 0123 698967773 Mon Feb 24 15:42:53 CST 1992
   ```

Changing System Run Levels

This procedure describes two methods for changing system run levels for multi-user or single-user systems.

When the system starts the first time, it enters the default run level defined by the initdefault entry in the **/etc/inittab** file. The system operates at that run level until it receives a signal to change it.

The following are the currently defined run levels:

0-9 When the **init** command changes to run levels 0-9, it kills all processes at the current run levels then restarts any processes associated with the new run levels.

0-1 Reserved for the future use of the operating system.

2 Default run level.

3-9 Can be defined according to the user's preferences.

a, b, c When the **init** command requests a change to run levels **a**, **b**, or **c**, it does not kill processes at the current run levels; it simply starts any processes assigned with the new run levels.

Q, q Tells the **init** command to reexamine the **/etc/inittab** file.

Changing Run Levels on Multiuser Systems

1. Check the **/etc/inittab** file to confirm that the run level to which you are changing supports the processes that you are running. The getty process is particularly important, since it controls the terminal line access for the system console and other logins. Ensure that the getty process is enabled at all run levels.
2. Use the **wall** command to inform all users that you intend to change the run level and request that users log off.
3. Use the **smit telinit** fast path to access the Set System Run Level menu.
4. Type the new run level in the System RUN LEVEL field.
5. Press Enter to implement all of the settings in this procedure.

   The system responds by telling you which processes are terminating or starting as a result of the change in run level and by displaying the message:

   ```
   INIT: New run level: n
   ```

   where *n* is the new run-level number.

Changing Run Levels on Single-User Systems

1. Check the **/etc/inittab** file to confirm that the run level to which you are changing supports the processes that you are running. The getty process is particularly important, since it controls the terminal line access for the system console and other logins. Ensure that the getty process is enabled at all run levels.
2. Use the **smit telinit** fast path to access the Set System Run Level menu.
3. Type the new system run level in the System RUN LEVEL field.
4. Press Enter to implement all of the settings in this procedure.

   The system responds by telling you which processes are terminating or starting as a result of the change in run level and by displaying the message:

   ```
   INIT: New run level: n
   ```

   where `n` is the new run-level number.

Changing the /etc/inittab File

This section contains procedures for using the four commands (**chitab**, **lsitab**, **mkitab**, and **rmitab**) that modify the records in the **etc/inittab** file.

Adding Records - mkitab Command

To add a record to the **/etc/inittab** file, type the following at a command prompt:

```
mkitab Identifier:Run Level:Action:Command
```

For example, to add a record for tty2, type the following at a command prompt:

```
mkitab tty002:2:respawn:/usr/sbin/getty /dev/tty2
```

In the above example:

`tty002`	Identifies the object whose run level you are defining.
`2`	Specifies the run level at which this process runs.
`respawn`	Specifies the action that the **init** command should take for this process.
`/usr/sbin/getty /dev/tty2`	Specifies the shell command to be executed.

Changing Records - chitab Command

To change a record to the **/etc/inittab** file, type the following at a command prompt:

```
chitab Identifier:Run Level:Action:Command
```

For example, to change a record for tty2 so that this process runs at run levels 2 and 3, type:

```
chitab tty002:23:respawn:/usr/sbin/getty /dev/tty2
```

In the above example:

`tty002`	Identifies the object whose run level you are defining.
`23`	Specifies the run levels at which this process runs.
`respawn`	Specifies the action that the **init** command should take for this process.
`/usr/sbin/getty /dev/tty2`	Specifies the shell command to be executed.

Listing Records - lsitab Command

To list all records in the **/etc/inittab** file, type the following at a command prompt:

```
lsitab -a
```

To list a specific record in the **/etc/inittab** file, type:

```
lsitab Identifier
```

For example, to list the record for tty2, type: `lsitab tty2`.

Removing Records

To remove a record from the **/etc/inittab** file, type the following at a command prompt:

```
rmitab Identifier
```

For example, to remove the record for tty2, type: `rmitab tty2`.

Stopping the System

The **shutdown** command is the safest and most thorough way to halt the operating system. When you designate the appropriate flags, this command notifies users that the system is about to go down, kills all existing processes, unmounts file systems, and halts the system. The following methods for shutting down the system are covered in this section:

- "Shutting Down the System without Rebooting"
- "Shutting Down the System to Single-User Mode" on page 8
- "Shutting Down the System in an Emergency" on page 8

Shutting Down the System without Rebooting

You can use two methods to shut down the system without rebooting: the SMIT fastpath, or the **shutdown** command.

Prerequisites

You must have root user authority to shut down the system.

Procedure

To shut down the system using SMIT:

1. Log in as root.
2. At the command prompt, type:

   ```
   smit shutdown
   ```

To shut down the system using the **shutdown** command:

1. Log in as root.
2. At the command prompt, type:

   ```
   shutdown
   ```

Shutting Down the System to Single-User Mode

In some cases, you might need to shut down the system and enter single-user mode to perform software maintenance and diagnostics.

1. Type `cd /` to change to the root directory. You must be in the root directory to shut down the system to single-user mode to ensure that file systems are unmounted cleanly.
2. Type `shutdown -m`. The system shuts down to single-user mode. A system prompt displays and you can perform maintenance activities.

Shutting Down the System in an Emergency

You can also use the **shutdown** command to shut down the system under emergency conditions. Use this procedure to stop the system quickly without notifying other users.

Type `shutdown -F`. The **-F** flag instructs the **shutdown** command to bypass sending messages to other users and shut down the system as quickly as possible.

Reactivating an Inactive System

Your system canbecome inactive because of a hardware problem, a software problem, or a combination of both. This procedure guides you through steps to correct the problem and restart your system. If your system is still inactive after completing the procedure, refer to the hardware problem-determination procedure in your system operator guide.

Use the following procedures to reactivate an inactive system:

- “Checking the Hardware”
- “Checking the Processes” on page 9
- “Restarting the System” on page 11

Checking the Hardware

Check your hardware by:

- “Checking the Power”
- “Checking the Operator Panel Display” on page 9 if available
- “Activating Your Display or Terminal” on page 9

Checking the Power

If the Power-On light on your system is active, go to “Checking the Operator Panel Display” on page 9

If the Power-On light on your system is not active, check that the power is on and the system is plugged in.

Checking the Operator Panel Display

If your system has an operator panel display, check it for any messages.

If the operator panel display on your system is blank, go to “Activating Your Display or Terminal”.

If the operator panel display on your system is not blank, go to the service guide for your unit to find information concerning digits in the Operator Panel Display.

Activating Your Display or Terminal

Check several parts of your display or terminal, as follows:

- Make sure the display cable is securely attached to the display and to the system unit.
- Make sure the keyboard cable is securely attached.
- Make sure the mouse cable is securely attached.
- Make sure the display is turned on and that its Power-On light is lit.
- Adjust the brightness control on the display.
- Make sure the terminal’s communication settings are correct.

If your system is now active, your hardware checks have corrected the problem.

If your system became inactive while you were trying to restart the system, go to “Restarting the System” on page 11.

If your system did not become inactive while you were trying to restart the system, go to “Checking the Processes”.

Checking the Processes

A stopped or stalled process might make your system inactive. Check your system processes by:

- “Restarting Line Scrolling”
- “Using the Ctrl-D Key Sequence”
- “Using the Ctrl-C Key Sequence” on page 10
- “Logging In from a Remote Terminal or Host” on page 10
- “Ending Stalled Processes Remotely” on page 10

Restarting Line Scrolling

Restart line scrolling halted by the Ctrl-S key sequence by doing the following:

1. Activate the window or shell with the problem process.
2. Press the Ctrl-Q key sequence to restart scrolling.

The Ctrl-S key sequence stops line scrolling, and the Ctrl-Q key sequence restarts line scrolling.

If your scroll check did not correct the problem with your inactive system, go to the next step, “Using the Ctrl-D Key Sequence” .

Using the Ctrl-D Key Sequence

End a stopped process by doing the following:

1. Activate the window or shell with the problem process.
2. Press the Ctrl-D key sequence. The Ctrl-D key sequence sends an end of file (EOF) signal to the process. The Ctrl-D key sequence may close the window or shell and log you out.

If the Ctrl-D key sequence did not correct the problem with your inactive system, go to the next step, "Using the Ctrl-C Key Sequence" .

Using the Ctrl-C Key Sequence

End a stopped process by doing the following:

1. Activate the window or shell with the problem process.
2. Press the Ctrl-C key sequence. The Ctrl-C key sequence stops the current search or filter.

If the Ctrl-C key sequence did not correct the problem with your inactive system, go to the next step, "Logging In from a Remote Terminal or Host" .

Logging In from a Remote Terminal or Host

Log in remotely in either of two ways:

- Log in to the system from another terminal if more than one terminal is attached to your system.
- Log in from another host on the network (if your system is connected to a network) by typing the **tn** command as follows:

  ```
  tn YourSystemName
  ```

  The system asks for your regular login name and password when you use the **tn** command.

If you were able to log in to the system from a remote terminal or host, go to the next step, "Ending Stalled Processes Remotely" .

If you were not able to log in to the system from a remote terminal or host, go to "Restarting the System" on page 11 .

You can also start a system dump to determine why your system became inactive. For more information, see System Dump Facility .

Ending Stalled Processes Remotely

End a stalled process from a remote terminal by doing the following:

1. List active processes by typing the following **ps** command:

   ```
   ps -ef
   ```

   The **-e** and **-f** flags identify all active and inactive processes.
2. Identify the process ID of the stalled process.

   For help in identifying processes, use the **grep** command with a search string. For example, to end the **xlock** process, type the following to find the process ID:

   ```
   ps -ef | grep xlock
   ```

   The **grep** command allows you to search on the output from the **ps** command to identify the process ID of a specific process.
3. End the process by typing the following **kill** command:

   > **Note:** You must have root user authority to use the **kill** command on processes you did not initiate.

   ```
   kill -9 ProcessID
   ```

   If you cannot identify the problem process, the most recently activated process might be the cause of your inactive system. End the most recent process if you think that is the problem.

If your process checks have not corrected the problem with your inactive system, go to “Restarting the System” .

You can also start a system dump to determine why your system became inactive. For more information, see System Dump Facility.

Restarting the System

If the first two procedures fail to correct the problem that makes your system inactive, you need to restart your system.

> **Note:** Before restarting your system, complete a system dump. For more information, see System Dump Facility .

This procedure involves the following:

- “Checking the Position of the Mode Switch, if Available”
- “Checking the State of the Boot Device”
- “Loading the Operating System”

Checking the Position of the Mode Switch, if Available

If your system has a Mode Switch, the correct position depends on the type of software you want to load.

Position the Mode Switch according to one of the following conditions:

- Use the Normal position to load the operating system.
- Use the Service position to boot the system from maintenance mode or hardware diagnostics.

Checking the State of the Boot Device

Your system boots with either a removable medium, an external device, a small computer system interface (SCSI) device, an integrated device electronics (IDE) device, or a local area network (LAN). Decide which method applies to your system, and use the following instructions to check the boot device:

- For a removable medium, such as tape, make sure the medium is inserted correctly.
- For IDE devices, verify that the IDE device ID settings are unique per adapter. If only one device is attached to the adapter, the IDE device ID must be set to the master device.
- For an externally attached device, such as a tape drive, make sure:
  - The power to the device is turned on.
  - The device cables are correctly attached to the device and to the system unit.
  - The ready indicator is on (if the device has one).
- For external SCSI devices, verify that the SCSI address settings are unique.
- For a LAN, verify that the network is up and operable.

If the boot device is working correctly, go to “Loading the Operating System” .

Loading the Operating System

Load your operating system by doing the following:

1. Turn off your system’s power.
2. Wait one minute.
3. Turn on your system’s power.
4. Wait for the system to boot.

If the operating system failed to load, boot the hard disk from maintenance mode or hardware diagnostics.

If you are still unable to restart the system, use an SRN to report the problem with your inactive system to your service representative.

System Hang Management

System hang management allows users to run mission critical applications continuouly while improving application availablity. System hang detection alerts the system administrator of possible problems and then allows the administrator to log in as root or to reboot the system to resolve the problem.

shconf Script

The **shconf** command is invoked when `System Hang Detection` is enabled. shconf configures which events are surveyed and what actions are to be taken if such events occur.

The user can specify the five actions described below and can specify the priority level to check, the time out while no process or thread executes at a lower or equal priority, the terminal device for the warning action and the getty action:

- Log an error in **errlog** file
- Display a warning message on the system console (alphanumeric console) or on a specified TTY
- Reboot the system
- Give a special **getty** to allow the user to log in as root and launch commands
- Launch a command

For the **Launch a command** and **Give a special getty** options, SHD will launch the special **getty** or the specified command at the highest priority. The special **getty** will print a warning message specifying that it is a recovering **getty** running at priority 0. The following table lists the default values when the SHD is enabled. Only one action is enabled per type of detection.

Option	Enablement	Priority	Timeout (seconds)
Log an error in **errlog** file	disabled	60	120
Display a warning message	disabled	60	120
Give a recovering getty	enabled	60	120
Launch a command	disabled	60	120
Reboot the system	disabled	39	300

Note : When `Launch a recovering getty on a console` is enabled, the **shconf** script adds the **-u** flag to the getty line in the **inittab** that is associated with the console login.

shdaemon is a process launched by init. It is in charge of handling the detection of system hang. It retrieves configuration information, initiates working structures, and starts detection times set in by the user.

shdaemon runs at priority 0 (zero).

SMIT Interface

You can manage the SHD configuration from the SMIT `System Environments` menu. From the `System Environments` menu, select `Change / Show Characteristics of Operating System`, then `System Hang Detection`. The options in this menu allow system administrators to enable or disable the detection mechanism.

The `Manage System Hang Detection` menu contains the following items:

- “System Hang Detection Status” on page 13

- “Change / Show Current Configuration for Priority Problem Detection”

System Hang Detection Status

The System Hang Detection Status menu displays the current state (enable or disable) of the SHD feature. The only change that can be made from this option is either to enable or disable system hang detection.

Change / Show Current Configuration for Priority Problem Detection

The Change / Show Current Configuration for Priority Problem Detection menu displays the current time-out and the process priority for each action:

```
Log an Error in the Error Log                [disable]
    Detection Time-out                       [120]
    Process Priority                         [60]

Display a warning message on a console       [disable]
    Detection Time-out                       [120]
    Process Priority                         [60]
    Terminal Device                          [console]

Launch a recovering getty on a console       [enable]
    Detection Time-out                       [120]
    Process Priority                         [60]
    Terminal Device                          [console]

Launch a command                             [disable]
    Detection Time-out                       [120]
    Process Priority                         [60]
    Script                                   [ ]

Automatically REBOOT system after Detection  [disable]
    Detection Time-out                       [300]
    Process Priority                         [39]
```

Chapter 2. Security

This chapter covers advanced system security, including auditing and the Trusted Computer Base (TCB).

The following topics are covered:

- "Setting Up and Maintaining System Security"
- "Trusted Computing Base" on page 17
- "Managing Protected Resources with Access Control" on page 21
- "Setting Up Auditing" on page 22
- "Administering Loadable Authentication Modules" on page 27

For information about Light Directory Access Protocol (LDAP), see LDAP Exploitation of the Security Subsystemsection in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Setting Up and Maintaining System Security

The following guidelines are for system administrators who need to implement and to maintain basic system security.

> **Attention:** Any operating environment might have unique security requirements that are not addressed in these guidelines. To establish a secure system, system administrators might need to implement additional security measures not discussed here.

- "Setting Up Security at Installation"
- "Periodic Tasks for Maintaining System Security" on page 17
- "Security Tasks for Adding Users" on page 17
- "Security Tasks for Removing Users" on page 17

These guidelines do *not* include the following security subjects:

- Extended accounting
- Auditing
- Trusted Computing Base (TCB)
- Extended access control list functions

See Auditing Overview and "Trusted Computing Base" on page 17 for information on these security subjects.

Setting Up Security at Installation

When installing the system, set the **Install Trusted Computing Base** option to yes on the Installation and Settings menu. Leaving the value at no during installation requires you to reinstall if you later decide that you want a more secure system. Selecting yes enables trusted path, trusted shell, and system integrity checking. After you have installed the operating system and any major software packages, perform the following actions:

1. If your system is running TCP/IP, see TCP/IP Security in *AIX 5L Version 5.1 System Management Guide: Communications and Networks* for recommendations.
2. Change the root password as soon as you log in to the new system.

3. Activate minimal accounting by using the procedure in “Setting Up an Accounting System” on page 123 . However, consider not activating disk accounting and printing accounting as specified in the procedure. Both of these functions produce a large amount of data, and neither is vital to system security.
4. If necessary, change the default user attributes by using the **chsec** command to edit the **/usr/lib/security/mkuser.default** file. If you are not going to use the STAFF group as the system default, set the *pgrp* variable to the name of the default group for your system. Set your default to the group with the least privileges to sensitive data on your system.
5. Set the minimum password criteria by using the **chsec** command to edit the default stanza of the **/etc/security/user** file, or by using the **chuser** command to set password restrictions on specific users in the **/etc/security/user** file. Set the password criteria to the ones specified in the table of Recommended, Default, and Maximum Password Attribute Values .
6. Define the TMOUT and TIMEOUT values in the **/etc/ profile** file.
7. Run the **tcbck** command to establish a baseline of the Trusted Computing Base (TCB). Print the **/etc/security/sysck.cfg** configuration file. Fix any problems now, and store the printout of the configuration file in a secure place.
8. Run the **errpt** command now. The **errpt** command reports software and hardware errors logged by the system.
9. If you are going to configure the **skulker** command, modify the default **cron** job in the **/usr/spool/cron/crontabs/root** file to send the output of the **skulker** command to a file for review.

   Note: Unless you have special system requirements, it is not generally recommended that you configure the **skulker** command.
10. Create a list of all directories and files in the system at this point. Change to the **/** (root) directory with the **cd** command, and then use the **su** command to gain root privilege. Type the following command:

    ```
    ls -Ra -l -a > listofallfiles
    ```

    If possible, print the `listofallfiles` file (it is several thousand lines long). Store the printout in a secure place to refer to later if your system develops problems.
11. Turn the system key (if present) to the Normal position. Remove the key, and store it in a secure location. In the Normal position the system can be rebooted, but not into Service mode, thus preventing anyone from resetting the root password. Single-user systems can leave the key in the Normal position.

    If you also want to prevent users from rebooting the machine at all, set the key to the Secure position. This is recommended for multiuser systems.
12. Create the initial user IDs for the system.
13. Decide if your system is to run continuously or is to be shut down every evening.

    Most multiuser systems should run continuously, although display terminals are shut off when not in use.

    If the system is shut down in the evenings, reschedule those **cron** jobs that the system sets to run at 3 a.m. every morning. These jobs include tasks such as daily accounting and the removal of unnecessary files, both of which have an impact on system security. Use the **at** command to check the **cron** jobs schedule for when your machine is off, and reschedule them for other times.

    If your system is going to run 24 hours a day, consider disabling all remote or dial-in terminals at the end of the day (or whenever no authorized users would be using them). You might want to set a **cron** job to do this automatically.

    Ensure that all the system-scheduled **cron** jobs, such as accounting and auditing report generation, do not start at the same time. If you have directed the output of these operations to a single file, the output for these reports could be interleaved, making them hard to read.

Periodic Tasks for Maintaining System Security

Performed the following tasks periodically.

- Perform system backups and check the backup tapes, probably weekly.
- Use the **tcbck** command daily or weekly.
- Run the **grpck**, **pwdck**, and **usrck** commands daily, or at least weekly.
- Update the **/etc/security/sysck.cfg** file whenever important files or **suid** programs are added to the system.
- Check the accounting output weekly.
- Run the **errpt** command periodically, at least weekly.

  The error logging system is active as long as the **errdemon** is running; the **errdemon** is started automatically when the system is booted. For more information about error logging, see the Error Logging Overview in *Messages Guide and Reference*.
- If you are using auditing, check the output at least weekly and back up the auditing output periodically. Auditing output grows quickly. Reduced the size of the files periodically.

Security Tasks for Adding Users

Perform the following tasks when adding users:

1. Assign users to appropriate groups.
2. Set initial passwords.
3. Explain to users how to create acceptable passwords. Ensure that users change their initial passwords when they first log in, and ensure they follow the password guidelines.
4. Give a written statement of your security policies to new users. The statement should include:
   - The policy on unattended terminals
   - The password policy
   - Directories users can safely use to store their own data

Security Tasks for Removing Users

When a user is removed from the system, perform the following tasks:

1. If the user is only being removed temporarily, consider just removing the ability of the user ID to log in to the system. For more information, see “Chapter 4. Users and Groups” on page 35.
2. If the user is being removed permanently, remove all the user information. See “Chapter 4. Users and Groups” on page 35 for more information.
3. Recover the system key (if present) from the user.
4. Remove or reassign all the user’s files on the system. You can use the **find** command to produce a list of all files owned by a user.
5. Remove any **at** jobs the user has scheduled. A user can schedule potentially damaging programs to run long after the user is removed from the system by using the **at** command.

Trusted Computing Base

The system administrator must determine how much trust can be given to a particular program. This determination includes considering the value of the information resources on the system in deciding how much trust is required for a program to be installed with privilege.

Checking the Trusted Computing Base

The **tcbck** command audits the security state of the Trusted Computing Base. The security of the operating system is jeopardized when the TCB files are not correctly protected or when configuration files have unsafe values. The **tcbck** command audits this information by reading the **/etc/security/sysck.cfg** file. This file includes a description of all TCB files, configuration files, and trusted commands.

> **Note:** If the **Install Trusted Computing Base** option was not selected during the initial installation, the **tcbck** command is disabled. The command can be correctly enabled only by reinstalling the system.

Using the tcbck Command

The **tcbck** command is normally used to:

- Assure the proper installation of security-relevant files
- Assure that the file system tree contains no files that clearly violate system security
- Update, add, or delete trusted files

The **tcbck** command can be used in three ways:

- Normal use
  - Noninteractive at system initialization
  - With the **cron** command
- Interactive use
  - Useful for checking out individual files and classes of files
- Paranoid use
  - Store the **sysck.cfg** file offline and restore it periodically to check out the machine

Checking Trusted Files

Run the **tcbck** command to check the installation of trusted files at system initialization. To perform this automatically and produce a log of what was in error, add the following command to the **/etc/rc** file:

```
tcbck -y ALL
```

This causes the **tcbck** command to check the installation of each file described by the **/etc/security/sysck.cfg** file.

Checking the File System

Run the **tcbck** command to check the file system any time you suspect the integrity of the system might have been compromised. This is done by issuing the following command:

```
tcbck -t tree
```

When the **tcbck** command is used with the *tree* parameter, all files on the system are checked for correct installation (this could take a long time). If the **tcbck** command discovers any files that are potential threats to system security, you can alter the suspected file to remove the offending attributes. In addition, the following checks are performed on all other files in the file system:

- If the file owner is root and the file has the **setuid** bit set, the **setuid** bit is cleared.
- If the file group is an administrative group, the file is executable, and the file has the **setgid** bit set, the **setgid** bit is cleared.
- If the file has the **tcb** attribute set, this attribute is cleared.
- If the file is a device (character or block special file), it is removed.
- If the file is an additional link to a path name described in **/etc/security/sysck.cfg** file, the link is removed.
- If the file is an additional symbolic link to a path name described in **/etc/security/sysck.cfg** file, the symbolic link is removed.

Note: All device entries must have been added to the **/etc/security/sysck.cfg** file prior to execution of the **tcbck** command or the system is rendered unusable. Use the **-l** flag to add trusted devices to **/etc/security/sysck.cfg**.

Adding a Trusted Program

To add a specific program to the **/etc/security/sysck.cfg** file, type:

```
tcbck -a PathName [attribute=value]
```

Only attributes whose values are not deduced from the current state of the file need be specified on the command line. All attribute names appear in the **/etc/security/sysck.cfg** file.

For example, the following command registers a new setuid-root program named **/usr/bin/setgroups**, which has a link named **/usr/bin/getgroups**:

```
tcbck -a /usr/bin/setgroups links=/usr/bin/get
groups
```

After installing a program, you might not know which new files are registered in the **/etc/security/sysck.cfg** file. These can be found and added with the following command:

```
tcbck -t tree
```

This command displays the name of any file that is to be registered in the **/etc/security/sysck.cfg** file.

Deleting a Trusted Program

If you remove a file described in the **/etc/security/sysck.cfg** file, also remove the description of this file. For example, if you have deleted the **/etc/cvid** program, the following command cause an error message to be shown:

```
tcbck -t ALL
```

The error message shown is:

```
3001-020 The file /etc/cvid was not found.
```

The description of this program can be removed with the following command:

```
tcbck -d /etc/cvid
```

Configuring the tcbck Program

The **tcbck** command reads the **/etc/security/sysck.cfg** file to determine which files to check. Each trusted program on the system is described by a stanza in the **/etc/security/sysck.cfg** file.

Each stanza has the following attributes:

class Name of a group of files. This attribute allows several files with the same class name to be checked by specifying a single argument to the **tcbck** command. More than one class can be specified, with each class being separated by a comma.

owner User ID or name of the file owner. If this does not match the file owner, the **tcbck** command sets the owner ID of the file to this value.

group Group ID or name of the file group. If this does not match the file owner, the **tcbck** command sets the owner ID of the file to this value.

mode Comma-separated list of values. The allowed values are SUID, SGID, SVTX, and TCB. The file permissions must be the last value and can be specified either as an octal value or as a 9-character string. For example, either **755** or **rwxr-xr-x** are valid file permissions. If this does not match the actual file mode, the **tcbck** command applies the correct value.

links Comma-separated list of path names linked to this file. If any path name in this list is not linked to the file, the **tcbck** command creates the link. If used without the *tree* parameter, the **tcbck** command prints a message that there are extra links but does not determine their names. If used with the *tree* parameter, the **tcbck** command also prints any additional path names linked to this file.

symlinks Comma-separated list of path names symbolically linked to this file. If any path name in this list is not a symbolic link to the file, the **tcbck** command creates the symbolic link. If used with the *tree* argument, the **tcbck** command also prints any additional path names that are symbolic links to this file.

program Comma-separated list of values. The first value is the path name of a checking program. Additional values are passed as arguments to the program when it is executed.

> **Note:** The first argument is always one of **-y**, **-n**, **-p**, or **-t**, depending on which flag the **tcbck** command was used with.

acl Text string representing the access control list for the file. It must be of the same format as the output of the **aclget** command. If this does not match the actual file ACL, the **sysck** command applies this value using the **aclput** command.

> **Note:** Note that the attributes SUID, SGID, and SVTX must match those specified for the mode, if present.

source Name of a file this source file is to be copied from prior to checking. If the value is blank, and this is either a regular file, directory, or a named pipe, a new empty version of this file is created if it does not already exist. For device files, a new special file is created for the same type device.

If a stanza in the **/etc/security/sysck.cfg** file does not specify an attribute, the corresponding check is not performed.

The **tcbck** command provides a way to define and maintain a secure software configuration. The **tcbck** command also ensures that all files maintained by its database are installed correctly and have not been modified.

Restricting Access to a Terminal

The **getty** and **shell** commands change the owner and mode of a terminal to prevent untrusted programs from accessing the terminal. The operating system provides a way to configure exclusive terminal access.

Using the Trusted Communication Path

A trusted communication path is established by pressing the SAK reserved key sequence (Ctrl-X, Ctrl-R). A trusted communication path is established under the following conditions:

- When logging in to the system.

  After you press the SAK:

  - If a new login screen scrolls up, you have a secure path.
  - If the trusted shell prompt is displayed, the initial login screen was an unauthorized program that might have been trying to steal your password. Find out who is currently using this terminal with the **who** command and then log off.
- When you want the command you enter to result in a trusted program running. Some examples of this include:
  - Running as root user. Run as root user only after establishing a trusted communication path. This ensures that no untrusted programs are run with root user authority.
  - Running the **su**, **passwd**, and **newgrp** commands. Run these commands only after establishing a trusted communication path.

  Attention: Use caution when using SAK; it kills all processes that attempt to access the terminal and any links to it (for example, **/dev/console** can be linked to **/dev/tty0**).

Configuring the Secure Attention Key

Each terminal can be independently configured so that pressing SAK at that terminal creates a trusted communication path. This is specified by the **sak_enabled** attribute in **/etc/security/login.cfg** file. If the value of this attribute is True, recognition of the SAK is enabled.

If a port is to be used for communications, (for example, by the **uucp** command), the specific port used has the following line in its stanza of the **/etc/security/login.cfg** file:

```
sak_enabled = false
```

This line or no entry disables the SAK for that terminal.

To enable SAK on a terminal, add the following line to the stanza for that terminal:

```
sak_enabled = true
```

Managing Protected Resources with Access Control

Access control also involves managing protected resources using the **setuid** and **setgid** programs and hard-copy labeling. The operating system supports several types of information resources, or objects. These objects allow user processes to store or communicate information.

The most important types of objects are:

- Files and directories (used for information storage)
- Named pipes, message queues, shared memory segments, and semaphores (used for information transfer between processes)

Each object has an associated owner, group, and mode. The mode defines access permissions for the owner, group, and other users.

The following are the direct access control attributes for the different types of objects:

Owner The owner of a specific object controls its discretionary access attributes. The owner's attributes are set to the creating process's effective user ID. For file system objects, the direct access control attributes for an owner cannot be changed without root privilege.

For System V Interprocess Communication (SVIPC) objects, either the creator or owner can change the owner. SVIPC objects have an associated creator that has all the rights of the owner (including access authorization). However, the creator cannot be changed, even with root privilege.

Group SVIPC objects are initialized to the effective group ID of the creating process. For file system objects, the direct access control attributes are initialized to either the effective group ID of the creating process or the group ID of the parent directory (this is determined by the group inheritance flag of the parent directory).

The owner of an object can change the group; the new group must be either the effective group ID of the creating process or the group ID of the parent directory. The owner of an object can change the group; the new group must be either the effective group or in the supplementary group ID of the owner's current process. (As above, SVIPC objects have an associated creating group that cannot be changed and share the access authorization of the object group.)

For more information about access control lists, see ″Access Control List″ in the *AIX 5L Version 5.1 System User's Guide: Operating System and Devices*.

Using setuid and setgid Programs

The permission bits mechanism allows effective access control for resources in most situations. But for more precise access control, the operating system provides **setuid** and **setgid** programs.

Most programs execute with the user and group access rights of the user who invoked them. Program owners can associate the access rights of the user who invoked them by making the program a **setuid** or **setgid** program; that is, a program with the setuid or setgid bit set in its permissions field. When that program is executed by a process, the process acquires the access rights of the owner of the program. A **setuid** program executes with the access rights of its owner, while a **setgid** program has the access rights of its group and both bits can be set according to the permission mechanism.

Although the process is assigned the additional access rights, these rights are controlled by the program bearing the rights. Thus, the **setuid** and **setgid** programs allow for user-programmed access controls in which access rights are granted indirectly. The program acts as a trusted subsystem, guarding the user's access rights.

Although these programs can be used with great effectiveness, there is a security risk if they are not designed carefully. In particular, the program must never return control to the user while it still has the access rights of its owner, because this would allow a user to make unrestricted use of the owner's rights.

> **Note:** For security reasons, the operating system does not support **setuid** or **setgid** calls within a shell script.

Administrative Access Rights

The operating system provides privileged access rights for system administration. System privilege is based on user and group IDs. Users with effective user or group IDs of 0 are recognized as privileged.

Processes with effective user IDs of 0 are known as root user processes and can:

- Read or write any object
- Call any system function
- Perform certain subsystem control operations by executing **setuid-root** programs.

You can manage the system using two types of privilege: the **su** command privilege and **setuid-root** program privilege. The **su** command allows all programs you invoke to function as root user processes, and **su** is a flexible way to manage the system, but it is not very secure.

Making a program into a **setuid-root** program means the program is a root user-owned program with the setuid bit set. A **setuid-root** program provides administrative functions that ordinary users can perform without compromising security; the privilege is encapsulated in the program rather than granted directly to the user.

It can be difficult to encapsulate all necessary administrative functions in **setuid-root** programs, but it provides more security to system managers.

Setting Up Auditing

Procedure

The following is an overview of the steps you must take to set up an auditing subsystem. Refer to the configuration files noted in these steps for more specific information.

1. Select system activities (events) to audit from the list in the **/etc/security/audit/events** file or edit the file to add a new event.
   - You only add an event to this file, only if you have included code to log that event in an application program (using the **auditwrite** or **auditlog** subroutine) or in a kernel extension (using the **audit_svcstart**, **audit_svcbcopy**, and **audit_svcfinis** kernel services).
   - Ensure that formatting instructions for any new audit events are included in the **/etc/security/audit/events** file. These specifications enable the **auditpr** command to write an audit trail when it formats audit records.

2. Group your selected audit events into sets of similar items called audit classes. Define these audit classes in the classes stanza of the **/etc/security/audit/config** file.
3. Assign the audit classes to the individual users and assign audit events to the files (objects) that you want to audit, as follows:
   - To assign audit classes to an individual user, add a line to the users stanza of the **/etc/security/audit/config** file. You can use the **chuser** command to assign audit classes to a user.
   - To assign audit events to an object (data or executable file), add a stanza for that file to the **/etc/security/audit/objects** file.
4. Configure the type of data collection that you want, using BIN collection, STREAM collection, or both methods:
   - *To configure BIN collection*:
     - Edit the start stanza in the **/etc/security/audit/config** file to enable BIN collection.
     - Edit the binmode stanza in the **/etc/security/audit/config** file to configure the bins and trail, and specify the path of the file containing the binmode back-end processing commands. The default file for back-end commands is the **/etc/security/audit/bincmds** file.
     - Include the shell commands that process the audit bins in an audit pipe in the **/etc/security/audit/bincmds** file.
   - *To configure STREAM collection*:
     - Edit the start stanza in the **/etc/security/audit/config** file to enable STREAM collection.
     - Edit the streammode stanza in the **/etc/security/audit/config** file to specify the path to the file containing the streammode processing commands. The default file containing this information is the **/etc/security/audit/streamcmds** file.
     - Include the shell commands that process the stream records in an audit pipe in the **/etc/security/audit/streamcmds** file.
5. When you have finished making any necessary changes to the configuration files, you are ready to enable the audit subsystem using the **audit** command.

Selecting Audit Events

The purpose of an audit is to detect activities that might compromise the security of your system. When performed by an unauthorized user, the following activities violate system security and are candidates for an audit:

- Engaging in activities in the Trusted Computing Base
- Authenticating users
- Accessing the system
- Changing the configuration of the system
- Circumventing the auditing system
- Initializing the system
- Installing programs
- Modifying accounts
- Transferring information into or out of the system

To audit an activity, you must identify the command or process that initiates the audit event and ensure that the event is listed in the **/etc/security/audit/events** file for your system. Then you must add the event either to an appropriate class in the **/etc/security/audit/config** file, or to an object stanza in the **/etc/security/audit/objects** file. See the **/etc/security/audit/events** file on your system for the list of audit events and trail formatting instructions. See the **auditpr** command for a description of how audit event formats are written and used.

Once you have selected the events to audit, you need to combine similar events into audit classes, as described in the section on selecting audit classes. Audit classes are then assigned to users.

Selecting Audit Classes

You can facilitate the assignment of audit events to users by combining similar events into sets called audit classes. These audit classes are defined in the classes stanza of the **/etc/security/audit/config** file.

Some typical audit classes might be:

general General events alter the state of the system and change user authentication. Audit attempts to circumvent system access controls.

system Events in the system group modify user and group accounts and install programs.

init Events in the init group are generated by the **init** program and its immediate descendants, the **login** and **cron** programs.

An example of a stanza in the **/etc/security/audit/config** file follows:

```
classes:
general = USER_SU,PASSWORD_Change,FILE_Unlink,
    FILE_Link,FILE_Rename
system = USER_Change,GROUP_Change,USER_Create,
    GROUP_Create
init = USER_Login,USER_Logout
```

Selecting an Audit Data Collection Method

Your selection of a data collection method depends on how you intend to use the audit data. If you need long-term storage of a large amount of data, select bin collection. If you want to process the data as it is collected, select stream collection. If you need both long-term storage and immediate processing, select both methods.

Bin collection Bin collection lets you store a large audit trail for a long time. Audit records are written to a file that serves as a temporary bin. After the file is filled, the data is processed by the **auditbin** daemon, and records are written to an audit trail file for storage.

Stream collection Stream collection lets you process audit data as it is collected. Audit records are written into a circular buffer within the kernel, and are retrieved by reading **/dev/audit**. The audit records can be displayed, printed to provide a paper audit trail, or converted into bin records by the **auditcat** command.

PKCS #11 Overview

> **Note:** The information in this section is specific to the POWER-based platform.

The PKCS #11 subsystem provides applications a method for accessing hardware devices (tokens) in a device neutral manner. The content in this document conforms to Version 2.01 of the PKCS #11 standard.

This subsystem has been implemented using three components:

- A slot manager daemon (**pkcsslotd**) which provides the subsystem with information regarding the state of available hardware devices. This daemon is started automatically during installation and when the system is rebooted.
- An API shared object (**/usr/lib/pkcs11/pkcs11_API.so**) is provided as a generic interface to the adapters for which PKCS #11 support has been implemented.
- An adapter specific library which provides the PKCS #11 support for the adapter. This tiered design allows the user to easily use new PKCS #11 devices when they come available with no recompilations of existing applications.

IBM 4758 Model 2 Cryptographic Coprocessor

The IBM 4758 Model 2 Cryptographic Coprocessor provides a secure computing environment. Before attempting to configure the PKCS #11 subsystem, verify that the adapter has been properly configured with a supported microcode.

Verifying the IBM 4758 Model 2 Cryptographic Coprocessor for use with the PKCS #11 subsystem

The PKCS #11 subsystem is designed to automatically detect adapters capable of supporting PKCS #11 calls during installation and at reboot. For this reason, any IBM 4758 Model 2 Cryptographic Coprocessor which is not properly configured will not be accessible from the PKCS #11 interface and calls sent to the adapter will fail. Complete the following to verify that your adapter is set up correctly:

1. Ensure that the software for the adapter is properly installed using the following command:

   ```
   lsdev -Cc adapter | grep crypt
   ```

   If the IBM 4758 Model 2 Cryptographic Coprocessor does not show in the resulting list, check that the card is seated properly and that the supporting software is correctly installed.
2. Determine that the proper firmware has been loaded onto the card using the **csufclu** utility:

   ```
   csufclu /tmp/l ST device_number_minor
   ```

   Verify that the Segment 3 Image has the PKCS #11 Application loaded. If it is not loaded refer to the adapter specific documentation to obtain the latest microcode and installation instructions.

   Note: If this utility is not available, then the supporting software has not been installed.

PKCS #11 Usage

Note: The information in this section is specific to POWER-based.

For an application to use the PKCS #11 subsystem, the subsystem's slot manager daemon must be running and the application must load in the API's shared object.

The slot manager is normally started at boot time by **inittab** calling the **/etc/rc.pkcs11** script. This script verifies the adapters in the system before starting the slot manager daemon. As a result, the slot manager daemon is not available before the user logs on to the system. After the daemon starts, the subsystem incorporates any changes to the number and types of supported adapters without intervention from the systems administrator.

The API can be loaded either by linking in the object at runtime or by using deferred symbol resolution. For example, an application can get the PKCS #11 function list in the following manner:

```
d CK_RV (*pf_init)();
void *d;
CK_FUNCTION_LIST *functs;

d = dlopen(e, RTLD_NOW);
if ( d == NULL ) {
   return FALSE;
}

pfoo = (CK_RV (*)())dlsym(d, "C_GetFunctionList");
if (pfoo == NULL) {
   return FALSE;
}

rc = pf_init(&functs);
```

PKCS #11 Subsystem Configuration

Note: The information in this section is specific to the POWER-based platform.

The PKCS #11 subsystem automatically detects devices supporting PKCS #11. However, in order for some applications to use these devices, some initial set up is necessary. These tasks include:

- "Initializing the Token"
- "Setting the Security Officer PIN"
- "Initializing the User PIN"

These tasks can be performed through the API (by writing a PKCS #11 application) or by using the SMIT interface. The PKCS #11 SMIT options are accessed either through `Manage the PKCS11 subsystem` off the main SMIT menu, or by using the **smit pkcs11** fastpath.

Initializing the Token

Each adapter or PKCS #11 token must be initialized before it can be used successfully. This initialization procedure involves setting a unique label to the token. This label allows applications to uniquely identify the token. Therefore, the labels should not be repeated. However; the API does not verify that labels are not re-used. This initialization can be done through a PKCS #11 application or by the system administrator using SMIT. If your token has a Security Officer PIN, the default value is set to 87654321. To ensure the security of the PKCS #11 subsystem, this value should be changed after initialization.

To initialize the token:

1. Enter the token management screen by typing `smit pkcs11`
2. Select `Initialize a Token`
3. Select a PKCS #11 adapter from the list of supported adapters.
4. Confirm your selection by pressing enter.

   Note: This will erase all information on the token.
5. Enter the Security Officer PIN (SO PIN) and a unique token label.

If the correct PIN is entered, the adapter will be initialized or reinitialized after the command has finished execution.

Setting the Security Officer PIN

If your token has an SO PIN, you can change the PIN from its default value. To do this:

1. Type `smit pkcs11`.
2. Select `Set the Security Officer PIN`.
3. Select the initialized adapter for which you want to set the SO PIN.
4. Enter the current SO PIN and a new PIN.
5. Verify the new PIN.

Initializing the User PIN

After the token has been initialized, it might be necessary to set the user PIN to allow applications to access token objects. Refer to your device specific documentation to determine if the device requires a user to log in before accessing objects.

To initialize the user PIN:

1. Enter the token management screen typing `smit pkcs11`.
2. Select `Initialize the User PIN`.

3. Select a PKCS #11 adapter from the list of supported adapters.
4. Enter SO PIN and the User PIN
5. Verify the User PIN
6. Upon verification, the User PIN must be changed

Resetting the User PIN

If you wish to reset the user PIN, you can either reinitialize the PIN using the SO PIN or set the user PIN by using the existing user PIN. To do this:

1. Enter the token management screen by typing `smit pkcs11`.
2. Select `Set the User PIN`.
3. Select the initialized adapter for which you want to set the user PIN.
4. Enter the current user PIN and a new PIN.
5. Verify the new user PIN.

Setting the PKCS #11 Function Control Vector

Your token might not support strong cryptographic operations without loading a function control vector. Please refer to your device specific documentation to determine if your token needs a function control vector and where to locate it.

If a function control vector is required you should have a key file. To load the function control vector:

1. Enter the token management screen by typing `smit pkcs11`.
2. Select `Set the function control vector`.
3. Select the PKCS #11 slot for the token.
4. Enter the path to the function control vector file.

Administering Loadable Authentication Modules

Loadable authentication modules allow the system administrator to extend the Identification and Authentication functions of the system. The standard administrative commands, such as **mkuser** and **chuser**, may be used to administer user information for these loadable authentication modules as though the users were locally defined. Some loadable authentication modules, such as the DCE module, may only support a limited number of operations, such as logging in, changing user identity or executing remote commands. Others, such as the LDAP module, support the full range of functions provided by the local user databases.

Loadable authentication modules are defined in the **/usr/lib/security/methods.cfg** file. Each stanza within that file defines a method which may be used by the administrator to create, delete, modify and view a user or group account. Once the accounts have been established, they may be used in the same manner as local accounts defined in the **/etc/passwd** and the **/etc/group** files.

> **Note:** Loadable authentication modules may not support all operations. Please refer to the documentation for each module to determine which operations are supported.

Administrative commands support a **-R** *module* option which may be used to specify the desired module. *Module* is the name of a stanza given in the **/usr/lib/security/methods.cfg** file. When an account is created a module name may be given to specify where the account is created. This module name will be used for all administrative operations performed on the account. Accounts which are unique do not require the use of the **-R** flag once the account has been created. The command will determine the name of the module for the account and automatically use that module for the operation.

User and group accounts which reside in a loadable authentication module can be administered by Web-based System Manager. The **lsuser** and **lsgroup** commands support discovering the name of all accounts provided that the loadable authentication module is capable of producing a list of all known users or groups. Please refer to the documentation for each module to determine if this functionality is provided.

Managing Loadable Authentication Modules

Loadable authentication modules may be either a single loadable module, known as a simple load module, or a pair of loadable modules combined to form a compound load module. Compound load modules combine the data storage functions of one module with the authentication functions of another module.

Simple Load Modules

A simple load module is defined by a single stanza in the **methods.cfg** file. The stanza defines the name that is used by the administrative commands and the **SYSTEM** and **registry** attributes in the **/etc/security/user** file. The **program** attribute specifies the location of the loadable module. The **program_64** attribute is used for the 64-bit environment.

This example shows the configuration of the LDAP simple loadable authentication module:

```
LDAP:
    program = /usr/lib/security/LDAP
    program_64 = /usr/lib/security/LDAP64
```

Compound Load Modules

A compound load module is defined by two or three stanzas in the **methods.cfg** file. A compound load module is formed when functions from a data storage and retrieval module are combined with functions from an authentication module. Each module can be defined separately and a third stanza can be defined to combine the two.

These examples show how the LDAP module can be combined with the AFS authentication module to provide AFS authentication for LDAP users. The following example adds AFS authentication to the LDAP module.

```
AFS:
    program = /usr/lib/security/AFS
    options = authonly

LDAP:
    program = /usr/lib/security/LDAP
    program_64 = /usr/lib/security/LDAP64
    options = auth=AFS
```

This example shows how the LDAP and AFS modules may be defined separately, then combined in the third stanza to provide the same function as the previous example. This method is used when users are defined in a single database, but are configured to authenticate with more than one authentication mechanism.

```
AFS:
    program = /usr/lib/security/AFS
    options = authonly

LDAP:
    program = /usr/lib/security/LDAP
    program_64 = /usr/lib/security/LDAP64

LDAPAFS:
    options = auth=AFS,db=LDAP
```

Note: User and group accounts may appear to be defined in more than one location if a data storage and retrieval module is used by more than one stanza. To avoid confusion, use the `auth=` option to change a module's authentication method. If different user's within the module use different authentication methods, consider using the **SYSTEM** attribute instead of a compound load module.

A module which is referenced by another stanza must have been defined prior to the reference. A stanza which references a stanza which has not yet been defined will be ignored.

A stanza which appears as the target of a `db=` or `auth=` option will be excluded from the list of loadable modules to use when a command does not request a specific module. A stanza may be referenced in than one compound module stanza. This may result in accounts appearing to be defined in more than one module.

Security

Each module provides its own security policy for administering user and group accounts. The module may grant administrative privileges to the root user, or it may require that the user acquire privilege in some other manner. Please refer to the documentation for the loadable authentication module for more details.

User and Group Management

Each loadable module defines a set of users and groups. The user and group definitions must be completely self-contained by the loadable module. Group accounts which are referenced by a user account must be defined within the same loadable module. User accounts which are members of group accounts must be defined there as well.

Privileges and access rights are granted based on a process's effective user and group identifier, not the name of the user or group. When multiple methods define the same user or group name the numerical identifier must be the same in all methods.

Creating User and Group Accounts

The same tools used for creating local user and group accounts are used to create user and group accounts. The default module name is stored in the **/usr/lib/security/mkuser.default** file in the **registry** attribute. The **mkuser** and **mkgroup** commands examine this attribute and, if present, use that module name to create the new account. The web-based system administration tools support account creation in loadable modules using the same mechanism. The default module name may be overriden with the **-R** flag to both commands. The web-based system administration tools do not support the **-R** flag and will only create accounts in the default registry.

Viewing User and Group Account Definitions

The **lsuser** and **lsgroup** commands display user and group account information. The commands search all available loadable modules for the account and report the information from the first module where the account is stored. A specific module may be requested with the **-R** flag.

A loadable authentication module may optionally support providing the names of all defined accounts. This is used by the commands when **ALL** is specified as the account name. This operation may take a considerable amount of time to complete as all account definitions are examined.

All modules provide some amount of support for viewing account information. A module is not required to support all user or group attributes. For a user account the minimum requirement is user name, password, user ID, primary group ID, full name, login directory and login shell. For a group account the minimum requirement is group name, group ID and group membership list.

Managing User and Group Accounts

User and group accounts are managed with a variety of commands. The procedures described in "Chapter 4. Users and Groups" on page 35 apply to loadable authentication modules as well. The commands accept an optional **-R** flag which is used to indicate where the account is defined. If the **-R** flag is not provided the command will query the **registry** attribute for the account then use that module for the operation.

Some modules do not support requests to modify account information. Commands which attempt to modify account information will report an error when an attribute is modified. Modules which do not support integrated account management must provide their own tools for administering accounts.

Removing User and Group Accounts

User and group accounts are removed with the **rmuser** and **rmgroup** commands. Load modules are not required to support this function. Attempting to remove an account from a loadable authentication module which does not provide this function will result in an error message.

Compound load modules remove an account from both modules when a request is made to remove an account. To remove the account from only one module you must use the **-R** flag to name the module with the account to be removed.

Chapter 3. Administrative Roles

AIX supports assigning portions of root user authority to non-root users. Different root user tasks are assigned different authorizations. These authorizations are grouped into roles and assigned to different users.

This chapter covers the following topics:

- "Setting Up and Maintaining Roles"
- "CE Login"
- "Working with Authorizations" on page 32
- "Managing Backup and Restore Roles" on page 32

Setting Up and Maintaining Roles

SMIT fast paths (shown in the following table) are available for implementing and maintaining roles.

Setting Up and Maintaining Roles Tasks	
Task	*SMIT Fast Path*
Add a Role	**smit mkrole**
Change Characteristics of a Role	**smit chrole**
Show Characteristics of a Role	**smit lsrole**
Remove a Role	**smit rmrole**
List All Roles	**smit lsrole**

CE Login

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

- Run diagnostics including service aids (for example, hot plug tasks, certify, format, etc.)
- Run all commands that can be run by a group **system**
- Configure and unconfigure devices that are not busy.

In addition, group **shutdown** is required to:

- Use the service aid to update system microcode
- Perform the **shutdown** and **reboot** operations.

To use CE Login:

1. Create a unique user name for your service provider.
2. Configure these characteristics for that user. For more information, see "Chapter 4. Users and Groups" on page 35 in *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*.
3. Give the new user name and password to your service provider to use when working on your system.

   Note: If you have several RS/6000 systems, you might want to set up an account on each system. It is recommended that you use the same user name and password on each system. The recommended CE login user name is **qserv**.

Working with Authorizations

Command to Authorization List

The following table lists the commands and the authorizations they use. For detailed information about each of these commands, see “Working with Authorizations” in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Command	Permissions	Authorizations
chfn	2555 root.security	UserAdmin
chuser	4550 root.security	UserAdmin, UserAudit
diag	0550 root.system	Diagnostics
lsuser	4555 root.security	UserAudit, UserAdmin
mkuser	4550 root.security	UserAdmin, UserAudit
rmuser	4550 root.security	UserAdmin
chgroup	4550 root.security	GroupAdmin
lsgroup	0555 root.security	
mkgroup	4550 root.security	GroupAdmin
rmgroup	4550 root.security	GroupAdmin
chgrpmem	2555 root.security	GroupAdmin
pwdadm	4555 root.security	PasswdManage, PasswdAdmin
passwd	4555 root.security	
chsec	4550 root.security	UserAdmin, GroupAdmin, PasswdAdmin, UserAudit
lssec	0550 root.security	PasswdAdmin
chrole	4550 root.security	RoleAdmin
lsrole	0550 root.security	
mkrole	4550 root.security	RoleAdmin
rmrole	4550 root.security	RoleAdmin
backup	4555 root.system	Backup
restore	4555 root.system	Restore

Managing Backup and Restore Roles

Users in the Backup and Restore roles can view and modify any file on the system. This includes the password and other security-oriented files. Be sure that trustworthy users are placed in these roles.

The following recommendation might prove helpful as you set up your system to perform backup and restore.

Setting Up Backup and Restore

For some customer environments, it is required that the device used in backing up and restoring the entire system be protected from other users. The steps below help you make certain that you set up the system backup and restore correctly.

1. Create a group called backup using the **mkgroup** command.

2. Assign the ownership of the system backup and restore device to root user and group backup with mode 660 using the **chown** command to assign ownership and **chmod** command to change permission.
3. Assign users in the Backup and Restore and ManageBackupRestore role to group backup using the **chuser** command.

This configuration allows only the root user and members of group backup to access the system backup device.

Chapter 4. Users and Groups

This chapter contains procedures for managing users and groups. Also included in this chapter is information on setting up the environment for authenticating a user (see “Setting Up the Disk Quota System” on page 36). See Disk Quota System Overview section in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices* for an overview on this topic.

Perform the following tasks to manage users and groups. You must have root authority to perform many of these tasks.

Managing Users and Groups Tasks		
Task	*SMIT Fast Path*	*Command or File*
Add a User	**smit mkuser**	
Set Initial Login Shell for a User[1] Environment	**smit chuser**	**chsh** *UserName*
Set Login Attributes for a User	**smit login_user**	
Change/Show Login Attributes for a Port	**smit login_port**	
Assign or Change a User’s Password	**smit passwd**	**passwd**
Change User’s Password Attributes	**smit passwdattrs**	
Manage Authentication Methods for a New User	**smit mkuser**	**/etc/security/users**
Manage Authentication Methods for an Existing User	**smit chuser**	**/etc/security/users**
Establish Default Attributes for New Users		Use **chsec** command to edit **/usr/lib/security/mkuser.default**
Change User Attributes	**smit chuser**	
Lock a User’s Account	**smit chuser**	**chuser account_locked=true** *AccountName*
Unlock a User’s Account	**smit chuser**	**chuser account_locked=false** *AccountName*
List Attributes for All Users	**smit lsuser**	
List All Attributes for a Specific User	**smit chuser**	**lsuser** *UserName*
List Specific Attributes for a Specific User		**lsuser -a** *Attributes User*
List Specific Attributes for All Users		**lsuser -a** *Attributes* **ALL**
Remove a User[2]	**smit rmuser**	
Turn Off/On Access for Users[3]	**smit chuser**	**chuser login=no** (or **yes**) *UserName*
Add a Group	**smit mkgroup**	
Change Group Attributes	**smit chgroup**	
List Groups	**smit lsgroup**	
List Specific Attributes for All Groups		**lsgroup -a** *Attributes* **|** **pg**
List All Attributes for a Specific Group		**lsgroup system**
List Specific Attributes for a Specific Group		**lsgroup -a** *Attributes Group*
Remove a Group[4]	**smit rmgroup**	**lsgroup -a** *Attributes Group*

Notes:

1. The shell you specify must be defined in the `usw` stanza of the **/etc/security/login.cfg** file.
2. You must remove information in other subsystems before removing a user, because the **cron** and **at** utilities both allow users to request programs to be run at a future date. Use the **crontab** command to remove a user's **cron** jobs. You can examine a user's **at** jobs with the **atq** command, then remove the jobs with the **atrm** command.
3. In general, this procedure is not suggested for systems using NIS. This procedure does not work at all for NIS clients and it works on NIS master servers only for users logging into the master server.
4. This procedure removes a group and all of its attributes from your network, but it does not remove all of the users in the group from the system. Also, if the group you want to remove is the primary group for any user, you must reassign that user to another primary group before removing the user's original primary group.

Setting Up the Disk Quota System

Note: The information in this section is specific to the POWER-based platform.

Prerequisites

You must have root user authority.

Procedure

1. Determine which file systems require quotas. Normally, you need to establish quotas only on those file systems that house users' home directories or other user files. The disk quota system can be used only with the journaled file system.

   Note: Because many editors and system utilities create temporary files in the **/tmp** file system, it must be free of quotas.
2. Use the **chfs** command to include the **userquota** and **groupquota** quota configuration attributes in the **/etc/filesystems** file. The following sample **chfs** command enables user quotas on the **/home** file system:

   ```
   chfs -a "quota = userquota" /home
   ```

   To enable both user and group quotas on the **/home** file system, enter:

   ```
   chfs -a "quota = userquota,groupquota" /home
   ```

   The corresponding entry in the **/etc/filesystems** is displayed as follows:

   ```
   /home:
   dev        = /dev/hd1
   vfs        = jfs
   log        = /dev/hd8
   mount      = true
   check      = true
   quota      = userquota,groupquota
   options    = rw
   ```
3. Optionally, specify alternate disk quota file names. The file names **quota.user** and **quota.group** are the default names located at the root directories of the file systems enabled with quotas. You can specify alternate names or directories for these quota files with the **userquota** and **groupquota** attributes in the **/etc/filesystems** file.

   The following sample **chfs** command establishes user and group quotas for the **/home** file system, and names the quota files **myquota.user** and **myquota.group**:

   ```
   chfs -a "userquota = /home/myquota.user" -a "groupquota = /home
          /myquota.group" /home
   ```

The corresponding entry in **/etc/filesystems** is displayed as follows:

```
/home:
dev        = /dev/hd1
vfs        = jfs
log        = /dev/hd8
mount      = true
check      = true
quota      = userquota,groupquota
userquota  = /home/myquota.user
groupquota = /home/myquota.group
options    = rw
```

4. Mount the specified file systems, if not previously mounted.
5. Set the desired quota limits for each user or group. Use the **edquota** command to create each user or group's soft and hard limits for allowable disk space and maximum number of files.

   The following sample entry shows quota limits for user davec:

   ```
   Quotas for user davec:
   /home: blocks in use: 30, limits (soft = 100, hard = 150)
           inodes in use: 73, limits (soft = 200, hard = 250)
   ```

   This user has used 30KB of the maximum 100KB of disk space. Of the maximum 200 files, davec has created 73. This user has buffers of 50KB of disk space and 50 files that can be allocated to temporary storage.

   When establishing disk quotas for multiple users, use the **-p** flag with the **edquota** command to duplicate a user's quotas for another user.

   To duplicate the quotas established for user davec for user nanc, type:

   ```
   edquota -p davec nanc
   ```
6. Enable the quota system with the **quotaon** command. The **quotaon** command enables quotas for a specified file system, or for all file systems with quotas (as indicated in the **/etc/filesystems** file) when used with the **-a** flag.
7. Use the **quotacheck** command to check the consistency of the quota files against actual disk usage.

   Note: It is recommended that you do this each time you first enable quotas on a file system and after you reboot the system.

   To enable this check and to turn on quotas during system startup, add the following lines at the end of the **/etc/rc** file:

   ```
   echo " Enabling filesystem quotas "
   /usr/sbin/quotacheck -a
   /usr/sbin/quotaon -a
   ```

Chapter 5. Logical Volumes

This chapter provides the following procedures for managing logical volume storage:

- “Managing Logical Volume Storage”
- “Reducing the File System Size in the rootvg Volume Group” on page 41
- “Configuring a Disk” on page 43
- “Replacing a Disk When the Volume Group Consists of One Disk” on page 45
- “Making an Available Disk a Physical Volume” on page 45
- “Migrating the Contents of a Physical Volume” on page 45
- “Importing or Exporting a Volume Group” on page 47
- “Changing a Volume Group to Nonquorum Status” on page 49
- “Creating a File System Log on a Dedicated Disk for a User-Defined Volume Group” on page 50
- “Changing the Name of a Logical Volume” on page 51
- “Removing a Logical Volume” on page 52
- “Defining a Raw Logical Volume for an Application” on page 54
- “Recovering from Disk Drive Problems” on page 55
- “Synchronizing the Device Configuration Database” on page 59
- “Using Removable Disk Management” on page 59
- “Removing a Disk with Data Using the Hot Removability Feature” on page 60
- “Removing a Disk without Data Using the Hot Removability Feature” on page 60
- “Adding a Disk Using the Hot Removability Feature” on page 60
- “Recovering from Disk Failure Using the Hot Removability Feature” on page 61

Managing Logical Volume Storage

The following tables show many tasks that help manage logical volume storage. The tables group tasks by those that primarily affect logical and physical volumes and those that primarily affect file systems. More complicated tasks are described in subsequent sections of this chapter.

Perform the following tasks to manage users and groups. You must have root authority to perform many of these tasks.

Managing Logical Volumes and Storage Tasks		
Task	*SMIT Fast Path*	*Command or File*
Add a logical volume[Note1]	**smit mklv**	
Add a volume group	**smit mkvg**	
Activate a volume group	**smit varyonvg**	
Add and activate a new volume group	**smit mkvg**	
Add fixed disk without data to existing volume group	**smit extendvg**	
Add fixed disk without data to new volume group	**smit mkvg**	
Change name of volume group [Note2]	1. **smit varyoffvg** 2. **smit exportvg** 3. **smit importvg** 4. **smit mountfs**	1. **varyoffvg** *OldVGName* 2. **exportvg** *OldVGName* 3. **importvg** *NewVGName* 4. **mount all**

Managing Logical Volumes and Storage Tasks		
Check size of a logical volume	**smit lslv**	
Copy a logical volume to a new logical volume[Note3]	**smit cplv**	
Copy a logical volume to an existing logical volume of the same size[Attn1]	**smit cplv**	
Copy a logical volume to an existing logical volume of smaller size[Attn1],[Note3]	Do not use SMIT[Attn2]	1. Create logical volume. For example: **mklv -y hd*X* vg00 4** 2. Create new files system on new logical volume. For example: **crfs -v jfs -d hd*X* -m /doc -A yes** 3. Mount file system. For example: **mount /doc** 4. Create directory at new mount point. For example: **mkdir /doc/options** 5. Transfer files system from source to destination logical volume. For example: **cp -R /usr/adam/oldoptions/* /doc/options**
Copy a logical volume to an existing logical volume of larger size[Attn1]	**smit cplv**	
Deactivate a volume group	**smit varyoffvg**	
Implement mirroring and data allocation	**smit mklvcopy**	
Implement mirroring only	**smit mklvcopy**	
Implement data allocation only	**smit chlv1**	
Implement write-verify and scheduling	**smit chlv1**	
Increase the maximum size of a logical volume	**smit chlv1**	
Increase the size of a logical volume	**smit lsvc**	
List all logical volumes by volume group	**smit lslv2**	
List all physical volumes in system	**smit lspv2**	
List contents of a physical volume	**smit lspv**	
List all volume groups	**smit lsvg2**	
List contents of a volume group	**smit lsvg1**	
Power off a disk	**smit offdsk**	
Power on a removable disk	**smit ondsk**	
Remove a volume group	**smit reducevg2**	
Remove a disk with data from the operating system	**smit exportvgrds**	
Remove a disk without data from the operating system	**smit reducevgrds**	
Reorganize a volume group	**smit reorgvg**	

Managing Logical Volumes and Storage Tasks		
Set automatic activation for a volume group	**smit chvg**	
Set logical volume policies	**smit chlv1**	
Unconfigure and power off a disk	**smit rmvdsk1** or **smit rmvdsk** then **smit opendoor**	

Attention:

1. Using this procedure to copy to an existing logical volume will overwrite any data on that volume without requesting user confirmation.
2. Do not use the SMIT procedure or the **cplv** command to copy a larger logical volume to a smaller one. Doing so results in a corrupted file system because some of the data (including the superblock) is not copied to the smaller logical volume.

Notes:

1. After you create a logical volume, the state will be closed. This means that no LVM structure is using that logical volume. It will remain closed until a file system has been mounted over the logical volume or the logical volume is opened for raw I/O. See also “Defining a Raw Logical Volume for an Application” on page 54 .
2. You cannot change the name of, import, or export **rootvg**.
3. You must have enough direct access storage to duplicate a specific logical volume.

Perform the following tasks to manage logical volumes and file systems. You must have root authority to perform many of these tasks.

Managing Logical Volumes and File Systems Tasks		
Task	*SMIT Fast Path*	*Command or File*
Add a journaled file system (JFS) to a previously defined logical volume menu	Create logical volume, then **smit crjfslv**	
Check size of a file system	**smit fs**	
Increase size of a file system	**smit chjfs**	
Listing all file systems on a disk	**smit lsmntdsk**	
Unmount file systems on a disk	**smit unmntdsk**	

Reducing the File System Size in the rootvg Volume Group

This procedure explains how to manually reduce the size of file systems in the rootvg volume group by creating a backup of your current rootvg volume group, and then reinstalling the operating system. It allows you to define the sizes of the logical partitions that are to be created during the installation process.

This procedure also explains how user-defined volume groups might be imported into your newly installed operating system.

Note: It is recommended that you create a separate backup of all file systems that are *not* contained in the rootvg volume group before performing this procedure.

Prerequisites

- You must have root authority or be a member of the system group to perform this task.
- Be sure to read and understand:
  - Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.
  - File Systems Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Procedure

This example uses the /**usr** file system as an example for reducing a file system in the rootvg volume group. If you want to reduce all file systems to their minimum size, the simplest way is to set SHRINK to yes during BOS install. Setting SHRINK to yes overrides any changes you make in the **/image.data** file described in the following:

1. With the key in the Normal position, log in as root.
2. Remove any files in /**usr** that you do not want.

   Attention: Only delete files that you have created or that you know are not needed on your system. If in doubt, do not delete the file.
3. Make sure all file systems in the rootvg volume group are mounted. If not, they are not included in the reinstalled system.
4. Type the command:

   ```
   mkszfile
   ```

   This creates the file /**image.data**, which contains a list of the active file systems in the rootvg volume group that are included in the installation procedure.
5. Use an editor to edit the /**image.data** file. If you edit the **/image.data** file, you must issue the **mksysb** command from the command line. Otherwise, your edited file is overwritten.
6. Change the size of /**usr** to reflect what you want the size of the file system to be in terms of logical partitions. In the following example, the **image.data** file currently shows the file size of **/usr** to be 58 logical partitions:

   ```
   lv_data:
        VOLUME_GROUP= rootvg
           .
           .
           .
           LPs= 58
           .
           .
           .
           MOUNT_POINT= /usr
           .
           .
           .
           LV_MIN_LPs= 51
   ```

   You can either increase or decrease the number of logical partitions needed to contain the file system data. The default size of each additional logical partition is 4MB (defined in the PP_SIZE entry of the **image.data** file).

   Attention: If you enter a value that is less than the minimum size required to contain the current data (indicated in the LV_MIN_LPs entry), the reinstallation process fails. Use the **df -k** command to see the current blocks used in the file systems; then divide this number by 1024 to get the total MB of the file system.
7. Change the FS_NAME in the fs_data to match the value that was chosen for LPs.

```
fs_data:
        FS_NAME= /usr
        .
        .
        .
        FS_SIZE= 475136
        .
        .
        .
        FS_MIN_SIZE= 417792
```

The FS_SIZE value is calculated:

```
FS_SIZE = PP_SIZE ( in KB ) * 2 ( 512-blocks) * LPs
```

Given the values for LV_DATA in step 6, FS_SIZE comes out to be:

```
475136     =     4096     *     2     * 58
```

8. Unmount all file systems that are *not* in the rootvg volume group.
9. If you have any user-defined volume groups, type the following commands to vary off and export them:

   ```
   varyoffvg VGName
   ```

   ```
   exportvg VGName
   ```
10. With a tape in the tape drive, type the following command:

    ```
    mksysb /dev/rmt0
    ```

    This will do a complete system backup, which includes file system size information (in the **/image.data** file) for use in the installation procedure.
11. Follow the instructions in Installation from a System Backup in *AIX 5L Version 5.1 Installation Guide* using the tape you created. The Use Maps option must be set to **no**, and the Shrink the File Systems option must be set to no. The new system must be installed using the option Install With Current System Settings for the logical-volume-size changes to take effect.
12. When the operating system installation is complete, you will need to reboot the system in Normal mode. The reduction of the file system is now complete.
13. If you have any user-defined volume groups, you can import them by typing the following:

    ```
    importvg -y VGName PVName
    ```
14. You can mount all file systems using the command:

    ```
    mount all
    ```

    Note: You might get ″Device Busy″ messages about file systems that are already mounted. These messages can be ignored.

Configuring a Disk

Three methods can be used to configure a new disk. Once a disk is configured, it is available for use by the system. If the Logical Volume Manager (LVM) is to use this disk, it must also be made a physical volume.

Use “Method 0” on page 44 if you are able to shut down and power off the system before attaching the disk. Otherwise, use “Method 1” on page 44 or “Method 2” on page 44. Use Method 1 if you know only the location of the disk. Use Method 2 if you know more information about the disk, such as the subclass, type, parent name, and where it is connected.

Prerequisites

The new disk must be connected to the system and powered on. Connect the new drive according to the procedure found in the *POWERstation and POWERserver Operator Guide*.

> **Attention:** If possible, shut down and power off any system to which you are attaching a physical disk.

Procedure

Method 0

Use this method when it is possible to shut down and power off the system before attaching the disk. Upon boot-up, the **cfgmgr** command automatically configures the disk. After boot-up is complete, log in as root and run **lspv**, look for a new disk entry in the output. For example:

```
hdisk1  none                    none
```

or:

```
hdisk1  00005264d21adb2e        none
```

After you have determined the name of the newly configured disk, note whether the new disk is listed with a PVID (16-digit number). If the new disk does not have a PVID, then use the procedure “Making an Available Disk a Physical Volume” on page 45 to allow the disk to be used by the LVM. If the new disk did not appear in the **lspv** output, refer to *AIX Version 4.3 Installation Guide*.

Method 1

Used this method when it is not possible to shut down or power off the system before attaching the disk.

1. Run the **lspv** command to note the physical disks already configured on the system. For example:

   ```
   hdisk0       000005265ac63976    rootvg
   ```

2. To configure all newly detected devices on the system (including the new disk) using the configuration manager, type:

   ```
   cfgmgr
   ```

3. Run the **lspv** command again, and look for a new disk entry in the output:

   ```
   hdisk1    none               none
   ```

   or:

   ```
   hdisk1   00005264d21adb2e     none
   ```

   After you have determined the name of the newly configured disk, use the procedure “Making an Available Disk a Physical Volume” on page 45 to allow the disk to be utilized by the Logical Volume Manager. If the new disk is not displayed in the list, refer to *AIX Version 4.3 Installation Guide*.

Method 2

Used this method when it is not possible to shut down or power off the system before attaching the disk. This method requires more information about the new disk but is usually faster than Method 1. To use method 2, you must know the following information:

- How the disk is attached (subclass)
- The type of the disk (type)
- Which system attachment the disk is connected to (parent name)
- The logical address of the disk (where connected).

Once you have this information, continue through the following steps:

1. Configure the disk and ensure that it is available as a physical volume by typing:

   ```
   mkdev -c disk -s subclass -t type -p parentname \
   -w whereconnected -a pv=yes
   ```

The `pv=yes` attribute makes the disk a physical volume and writes a boot record with a unique physical volume identifier onto the disk (if it does not already have one).

The following is an example for adding a 670 MB disk with a SCSI ID of 6 and logical unit number of 0 to the scsi3 SCSI bus:

```
mkdev -c disk -s scsi -t 670mb -p scsi3 -w 6,0 -a pv=yes
```

Replacing a Disk When the Volume Group Consists of One Disk

If you can access a disk that is going bad as part of a volume group, see Add fixed disk without data to existing volume group, or Add fixed disk without data to new volume group , and “Migrating the Contents of a Physical Volume” for information about adding individual disks and moving data.

If the disk is bad and cannot be accessed, follow these steps:

1. Export the volume group.
2. Replace the drive.
3. Recreate the data from backup media that exists.

Making an Available Disk a Physical Volume

To be assigned to volume groups and used by the LVM, a disk must be configured as a physical volume.

Prerequisites

- The disk name must be known to the system and the disk must be available.

  To configure a disk drive, see “Configuring a Disk” on page 43.
- The disk must not be currently in use by the system or any programs.

Procedure

To change an available disk to a physical volume, enter:

```
chdev -l hdisk3 -a pv=yes
```

This causes the available disk (`hdisk3`) to be assigned a physical volume identifier (PVID) if it does not already have one.

> **Note:** This command has no effect if the disk is already a physical volume.

Migrating the Contents of a Physical Volume

This procedure describes how to move the physical partitions belonging to one or more specified logical volumes from one physical volume to one or more other physical volumes in a volume group.

You might want to use this procedure to move the data from a failing disk before it is removed for repair or replacement. This procedure can be used on physical volumes in the rootvg volume group or on physical volumes in a user-defined volume group.

> **Attention:** When the boot logical volume is migrated from a physical volume, the boot record on the source is cleared. Failure to clear this record might result in a system hang. When you execute the **bosboot** command, you must also execute **mkboot -c** (see step 4 of the following procedure.)

Prerequisites

Be sure you read and understand the following:

- The **migratepv** command
- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Procedure

1. Determine which disks are in the volume group. Make sure that the source and destination physical volumes are in the same volume group. If the source and destination physical volumes are in the same volume group, proceed to step 3. Type:

   ```
   lsvg -p VGname
   ```

   The output looks similar to the following:

   ```
   rootvg:
   PV_NAME    PV STATE   TOTAL PPs   FREE PPs   FREE DISTRIBUTION
   hdisk0     active     159         0          00..00..00..00..00
   ```
2. If you are planning to migrate to a new disk, such as when you have a failing disk, perform the following steps:
   a. Make sure the disk is available by typing the following:

      ```
      lsdev -Cc disk
      ```

      The output resembles the following:

      ```
      hdisk0  Available  00-08-00-30  670 MB  SCSI  Disk Drive
      hdisk1  Available  00-08-00-20  857 MB  SCSI  Disk Drive
      ```
   b. If the disk is listed and in the available state, make sure it does not belong to another volume group, type the following command:

      ```
      lspv
      ```

      In the following example, `hdisk1` can be used as a destination disk:

      ```
      hdisk0     0000078752249812   rootvg
      hdisk1     000000234ac56e9e   none
      ```
   c. If the disk is not listed or is not available, you need to check or install the disk.
   d. Add the new disk to the volume group by typing the following command:

      ```
      extendvg VGName hdiskNumber
      ```
3. Make sure that you have enough room on the target disk for the source that you want to move:
   a. Determine the number of physical partitions on the source disk by typing the following command (*SourceDiskNumber* is of the form ’hdiskNumber’):

      ```
      lspv SourceDiskNumber | grep "USED PPs"
      ```

      The output looks similar to the following:

      ```
      USED PPs:      159 (636 megabytes)
      ```

      In this example, you need 159 FREE PPs on the destination disk to successfully complete the migration.
   b. Determine the number of free physical partitions on the destination disk or disks typing the following command for each destination disk (*DestinationDiskNumber* will be of the form ’hdiskNumber’):

      ```
        lspv DestinationDiskNumber | grep "FREE PPs"
      ```

      Add the FREE PPs from all of the destination disks. If the sum is larger than the number of USED PPs from step 3, you have enough space for the migration.

4. Follow this step only if you are migrating data from a disk in the rootvg volume group. If you are migrating data from a disk in a user-defined volume group, proceed to step 5.

   Check to see if the boot logical volume (**hd5**) is on the source disk by typing:

   ```
   lspv -l SourceDiskNumber | grep hd5
   ```

   If you get no output, the boot logical volume is not located on the source disk. Continue to step 5.

   If you get output similar to the following:

   ```
   hd5          2   2   02..00..00..00..00   /blv
   ```

   then run the following command:

   ```
   migratepv -l hd5 SourceDiskNumber DestinationDiskNumber
   ```

   Next, you get a message warning you to perform the **bosboot** command on the destination disk. You must also perform a **mkboot -c** command to clear the boot record on the source. Type the following:

   ```
   bosboot -a -d /dev/DestinationDiskNumber
   ```

   then type:

   ```
   bootlist -m normal DestinationDiskNumber
   ```

   then type:

   ```
   mkboot -c -d /dev/SourceDiskNumber
   ```

5. Now you can migrate your data. Type the following SMIT fast path:

   ```
   smit migratepv
   ```

6. List the physical volumes (PF4), and select the source physical volume you examined previously.
7. Go to the **DESTINATION** physical volume field. If you accept the default, all the physical volumes in the volume group are available for the transfer. Otherwise, select one or more disks with adequate space for the partitions you are moving (from step 4).
8. If you wish, go to the Move only data belonging to this **LOGICAL VOLUME** field, and list and select a logical volume. You move only the physical partitions allocated to the logical volume specified that are located on the physical volume selected as the source physical volume.
9. Press Enter to move the physical partitions.
10. If you now want to remove the source disk from the volume group, such as when it is failing, type the following command:

    ```
    reducevg VGNname SourceDiskNumber
    ```

11. If you want to physically remove the source disk from the system, such as when it is failing, enter the following command:

    ```
    rmdev -l SourceDiskNumber -d
    ```

Importing or Exporting a Volume Group

The following procedure explains how to import and export a volume group. The import procedure is used to make the volume group known to a system after the group is exported and moved from another system. It is also used to ″reintroduce″ (make known to the system) a group that was previously used on the system but was exported. If the **importvg** command is not working correctly, refreshing the device configuration database might help. See “Synchronizing the Device Configuration Database” on page 59.

The export steps remove the definition of a volume group from a system before the group is moved to a different system.

The procedures together can be used to move a volume group from one system to another.

You can also use this procedure to add a physical volume which contains data to a volume grou. You can do this by putting the disk to be added in its own volume group.

Note: The rootvg volume group cannot be exported or imported.

Some of the reasons for organizing physical volumes into separate volume groups are:

- To separate user file systems from the operating system to facilitate system updates, reinstallations, and crash recoveries
- To facilitate the moving of portable disks from one system to another
- To allow removal of disks for security or maintenance reasons
- To switch physical volumes between multiple system units

  For more details, see Developing a Volume Group Strategy

Prerequisites

Be sure you read and understand the following before you import or export a volume group:

- The **importvg** and **exportvg** commands
- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Attention: The **importvg** command changes the name of an imported logical volume if there currently is a logical volume with the same name already on the system. An error message is printed to standard error if an imported logical volume is renamed. The **importvg** command also creates file mount points and entries in **/etc/filesystems** if possible (if there are no conflicts).

Import/Export Volume Group Tasks		
Task	*SMIT Fast Path*	*Command or File*
Import a volume group	**smit importvg**	
Export a volume group	1. Unmount files systems on logical volumes in the volume group: **smit unmntdsk** 2. Vary off the volume group: **smit varyoffvg** 3. Export the volume group: **smit exportvg**	

Attention: A volume group that has a paging space volume on it cannot be exported while the paging space is active. Before exporting a volume group with an active paging space, ensure that the paging space is not activated automatically at system initialization by typing the following command:

```
chps -a n paging_space name
```

Then, reboot the system so that the paging space is inactive.

Notes:

1. If you do not activate the volume group through **smit importvg**, you must run the **varyonvg** command to enable access to the file systems and logical volumes.
2. If you imported a volume group that contains file systems, or if you activated the volume group through **smit importvg**, run the **fsck** command before you mount the file systems.
3. If you are moving the volume group to another system, be sure to unconfigure the disks before moving them.
4. The **smit exportvg** process deletes references to file systems in **/etc/filesystems**, but it leaves the mount points on the system.

Changing a Volume Group to Nonquorum Status

The purpose of a nonquorum volume group is to have data continuously available even when there is no quorum. A *quorum* is a state in which 51% or more of the physical volumes in a group are accessible. You might want to change a volume group to nonquorum status in systems configured as follows:

- A two-disk volume group in which the logical volumes are mirrored.
- A three-disk volume group in which the logical volumes are mirrored either once or twice.

In either configuration, if a disk failure occurs, the volume group remains active as long as there is one logical volume copy intact on a disk.

Both user-defined and rootvg volume groups can operate in nonquorum status, but the methods used to configure them as nonquorum and for recovery after hardware failures are different for user-defined and rootvg volume groups.

> **Attention:** If a logical volume has its only copies residing on a disk that becomes unavailable, the information is not available to the user regardless of the quorum or nonquorum status of the volume group.

Prerequisites

- To make recovery of nonquorum groups possible, make sure to:
  - Mirror the JFS log logical volume if JFS file systems are in use on the system.
  - Place the copies on separate disks. If you are unsure of the configuration, type the following command to check the physical location (PV1, PV2, and PV3) of each logical partition. (To place the copies on separate disks, the PV1, PV2, and PV3 columns must contain different hdisk numbers.):

    ```
    lslv -m LVName
    ```
- Be sure you read and understand the following before attempting to mirror nonquorum volume groups:
  - Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
  - Developing a Volume Group Strategy in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Changing User-Defined Volume Groups to Nonquorum Status

To activate a nonquorum user-defined volume group, all of the volume group’s physical volumes must be accessible or the activation fails. Because nonquorum volume groups stay online until the last disk becomes inaccessible, it is necessary to have each disk accessible at activation time.

1. Run the following command to see whether the user-defined volume group is varied on.

   ```
   lsvg -o
   ```

   If the user-defined volume group is not displayed in the list, follow step 3. Otherwise, follow step 2.
2. To make a standard user-defined volume group a nonquorum volume group, type the following command;

   ```
   chvg -Qn VGName
   ```
3. If the volume group is not active (varied on), type the following command to activate it and make effective the change to nonquorum status:

   ```
   varyonvg VGName
   ```
4. If the volume group is already activated (varied on), type the following commands to make the change to nonquorum status effective:

   ```
   varyoffvg VGname
   ```

   then type:

```
chvg -Qn VGName
```

then type:

```
varyonvg VGName
```

Changing the rootvg Volume Group to Nonquorum Status

> **Note:** Do not power on the system when a disk associated with the rootvg volume group is missing unless the missing disk cannot possibly be repaired. The Logical Volume Manager (LVM) always uses the **-f** flag to forcibly activate (vary on) a nonquorum rootvg; this operation involves risk. The reason for the forced activation is that the system cannot be brought up unless rootvg is activated. In other words, LVM makes a last ditch attempt to activate (vary on) a nonquorum rootvg even if only a single disk is accessible.

1. To make rootvg a nonquorum volume group, type the following command:

   ```
   chvg -Qn rootvg
   ```

2. Shut down and reboot the system to make effective the change to nonquorum status, type:

   ```
   shutdown -Fr
   ```

Creating a File System Log on a Dedicated Disk for a User-Defined Volume Group

A *file system log* is a formatted list of file system transaction records. The log for this system is called the JFS log (journaled file system log) and is used in case the system goes down before the transactions have been completed. The JFS log ensures file system integrity but not necessarily data integrity. A dedicated disk is created on hd8 for rootvg when the system is installed. The JFS log size is 4 MB. You can also create a JFS log on a separate disk for other volume groups, as shown in the following procedure. You might want to do this to improve performance under certain conditions, for example, if you have an NFS server and you want the transactions for this server to be processed without competition from other processes.

Prerequisites

- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- Developing a Logical Volume Strategy in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Procedure

You can use Web-based System Manager (type `wsm`, then select `lvm`) instead of the following procedure. If you use the following procedure, a volume group (fsvg1) is created, with two physical volumes, one of which is the dedicated device for the file system log. The log is on hdisk1 and the file system is on hdisk2 (a 256 MB file system mounted at **/u/myfs**).

> **Note:** You can place little-used programs, for example, **/blv**, on this physical volume without impacting performance. It is not required that it be empty except for the JFS log.

1. Add a new volume group (in this example, fsvg1 is the new volume group name). Type the SMIT fast path:

   ```
   smit mkvg
   ```

2. Select the volume group name you created using. Type the SMIT fast path:

   ```
   smit mklv
   ```

3. On the Add a Logical Volume dialog screen, set the following fields with your data. For example:

```
Logical Volumes NAME
fsvg1log

Number of LOGICAL PARTITIONS            1

PHYSICAL VOLUME names                   hdisk1

Logical volume TYPE                     jfslog

POSITION on Physical Volume             center
```

After you set the fields, press Enter.

4. Exit SMIT and type the following on a command line:

   ```
   /usr/sbin/logform /dev/fsvg1log
   ```

   Answer **y** to the following prompt:

   ```
   Destroy /dev/fsvg1log
   ```

   and press Enter.

   > **Note:** The preceding command formats the JFS-log logical volume so that it can record file-system transactions. Nothing is destroyed despite the wording in the prompt.

5. Type the following SMIT fast path:

   ```
   smit mklv
   ```

6. Type the name of the new volume group (`fsvg1` in this example). In the Logical Volumes dialog screen, fill in the following fields with your data. For example:

   ```
   Logical Volumes NAME
   fslv1

   Number of LOGICAL PARTITIONS            64

   PHYSICAL VOLUME names                   hdisk2

   Logical volume TYPE                     jfs
   ```

   Press Enter.

7. Exit SMIT and type the following on the command line:

   ```
   crfs -v jfs -d fslv1 -m /u/myfs -a
   logname=/dev/fsvg1log

   mount /u/myfs
   ```

8. To verify that you have set up the file system and log correctly, type the following command:

   ```
   lsvg -l fsvg1
   ```

   There are two logical volumes of the following types listed:

   ```
   /dev/fsvg1log   jfslog
   ```

   then type:

   ```
   fslv1     jfs
   ```

Changing the Name of a Logical Volume

This procedure enables you to rename a logical volume without losing any data on the logical volume. The file system associated with the logical volume must be unmounted and then renamed.

Prerequisites

It is important to have an understanding of the following:

- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- File Systems Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Procedure

In this example, the logical volume is changed from lv00 to hd33.

1. Unmount the file system associated with the logical volume, type:

   ```
   unmount /test1
   ```

   Note: You cannot use the **umount** command on a device in use. A device is in use if any file is open for any reason or if a user's current directory is on that device.
2. Rename the logical volume, type:

   ```
   chlv -n hd33 lv00
   ```
3. Change the **dev** parameter of the mount point of the file systems associated with the logical volume in the **/etc/filesystems** file to match the new name of the logical volume. For example: `/dev/lv00` becomes `/dev/hd33`

   Note: If you rename a JFS log, you are prompted to run **chfs** on all file systems that use the renamed log device.
4. Remount the file systems, type:

   ```
   mount /test1
   ```

Removing a Logical Volume

To remove a logical volume, you can use Web-based System Manager or you can use one of the following procedures. Use Web-based System Manager (type `wsm`, then select `LVM`) instead of **smit rmlv** or type `wsm`, then select `File systems` instead of **smit rmfs**. The primary difference between the following procedures is that the **smit rmfs** procedure removes the file system, its associated logical volume, and the record of the file system in the **/etc/filesystems** file. The **smit rmlv** procedure removes the logical volume but does not remove the file system record.

If you use one of the following procedures instead of Web-based System Manager, use **smit rmfs** to remove a logical volume with a JFS file system mounted on it. Use **smit rmlv** if you want to remove a logical volume with a non-JFS file system mounted on it or a logical volume that does not contain a file system.

Prerequisites

It is important to have an understanding of the following:

- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- Developing a Logical Volume Strategy in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- File Systems Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Remove a Logical Volume Using smit rmfs

Using this procedure removes a JFS file system, any logical volume on which it resides, the associated stanza in the **/etc/filesystems** file, and, optionally, the mount point (directory) where the file system is mounted.

Attention: Using this procedure destroys all data in the specified file systems and logical volume.

1. Unmount the file system that resides on the logical volume with a command similar to the following example:

   ```
   umount /adam/usr/local
   ```

   Note: You cannot use the **umount** command on a device in use. A device is in use if any file is open for any reason or if a user's current directory is on that device.
2. To select which file system to remove, type:

   ```
   smit rmfs
   ```
3. Go to the Remove Mount Point field and toggle to your preference. Selecting yes removes the mount point (directory) where the file system is mounted if the directory is empty.

Remove a Logical Volume Using smit rmlv

Using this procedure removes a non-JFS file system, provided such a system exists and is mounted, any logical volume on which it resides, the associated stanza in the **/etc/filesystems** file, and, optionally, the mount point (directory) where the file system is mounted. It also can be used to remove a logical volume that does not contain a file system. If the logical volume does not have a file system, go to step 3.

Attention: This procedure destroys all data in the specified logical volume.

1. Unmount the file system that resides on the logical volume. For example:

   ```
   umount /adam/usr/local
   ```

   Note: You cannot use the **umount** command on a device in use. A device is in use if any file is open for any reason or if a user's current directory is on that device.
2. Type the following fast path to list relevant information about your file systems:

   ```
   smit lsfs
   ```

   A partial listing follows:

   ```
   Name           Node     Mount Point

   /dev/testlv     xxx      /test

   /dev/locallv   xxx       /adam/usr/local
   ```

   Assuming standard naming conventions for the second item, the file system is named `/adam/usr/local` and the logical volume is `locallv`. To verify this, type the following fast path:

   ```
   smit lslv2
   ```
3. To select which logical volume to remove, type:

   ```
   smit rmlv
   ```
4. If the logical volume had a non-JFS file system mounted on it, remove the file system from the **/etc/filesystems** file as follows:

   ```
   rmfs /adam/usr/local
   ```

   Or, you can use the device name as follows:

   ```
   rmfs /dev/locallv
   ```

Defining a Raw Logical Volume for an Application

This procedure is used to define an area of physical and logical disk space that is under the direct control of an application rather than under control of the operating system and file system. The applications use character (raw) input and output rather than the block input and output of file systems, which require more software overhead. Bypassing the file system overhead enables applications to perform better. Raw logical volumes are most commonly used with database applications because of their need for high performance. While there is ordinarily a significant increase in performance, the actual amount of the increase depends on the database size and the driver provided by the application.

To prepare a raw logical volume, you simply create an ordinary logical volume without creating a file system on it.

> **Note:** Do not be too concerned with the name of the application or how its documents use raw storage. The term used could be any one of the following: partition, slice, file system, raw access, raw disk, or logical volume. The important naming concerns are dealt with as follows:
>
> - Use the correct command to define and name the device for the operating system. For a logical volume, use the **mklv** command to create **/dev**/*rLVName* and **/dev**/*LVName* (for example, `/dev/rhdX` and `/dev/hdX`).
> - Provide the application with the character or block special device file as appropriate. The application will link to this device when performing opens, reads, writes, and so on.
>
> **Attention:** Each logical volume has a logical-volume control block (LVCB) located in the first 512 bytes. Data begins in the second 512-byte block. Take care when reading and writing directly to the logical volume, as is done with raw logical volumes, because the LVCB is not protected from raw-logical-volume access. If the LVCB is overwritten, commands that try to update the LVCB will fail and give a warning message. Although the logical volume will continue to operate correctly and the overwrite of the LVCB is an allowable event, it is not recommended that the LVCB be destroyed by raw-logical-volume I/O.

Prerequisites

Be sure to read the following before attempting to create a raw logical volume:

- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- File Systems Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Procedure

To find the free physical partitions (PPs) where you can create the raw logical volume, use Web-based System Manager (type `wsm`, then select `lvm`) or the SMIT fast path as follows:

1. Type:

   ```
   smit lspv
   ```

   Press Enter.
2. Type the volume group name, for example:

   ```
   rootvg
   ```

   Press Enter.
3. Move the cursor to the disk that is most likely to have free physical partitions (possibly a disk with a higher number such as hdisk2 or hdisk3). Press Enter.
4. Check the FREE PPs field and multiply this number by the PP SIZE field to get the total number of megabytes available on that disk for a raw logical volume.

5. Make sure the number of free partitions is adequate based on your site's needs and the application's requirements. If the free space is not adequate, return to the previous menu and enter the name of a different disk or add a new physical volume if the free space is still not adequate. Exit SMIT.
6. Create the raw logical volume typing the following on the command line:

   ```
   mklv -y LVname VGName 38
   ```

In this example, `-y` indicates that you are going to name the logical volume instead of using a system name. The number `38` represents the number of 4 MB physical partitions. The raw volume capacity in this example is thus 152 MB. The raw logical volume you have created is now ready for your application to use.

For the next step, consult your application's instructions on how to use the raw space created. The instructions include how to open **/dev**/*LVName* and how to use it.

Recovering from Disk Drive Problems

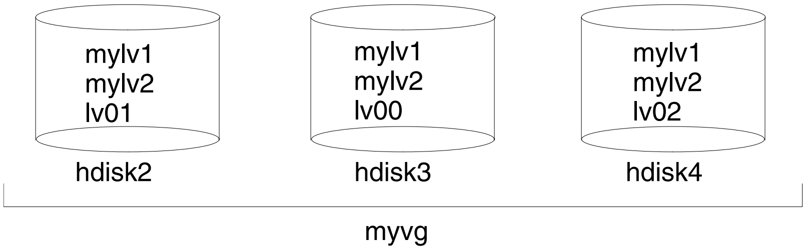
This procedure describes how to recover or restore data in logical volumes if a disk drive is failing. Before proceeding with this procedure, you should try the procedure "Migrating the Contents of a Physical Volume" on page 45. That procedure is the preferred way to recover data from a failing disk.

- If your drive is failing and you can repair the drive without reformatting it, no data will be lost. See "Recovering a Disk Drive without Reformatting".
- If the disk drive must be reformatted or replaced, make a backup, if possible, and remove the disk drive from its volume group and system configuration before replacing it. Some data from single-copy file systems might be lost. See "Recovering Using a Reformatted or Replacement Disk Drive" on page 56 .

Prerequisites

- Run diagnostics on the failed disk drive. For instructions, see How to Run Hardware Service Aids in your system unit operator guide.
- The following scenario is used in the next three procedures. The volume group called myvg contains three disk drives. The disks in this scenario are called hdisk2, hdisk3, and hdisk4. Assume the hdisk3 disk drive goes bad.

  The hdisk2 disk drive contains the nonmirrored logical volume lv01 and a copy of the logical volume mylv. The mylv logical volume is mirrored and has three copies, each of which takes up two physical partitions on its disk. The hdisk3 disk drive contains another copy of mylv and the nonmirrored logical volume lv00. Finally, hdisk4 contains a third copy of mylv as well as lv02. The following figure shows this scenario.



Recovering a Disk Drive without Reformatting

If you fix the bad disk and place it back in the system without reformatting it, then you can simply let the system automatically activate and resynchronize the stale physical partitions on the drive at boot time. A stale physical partition is a physical partition that contains data you cannot use. To discover if a physical partition is stale, use the **lspv -M** command to display information about a physical volume. Stale physical partitions will be marked stale.

Recovering Using a Reformatted or Replacement Disk Drive

If you must reformat or replace the failing drive, remove all references to nonmirrored file systems from the failing disk and remove it from the volume group and system configuration before replacing it. If you do not do this, you create problems in the ODM and system configuration databases.

Before Removing the Failed Drive

1. You should be familiar with which logical volumes are on the failing drive. To look at the contents of the failing drive, use one of the other drives. For example, use hdisk4 to look at hdisk3:

   ```
   lspv -M -n hdisk4 hdisk3
   ```

   The **lspv** command displays information about a physical volume within a volume group. The output might look something like the following:

   ```
   hdisk3:1        mylv:1
   hdisk3:2        mylv:2
   hdisk3:3        lv00:1
   hdisk3:4-50
   ```

   The first column displays the physical partitions and the second column displays the logical partitions. Partitions 4 through 50 are free.
2. Back up all single-copy logical volumes on the failing device, if possible.
3. If you have single-copy file systems, unmount them from the disk. Mirrored file systems do not have to be unmounted. Single-copy file systems are those that have the same number of logical partitions as physical partitions on the output from the **lspv** command. In the example scenario, `lv00` on the failing disk `hdisk3` is a single-copy file system. Type the command:

   ```
   unmount /Directory
   ```
4. Remove all single-copy file systems from the failed physical volume by typing the **rmfs** command:

   ```
   rmfs /Directory
   ```
5. Remove all mirrored logical volumes located on the failing disk by reducing the number of copies of the physical partitions to only those that are currently available. The **rmlvcopy** command removes copies from each logical partition. For example, type:

   ```
   rmlvcopy mylv 2 hdisk3
   ```

   By removing the copy on hdisk3, you reduce the number of copies of each logical partition belonging to the mylv logical volume from three to two (one on hdisk4 and one on hdisk2),

   > **Note:** Do not use **rmlvcopy** on the hd5 and hd7 logical volumes from physical volumes in the rootvg volume group. The system does not allow you to remove these logical volumes because there is only one copy of these.
6. Remove the primary dump device (logical volume hd7) if the failing physical volume was a part of the rootvg volume group that contained it. For example, type:

   ```
   sysdumpdev -P -p /dev/sysdumpnull
   ```

   The **sysdumpdev** command changes the primary or secondary dump device location for a running system. When you reboot, the dump device returns to its original location.
7. Remove any paging spaces located on the disk using the **rmps** command. If you cannot remove paging spaces because they are currently in use, you must flag the paging space as not active and reboot before continuing with this procedure. If there are active paging spaces, the **reducevg** command might fail.

8. Remove any other logical volumes, such as those with only one copy, using the **rmlv** command. For example, type:

   ```
   rmlv -f lv00
   ```

   The **rmlv** command removes a logical volume from a volume group.
9. Reduce the size of the volume group by omitting the failed drive using the **reducevg** command. For example, type:

   ```
   reducevg -df myvg hdisk3
   ```

   This example reduces the size of the myvg volume group by omitting the hdisk3 drive.

   You can now power off the old drive using the SMIT fast path **smit rmvdsk**. Change the KEEP definition in database field to No. Power off the system and allow your next level of support to add the new or reformatted disk drive.
10. Shut down the system, by typing:

    ```
    shutdown -F
    ```

    The **shutdown** command halts the operating system.

After Reformatting a Drive

Because the disk has been reformatted, the volume group defined in the disk is gone. If you have forgotten to or were unable to use the **reducevg** command on the disk from the old volume group before the disk was formatted, the following procedure can help clean up the VGDA/ODM information.

1. If the volume group consisted of only one disk that was reformatted, type:

   ```
   exportvg VGName
   ```
2. If the volume group consists of more than one disk, first run the command:

   ```
   varyonvg VGName
   ```
3. You receive a message about a missing or unavailable disk, and the disk you have now reformatted is listed. Note the PVID of that disk, which is listed in the **varyonvg** message. It is the 16-character string between the name of the missing disk and the label PVNOTFND.

   ```
   hdiskX PVID PVNOTFND
   ```
4. Type:

   ```
   varyonvg -f VGName
   ```

   The missing disk is now displayed with the PVREMOVED label.

   ```
   hdiskX PVID PVREMOVED
   ```
5. Then, type the command:

   ```
   reducevg -df VGName PVID
   ```

   Attention: The logical volumes defined on this missing disk is deleted from the ODM and VGDA areas of the remaining disks that make up the volume group *VGN*ame.

After Adding a Reformatted or Replacement Disk Drive

If you would prefer not to reboot the system after reformatting the disk drive, you must configure the disk and create the device entry, by typing:

```
cfgmgr
mkdev -1 hdisk3
```

If you want to reboot the system, this automatically configures the new drive. After rebooting, use the following procedure:

1. List all the disks using the **lsdev** command. Then find the name of the disk you just attached. For example, type:

   ```
   lsdev -C -c disk
   ```

In this example, the disk that was just attached is called by the same name as before (hdisk3).

2. Make the disk available using the **chdev** command by typing:

   ```
   chdev -l hdisk3 -a pv=yes
   ```

3. Add the new disk drive to the volume group using the **extendvg** command. For example, type:

   ```
   extendvg myvg hdisk3
   ```

   The **extendvg** command increases the size of the volume group by adding one or more physical volumes. This example adds the hdisk3 drive to the myvg volume group.

4. Recreate the single-copy logical volumes on the disk drive you just attached using the **mklv** command. For example, type:

   ```
   mklv -y lv00 myvg 1 hdisk3
   ```

   This example recreates the lv00 logical volume on the hdisk3 drive. The `1` means that this logical volume is not mirrored.

5. Recreate the file systems on the logical volume using the **crfs** command, by typing:

   ```
   crfs -v jfs -d LVname -m /Directory
   ```

6. Restore single-copy file system data from backup media. See "Restoring from Backup Image Individual User Files" on page 83.

7. Recreate the mirrored copies of logical volumes using the **mklvcopy** command. For example:

   ```
   mklvcopy mylv 3 hdisk3
   ```

   The **mklvcopy** command creates copies of data within a logical volume. This example creates a mirrored third partition (the mylv logical volume) onto hdisk3.

8. Synchronize the new mirror with the data on the current mirrors (on hdisk2 and hdisk4):

   ```
   syncvg -p hdisk3
   ```

   The **syncvg** command synchronizes logical volume copies that are not current.

After performing this procedure, all mirrored file systems should be restored and up-to-date. If you were able to back up your single-copy file systems, they will also be ready to use. You should be able to proceed with normal system use.

Example of Recovery from a Failed Disk Drive

To recover from a failed disk drive, back out the way you came in; that is, list the steps you went through to create the volume group, and then go backwards. The following example is an illustration of this technique. It shows how a mirrored logical volume was created and then how it was altered, backing out one step at a time, when a disk failed.

> **Note:** The following example of a specific instance and is given for illustration only. It is not intended as a general prototype on which to base any general recovery procedures.

1. Create a volume group called workvg on hdisk1, by typing:

   ```
   mkvg -y workvg hdisk1
   ```

2. Create two more disks for this volume group, by typing:

   ```
   extendvg workvg hdisk2

   extendvg workvg hdisk3
   ```

3. Create a logical volume of 40 MB that has three copies. Each copy is on one of each of the three disks that comprise workvg. Type:

   ```
   mklv -y testlv workvg 10

   mklvcopy testlv 3
   ```

Assume that hdisk2 fails.

4. Reduce the number of mirrored copies for the logical volume from three to two, and inform the LVM that you are not counting on the copy on hdisk2 anymore. Type:

   ```
   rmlvcopy testlv 2 hdisk2
   ```

5. Detach hdisk2 from the system in such a way that the ODM and VGDA are updated. Type:

   ```
   reducevg workvg hdisk2
   ```

6. Communicate to the ODM and the disk driver that you are taking hdisk2 offline for replacement. Type:

   ```
   rmdev -l hdisk2 -d
   ```

7. Shut down the system. Type:

   ```
   shutdown -F
   ```

8. Put in a new disk. It might not have the same SCSI ID as the former hdisk2.
9. Reboot the machine.

   Because you have a new disk (the system sees that there is a new PVID on this disk), the system chooses the first OPEN hdisk name. Because the **-d** flag was used in step 6, the name hdisk2 was released. Thus the configurator chooses hdisk2 for the name of the new disk. If the **-d** flag had not been used, hdisk4 would have been chosen as the new name.

10. Add this disk into the workvg system, by typing

    ```
    extendvg workvg hdisk2
    ```

11. Create two mirrored copies of the logical volume. The Logical Volume Manager automatically places the third logical volume copy on the new hdisk2. Type:

    ```
    mklvcopy testlv 3
    ```

Synchronizing the Device Configuration Database

The device configuration database might be inconsistent with the Logical Volume Manager (LVM) because of system malfunction. If it is, you receive a message from a logical volume command such as:

```
0516-322 The Device Configuration Database is inconsistent ...
```

```
0516-306 Unable to find logical volume mylv in the Device
Configuration Database.
```

(where `mylv` is normally available)

Use this procedure to synchronize the device configuration database with the LVM information.

Procedure

> **Attention:** Do not remove the **/dev** entries for volume groups or logical volumes. Do not change the database entries for volume groups or logical volumes using the Object Data Manager.

During normal operations, the device configuration database remains consistent with the Logical Volume Manager information. If for some reason it is not consistent, use the **varyonvg** command in preparation for resynchronizing the data for the specified volume group, by typing:

```
varyonvg VGName
```

Using Removable Disk Management

This section describes how to remove or add disks with the hot removability feature. *Hot removability* allows you to remove or add disks without turning the system off. This feature is only available on certain systems. For more information, refer to *7013 J Series Operator Guide* for details on the hot removability feature. For details on physical removal and insertion of disks, see *7013 J Series Service Guide*.

You can use the hot removability feature to:

- Remove a disk in a separate non-rootvg volume group for security or maintenance purposes. (See “Removing a Disk with Data Using the Hot Removability Feature”.)
- Permanently remove a disk from a volume group. (See “Removing a Disk without Data Using the Hot Removability Feature”.)
- Add a disk. (See “Adding a Disk Using the Hot Removability Feature”.)
- Correct a disk failure. (See “Recovering from Disk Failure Using the Hot Removability Feature” on page 61.)

Removing a Disk with Data Using the Hot Removability Feature

The following procedure describes how to remove a disk that contains data, in order to move the disk to another system without turning the system off.

Prerequisites

The disk you are removing must be in a separate non-rootvg volume group. To verify that the disk is in a separate non-rootvg volume group, list configuration information for volume groups see “Managing Logical Volume Storage” on page 39.

Procedure

1. Unmount any file systems on the logical volumes on the disk using the procedure “Mounting or Unmounting a File System” on page 65.
2. Deactivate and export the volume group in which the disk resides; unconfigure the disk and turn it off using the procedure Remove a disk with data from the operating system.

   If the operation is successful, a message indicates the cabinet number and disk number of the disk to be removed.
3. If the disk is placed at the front side of the cabinet, the disk shutter automatically opens.
4. Ensure that the yellow LED is off for the disk you want to remove.
5. Physically remove the disk. For more information about the removal procedure, see the section on removal in *7013 J Series Service Guide*.

Removing a Disk without Data Using the Hot Removability Feature

The following procedure describes how to remove a disk that contains no data or data that you do not want to keep. This procedure erases all of the data on the disk.

1. Unmount any file systems on the logical volumes on the disk using the procedure “Mounting or Unmounting a File System” on page 65 .
2. Remove a disk from its volume group, unconfigure the disk, and turn it off using the procedure Remove a disk without data from the operating system of Managing Logical Volume Storage .

   If the operation is successful, a message indicates the cabinet number and disk number of the disk to be removed.
3. Perform steps 3 to 5 of the procedure “Removing a Disk with Data Using the Hot Removability Feature”.

Adding a Disk Using the Hot Removability Feature

The following procedure describes how to turn on and configure a disk using the hot removability feature.

1. Install the disk in a free slot of the cabinet. For detailed information about the installation procedure, see *7013 J Series Service Guide*.
2. Perform the procedure Power on a removable disk of Managing Logical Volume Storage.

3. If the disk has no data, add a physical volume to the volume group.

   If the disk contains data, go to the procedure “Importing or Exporting a Volume Group” on page 47.

Recovering from Disk Failure Using the Hot Removability Feature

The following procedure describes how to recover from disk failure using the hot removability feature.

Procedure

Use the procedure “Recovering from Disk Drive Problems” on page 55. The notes below provide extra information that applies to disks with the hot removability feature.

Notes:

1. To unmount file systems on a disk, use the procedure “Mounting or Unmounting a File System” on page 65.
2. To remove the disk from its volume group and from the operating system, use the procedure “Removing a Disk without Data Using the Hot Removability Feature” on page 60.
3. To replace the failed disk with a new one, you do not need to shut down the system. Follow steps 1 and 2 of the procedure “Adding a Disk Using the Hot Removability Feature” on page 60. Then follow the procedure “Configuring a Disk” on page 43 and finally continue with step 4 of procedure “After Adding a Reformatted or Replacement Disk Drive” on page 57.

Chapter 6. File Systems

This chapter provides procedures for working with directories, disk space, access control, mounted file systems and directories, and file system recovery. Topics included are:

- “Managing File Systems”
- “Verifying File Systems” on page 64
- “Mounting or Unmounting a File System” on page 65
- “Mounting or Unmounting a Group of File Systems” on page 65
- “Making an Online Backup of a Mounted File System” on page 66
- “Using File Systems on Read/Write Optical Media” on page 66
- “Fixing Disk Overflows” on page 68
- “Fixing a Damaged File System” on page 70
- “Recovering from File System, Disk Drive, or Controller Failure” on page 71
- “Reformatting a Disk Drive” on page 72
- “Getting More Space on a Disk Drive” on page 72

Managing File Systems

This section shows how to list, add, and change local and remote file systems that are mounted and how to show characteristics of individual file systems such as size and mount point.

Managing File Systems Tasks	
Web-based System Manager File Systems (application)	Type `wsm`, then select `File Systems`.
-OR-	
Task	*SMIT Fast Path*
Add a journaled file system (JFS) or an enhanced journaled file system (JFS2)	**smit crfs**
Add a journaled file system (JFS) to an existing logical volume	**smit crjfslv**
Add an enhanced journaled file system (JFS2) to an existing logical volume	**smit crjfs2lvstd**
Change the attributes of a journaled file system (JFS) or an enhanced journaled file system (JFS2)	**smit chfs**
List Mounted File Systems	**smit fs**
List of File Systems on a Removeable Disk	**smit lsmntdsk**
Remove a journaled file system (JFS) or an enhanced journaled file system (JFS2)	**smit rmfs**

Note: You should not change the names of system-critical file systems, which are **/** (root) on logical volume 4 (hd4), **/usr** on hd2, **/var** on hd9var, **/tmp** on hd3, and **/blv** on hd5. If you use the hdX convention, start at hd10.

Verifying File Systems

File system inconsistencies can stem from the following:

- Stopping the system with file systems mounted.
- Physical disk deterioration or damage. Use this procedure before mounting any file system.

Some reasons to verify file systems are:

- After a malfunction. For example, if a user cannot change directories to a directory that has that user's permissions (uid).
- Before backing up file systems to prevent errors and possible restoration problems.
- At installation or system boot to make sure that there are no operating system file errors.

Prerequisites

- An understanding of the **fsck** command.
- Unmount the file systems being checked, except for **/** (root) and **/usr**, otherwise the **fsck** command fails.
- Check the **/** and **/usr** file systems only from the maintenance shell, see "Check a File System").
- You must have write permission on files, or **fsck** does not repair them (even if you answer Yes to repair prompts).

Check a User File System

1. Use the **smit fsck** fast path to access the Verify a File System menu.
2. Either specify the name of an individual file system to check in the **NAME of file system** field, or proceed to the **TYPE of file system** field and select a general file system type to check, such as a journaled file system (JFS).
3. If you want a fast check, specify Yes in the **FAST check?** field. The fast-check option specifies that the **fsck** command checks only those file systems that are likely to have inconsistencies. The most likely candidates are the file systems that were mounted when the system stopped at some point in the past. This option dramatically reduces the number of files that need checking.
4. Specify in the **SCRATCH file** field the name of a temporary file on a file system not being checked.
5. Start the file system check.

Check a File System

The **fsck** command requires that target file systems be unmounted. In general, the **/** (root) and **/usr** file systems cannot be unmounted from a disk-booted system. If the **fsck** command is to be run on **/** or **/usr**, then the system must be shut down and rebooted from removable media. This procedure describes how to run **fsck** on the **/** and **/usr** file systems from the maintenance shell.

1. With the key mode switch in the Service position, boot from your installation media.
2. From the Installation menu, choose the **Maintenance** option.
3. From the Maintenance menu, choose the option to access a volume group.

   Note: Once you choose this option, you cannot return to the Installation menu or Maintenance menu without rebooting the system.
4. Choose the volume group you believe is the rootvg volume group. A list of logical volumes that belong to the volume group you selected is displayed.
5. If this list confirms that this is the rootvg volume group, choose **2** to access the volume group and to start a shell before mounting file systems. If not, choose **99** to display a list of volume groups and return to step 4.

6. Run the **fsck** command using the appropriate options and file system device names. The **fsck** command checks the file system consistency and interactively repairs the file system. The **/** (root) file system device is **/dev/hd4** and the **/usr** file system device is **/dev/hd2**. To check **/**, type the following:

   ```
   $ fsck -y /dev/hd4
   ```

   The **-y** flag is recommended for less experienced users (see the **fsck** command).

   You might also want to check the **/tmp** and **/var** file systems at this time. The device for **/tmp** is **/dev/hd3**, and the device for **/var** is **/dev/hd9var**.
7. When you have completed checking the file systems, turn the key to Normal and reboot the system.

Mounting or Unmounting a File System

This procedure describes how to mount and unmount remote and local file systems.

Mounting makes file systems, files, directories, devices, and special files available for use at a particular location in the file tree. It is the only way a file system is made accessible to users.

Prerequisites

Check the file systems before mounting by using the procedure “Verifying File Systems” on page 64 or running the **fsck** command.

Mounting or Unmounting a File System Tasks	
Web-based System Manager File System (application)	Type `wsm`, then select `File Systems`
-OR-	
Task	*SMIT Fast Path*
Mount a Journaled File System (JFS) or an enhaced journaled file system (JFS2)	**smit mountfs**
Unmount a File System on a Fixed Disk	**smit umountfs**
Unmount a File System on a Removeable Disk	**smit umntdsk**

Note: If an unmount fails, it might be because a user or process has an opened file in the file system being unmounted. The **fuser** command lets you know which user or process might be causing the failure.

Mounting or Unmounting a Group of File Systems

This procedure describes how to mount or unmount a group of file systems. A file system group is a collection of file systems which have the same value for the **type=** identifier in the **/etc/filesystems** file. The **type=** value can be used to group associated file systems for mounting and unmounting. For example, all of the file systems on a remote host could have the same **type=** value, allowing all of the file systems on a remote machine to be mounted with a single command.

Mounting or Unmounting a Group of File Systems Tasks		
Task	*SMIT Fast Path*	*Command or File*
Mount a Group of File Systems	**smit mountg**	**mount -t** *GroupName*
Unmount a Group of File Systems	**smit umountg**	**umount -t** *GroupName*

Making an Online Backup of a Mounted File System

Making an online backup of a mounted JFS file system creates a snapshot of the logical volume that contains the file system. This procedure describes how to split off a mirrored copy to be used to make a backup.

Prerequisites

In order to make an online backup of a mounted file system, the logical volume that the file system resides on must be mirrored. The JFS log logical volume for the file system must also be mirrored.

> **NOTE:** Because the file writes are asynchronous, the snapshot might not contain all data that was written immediately before the snapshot is taken. Modifications that start after the snapshot begins might not be present in the backup copy. Therefore, it is recommended that file system activity be minimal while the split is taking place.

Split Off a Mirrored Copy of the File System

- Use the **chfs** command with the **splitcopy** attribute to split off a mirrored copy of the file system.

  The user can control which copy is used as the backup by using the **copy** attribute. The second copy is the default if a copy is not specified by the user.

  The following example shows a copy of the file system **/testfs** split off. The example assumes that there are two copies of the file system.

  ```
  chfs -a splitcopy=/backup -a copy=2 /testfs
  ```

  Once this command completes successfully, a copy of the file system is available read-only in **/backup**.

  Note that additional changes made to the original file system after the copy is split off are not reflected in the backup copy.

Reintegrate a Mirrored Copy of the File System

- Once a backup has been made, the copy can be reintegrated as a mirrored copy using the **rmfs** command. For example, type:

  ```
  rmfs /backup
  ```

  The **rmfs** command removes the file system copy from its split off state and allows it to be reintegrated as a mirrored copy.

For additional information about mirrored logical volumes, see the Logical Volume Storage Overviewin *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*, or the **mklv** and **mklvcopy** commands.

Using File Systems on Read/Write Optical Media

Two types of file systems can be used on read/write optical media:

- CD-ROM file system (CDRFS)
- Journaled file system (JFS)

CD-ROM File Systems

A CD-ROM file system stored on read/write optical media is mounted the same way as a file system on a CD-ROM drive, provided that the optical media is write-protected. You must specify the following information when mounting the file system:

Device name	Defines the name of device containing the media.
Mount point	Specifies the directory where the file system will be mounted.
Automatic mount	Specifies whether the file system will be mounted automatically at system restart.

CD-ROM File Systems Tasks		
Task	*SMIT Fast Path*	*Command or File*
Adding a CD-ROM file system [1]	**smit crcdrfs**	1. Add the file system: **crfs -v cdrfs -p ro -d***DeviceName* **-m** *MountPoint* **-A** *AutomaticMount* 2. Mount the file system: **mount** *MountPoint*
Removing a CD-ROM file system[2]	1. Unmount the file system: **smit umountfs** 2. Remove the file system: **smit rmcdrfs**	1. Unmount the file system: **umount** *FileSystem* 2. Remove the file system: **rmfs** *MountPoint*

Notes:

1. Make sure the read/write optical media is write-protected.
2. A CD-ROM file system must be unmounted from the system before it can be removed.

Journaled File Systems

The journaled file system provides a read/write file system similar to those on a hard disk. You must have system authority to create or import a read/write file system on read/write optical media (that is, your login must belong to the system group) and you must have the following information:

Volume group name	Specifies the name of the volume group
Device name	Specifies the logical name of the read/write optical drive
Mount point	Specifies the directories where the file systems will be mounted
Size file system	Specifies the size of the file system in 512-byte blocks
Automatic mount	Specifies whether the file system will be mounted automatically at system restart

Notes:

1. Any volume group created on read/write optical media must be self contained on that media. Volume groups cannot go beyond one read/write optical disk.
2. When accessing a previously created journaled file system, the volume group name does not need to match the one used when the volume group was created.

Journaled File Systems Tasks		
Web-based System Manager File Systems (application)		Type `wsm`, then select `File Systems`
OR		
Task	*SMIT Fast Path*	*Command or File*

Journaled File Systems Tasks		
Add a journaled file system (JFS)	1. Insert optical disk into drive. 2. Create a volume group (if necessary): **smit mkvg** 3. Create a journaled file system: **smit crfs**	1. Insert optical disk into drive. 2. Create a volume group (if necessary): **mkvg -f -y** *VGName* **-d 1** *DeviceName* 3. Create a journaled file system: **crfs -v jfs -g** *VGName* **-a size=***SizeFileSystem* **-m** *MountPoint* **-A** *AutomaticMount* **-p rw** 4. Mount the file system: **mount** *MountPoint*
Accessing previously created journaled file systems (JFS)[1]	1. Insert optical disk into drive. 2. Import the volume group: **smit importvg**	1. Insert optical disk into drive. 2. Import the volume group: **importvg -y** *VGName* *DeviceName* 3. Mount the file system: **mount** *MountPoint*
Removing a journaled file system (JFS)[2]	1. Unmount the file system: **smit umountfs** 2. Remove the file system: **smit rmjfs**	1. Unmount the file system: **umount** *FileSystem* 2. Remove the file system: **rmfs** *MountPoint*

Notes:

1. This procedure is required whenever inserting media containing journaled file systems.
2. Removing a journaled file system destroys all data contained in that file system and on the read/write optical media.

Fixing Disk Overflows

A disk overflow occurs when too many files fill up the allotted space. This can be caused by a runaway process that creates many unnecessary files. You can use the following procedures to correct the problem:

- To identify the processes that may be causing the overflow, go to “Identifying Problem Processes”.
- To terminate the process, go to “Terminating the Process” on page 69.
- To reclaim file space without terminating the process, go to “Reclaiming File Space without Terminating the Process” on page 69.
- To fix an overflow in the **/usr** directory, go to “Fixing a /usr Overflow” on page 69.
- To fix an overflow in a user file system, go to “Fixing a User File System Overflow” on page 70.

Prerequisites

You must have root user authority to remove processes other than your own.

Identifying Problem Processes

1. To check the process status and identify processes that might be causing the problem, type:

   ```
   ps -ef | pg
   ```

   The **ps** command shows the process status. The **-e** flag writes information about all processes (except kernel processes), and the **-f** flag generates a full listing of processes including what the command name and parameters were when the process was created. The **pg** command limits output to a single page, so you are not confronted with reams of information scrolling quickly off the screen.

Check for system or user processes that are using excessive amounts of a system resource, such as CPU time. System processes such as **sendmail**, **routed**, and **lpd** seem to be the system processes most prone to becoming runaways.

2. To check for user processes that use more CPU than expected, type:

```
ps -u
```

Terminating the Process

1. To suspend or terminate the process causing the problem, type:

```
kill -9 1182
```

In this example, the **kill** command terminates the execution of the process numbered 1182.

2. Remove the files the process has been making, by typing:

```
rm file1 file2 file3
```

Reclaiming File Space without Terminating the Process

When an active file is removed from the file system, the blocks allocated to the file remain allocated until the last open reference is removed, either as a result of the process closing the file or because of the termination of the processes that have the file open. If a runaway process is writing to a file and the file is removed, the blocks allocated to the file are not freed until the process terminates.

To reclaim the blocks allocated to the active file without terminating the process, redirect the output of another command to the file. The data redirection truncates the file and reclaims the blocks of memory. For example:

```
$ ls -l
total 1248
-rwxrwxr-x      1 web   staff   1274770 Jul 20 11:19 datafile
$ date > datafile
$ ls -l
total 4
-rwxrwxr-x      1 web   staff        29 Jul 20 11:20 datafile
```

The output of the **date** command replaced the previous contents of the **datafile** file. The blocks reported for the truncated file reflect the size difference from 1248> to 4. If the runaway process continues to append information to this newly truncated file, the next **ls** command produces the following results:

```
$ ls -l
total 8
-rxrwxr-x       1 web   staff   1278866 Jul 20 11:21 datefile
```

The size of the **datafile** file reflects the append done by the runaway process, but the number of blocks allocated is small. The **datafile** file now has a hole in it. File holes are regions of the file that do not have disk blocks allocated to them.

Fixing a /usr Overflow

Use this procedure to fix an overflowing file system in the **/usr** directory.

1. Remove printer log files by typing:

```
rm -f /usr/adm/lp-log
rm -f /usr/adm/lw-log
```

2. Remove **uucp** log files by typing:

```
rm -f /usr/spool/uucp/LOGFILE
rm -f /usr/spool/uucp/SYSLOG
rm -f /usr/spool/uucp/ERRLOG
```

3. Remove unnecessary files in **/tmp** and **/usr/tmp**. It is a good practice to do this weekly. For example, type:

   ```
   find /tmp -type f -atime +7 -exec rm -f {} \;
   find /usr/tmp -type f -atime +7 -exec rm -f {} \;
   ```

4. Delete lines in **/var/adm/wtmp** if you do not need the files for accounting. Because **/var/adm/wtmp** contains records of date changes that include old and new dates, you can delete the old records. However, since **wtmp** is a binary file, you must first convert it to ASCII. To edit **/var/adm/wtmp**:

   a. Convert the **wtmp** file from a binary file to an ASCII file called **wtmp.new** by typing:

      ```
      /usr/sbin/acct/fwtmp < /var/adm/wtmp >
      wtmp.new
      ```

   b. Edit the **wtmp.new** file to shorten it by typing:

      ```
      vi wtmp.new
      ```

   c. Convert the **wtmp.new** file from ASCII back to the **wtmp** binary format by typing:

      ```
      /usr/sbin/acct/fwtmp -ic < wtmp.new >
      /var/adm/wtmp
      ```

Fixing a User File System Overflow

Use this procedure to fix an overflowing user file system.

1. Remove old backup files and core files. The following example removes all ***.bak**, **.*.bak**, **a.out**, **core**, *, or **ed.hup** files.

   ```
   find / \( -name "*.bak" -o -name core -o -name a.out
   -o \
           -name "...*" -o -name ".*.bak" -o -name ed.hup \) \
           -atime +1 -mtime +1 -type f -print | xargs -e rm -f
   ```

2. To prevent files from regularly overflowing the disk, run the **skulker** command as part of the **cron** process and remove files that are unnecessary or temporary.

   The **skulker** command purges files in **/tmp** directory, files older than a specified age, **a.out** files, core files, and **ed.hup** files. It is run daily as part of an accounting procedure run by the **cron** command during off-peak periods (assuming you have turned on accounting).

   The **cron** daemon runs shell commands at specified dates and times. Regularly scheduled commands such as **skulker** can be specified according to instructions contained in the **crontab** files. Submit **crontab** files with the **crontab** command. To edit a **crontab** file, you must have root user authority.

   For more information about how to create a **cron** process or edit the **crontab** file, refer to “Setting Up an Accounting System” on page 123.

Fixing a Damaged File System

To fix a damaged file system, you must diagnose the problem and then repair it. The **fsck** command performs the low-level diagnosing and repairing.

Prerequisites

- You must have root user authority to execute this task.
- The damaged file system must be unmounted. The **fsck** command can only check unmounted file systems.

Procedure

1. Assess file system damage by running the **fsck** command. In the following example, the **fsck** command checks the unmounted file system located on the **/dev/hd1** device:

   ```
   fsck /dev/hd1
   ```

The **fsck** command checks and interactively repairs inconsistent file systems. Normally, the file system is consistent, and the **fsck** command merely reports on the number of files, used blocks, and free blocks in the file system. If the file system is inconsistent, the **fsck** command displays information about the inconsistencies found and prompts you for permission to repair them. The **fsck** command is conservative in its repair efforts and tries to avoid actions that might result in the loss of valid data. In certain cases, however, the **fsck** command recommends the destruction of a damaged file. Refer to the **fsck** command for a list of inconsistences that **fsck** checks for.

2. If the file system cannot be repaired, restore it from backup.

   The following example restores an entire file system backup on the **/dev/hd1** device. It destroys and replaces any file system previously stored on the **/dev/hd1** device. If the backup was made using incremental file system backups, restore the backups in increasing backup-level order (for example, 0, 1, 2).

   ```
   mkfs /dev/hd1
   mount /dev/hd1 /filesys
   cd /filesys
   restore -r
   ```

   The **mkfs** command makes a new file system on the specified device. The command initializes the volume label, file system label, and startup block. For more information about restoring a file system from backup, refer to ″Restoring from Backup Image Individual User Files″ .

   When using **smit restore** to restore an entire file system, enter the target directory, restore device (other than **/dev/rfd0**), and number of blocks to read in a single input operation.

Recovering from File System, Disk Drive, or Controller Failure

File systems can get corrupted when the i-node or superblock information for the directory structure of the file system gets corrupted. This can be caused by a hardware-related ailment or by a program that gets corrupted that accesses the i-node or superblock information directly. (Programs written in assembler and C can bypass the operating system and write directly to the hardware.) One symptom of a corrupt file system is that the system cannot locate, read or write data located in the particular file system.

A disk drive can intermittently (or permanently) suffer read/write problems. If you hear a drive that makes loud squealing or scratching noises, it probably is about to fail. Usually, however, you will not notice that a drive has gone bad while it is still running. It is when you try to restart the system that the device refuses to work. (At this point, it is usually too late to retrieve the lost data.)

A controller failure can act much like a drive failure. However, when a drive fails, you cannot access that particular drive; when a controller fails, you cannot get access to all of the drives in the system (or many of them). A controller fails because some electrical component on the controller board fails.

> **Note:** Hardware problems are usually the most difficult to diagnose. No two hardware failures are exactly the same. This is usually the case because different components on the same kind of board can fail, causing a totally different set of symptoms and problems.

Prerequisites

You must have root user or system group authority to execute this task.

Procedure

1. Make sure that you have backups of the data.
2. Reboot the machine with diagnostic diskettes, and determine whether the problem is the file system, disk drive, or controller.

3. If the file system is the problem, use the **fsck** command or the **smit fsck** fast path to correct the problem. (For information about using the **fsck** command, refer to “Fixing a Damaged File System” on page 70.)
4. If the disk drive is the problem, determine whether you can still address the disk drive (if it is available). There are two ways to do this:
   - Use the **smit lsattrd** fast path.
   - Use the **lsdev** command and check for the problem disk drive in the output, for example:

     ```
     lsdev -C -d disk -S a
     ```
5. If you can still address the disk drive, reformat it, marking the bad sectors. For information about reformatting a disk drive, refer to “Reformatting a Disk Drive”.
6. If the controller card or other hardware is the problem, replace it with another card.

Reformatting a Disk Drive

Disk drives have moving parts. These parts include the rotating platters and the read/write heads that move back and forth over the platters. When a disk is first formatted, it starts placing the format down at the beginning of where the heads can write. (On most drives, this is usually the inner part of the disk drive toward the small hole in the platter.) When a disk drive is first formatted, it is new and the parts have not been used very much; hence they don’t have much wear on them. As the drive is used, the read/write mechanism tends to start drifting away from the original format because it no longer lines up to the same starting point.

If the read/write heads drift too far away from the original format of the drive, they are no longer able to read the information stored on the platters and need to be reformatted. You need to reformat a disk drive when it can no longer read information that is stored on it.

When a disk drive is formatted, all of the data that was stored on it is lost. Because all your data is lost, you might want to copy the data to another drive or to diskettes before reformatting the disk drive. For more information, refer to the **tar**, **cpio**, or **restore** commands.

Prerequisites

You must have root user authority to execute this task.

Procedure

1. Reboot your machine with diagnostic diskettes or CD-ROM disk.

2. Choose the **Service Aids** option from the Function Selection menu.

3. Choose the **Disk Media** option.

4. Choose the **Format Disk and Certify** option to format and certify your disk drive.

   Note: You can also use the **diag** or **smit diag** commands to reformat a disk drive.

Getting More Space on a Disk Drive

If you run out of space on a disk drive, there are several ways to remedy the problem. You can automatically track and remove unwanted files, restrict users from certain directories, or mount space from another disk drive.

Prerequisites

You must have root user, system group, or administrative group authority to execute these tasks.

Clean Up File Systems Automatically

Use the **skulker** command to clean up file systems by removing unwanted files by typing:

```
skulker -p
```

The **skulker** command is used to periodically purge obsolete or unneeded files from file systems. Candidate files include files in the **/tmp** directory, files older than a specified age, **a.out** files, core files, or **ed.hup** files.

Normally, the **skulker** command is run daily, often as part of an accounting procedure run by the **cron** command during off-peak hours. You must have root user authority to run this command. For more information about using the **skulker** command in a **cron** process, see "Fixing Disk Overflows" on page 68 .

For information on typical **cron** entries, see "Setting Up an Accounting System" on page 123 .

Restrict Users from Certain Directories

Another way to free up disk space and possibly to keep it free is to restrict and monitor disk usage.

- Restrict users from certain directories by typing:

  ```
  chmod 655 rootdir
  ```

  This sets read and write permissions for the owner (root) and sets read-only permissions for the group and others.
- Monitor the disk usage of individual users. For example, if you added the following line to the cron file **/var/spool/cron/crontabs/adm**, the **dodisk** command would run at 2 a.m. (`0 2`) each Thursday (`4`):

  ```
  0 2 * * 4 /usr/sbin/acct/dodisk
  ```

  The **dodisk** command initiates disk-usage accounting. This command is usually run as part of an accounting procedure run by the **cron** command during off-peak hours. See "Setting Up an Accounting System" on page 123 for more information on typical **cron** entries.

Mount Space from Another Disk Drive

Another way to get more space on a disk drive is to mount space from another drive. There are two ways to mount space from one disk drive to another:

- Use the **smit mountfs** fast path.
- Use the **mount** command. For example:

  ```
  mount -n nodeA -vnfs /usr/spool /usr/myspool
  ```

  The **mount** command makes a file system available for use at a specific location.

For more information about mounting file systems, see "Mounting or Unmounting a File System" on page 65 .

Chapter 7. Paging Space and Virtual Memory

This chapter includes the following procedures for allocating page space.

- “Adding and Activating a Paging Space”
- “Changing or Removing a Paging Space”
- “Resizing or Moving the hd6 Paging Space” on page 76

Adding and Activating a Paging Space

To make a paging space available to the operating system, you must add the paging space and then make it available.

> **Attention:** Do not add paging space to volume groups on portable disks because removing a disk with an active paging space causes the system to crash.

To improve paging performance, use multiple paging spaces and locate them on separate physical volumes whenever possible. However, more than one space can be located on the same physical volume. Although you can use multiple physical volumes, it is a good idea to select only those disks within rootvg volume group unless you are thoroughly familiar with the system.

The total amount of paging space is often determined by trial and error but one commonly used guideline is to double the RAM size and use that figure as a paging space target. If you get error messages like the following, increase the paging space:

```
INIT: Paging space is low!
```

Another possibility is that users might get a message similar to the following from an application, in which case you also increase the paging space:

```
You are close to running out of paging space.
You may want to save your documents because
this program (and possibly the operating system)
could terminate without future warning when the
paging space fills up.
```

Adding/Activating Paging Space Tasks	
Task	*SMIT Fast Path*
Add paging space	**smit mkps**
Activate paging space	**smit swapon**
List all paging spaces	**smit lsps**

Changing or Removing a Paging Space

This procedure describes how to change or remove an existing paging space.

> **Attention:** Removing default paging spaces incorrectly can prevent the system from restarting. This procedure is for experienced system managers only.

> **Note:** You must deactivate the paging space before you can remove it. A special procedure is required for removing the default paging spaces (hd6, hd61, and so on). These paging spaces are activated during boot time by shell scripts that configure the system. To remove one of the default paging spaces, these scripts must be altered and a new boot image must be created.

Changing/Removing Paging Space Tasks	
Task	*Procedure*
Changing the characteristics of a paging space	**smit chps**
Removing a paging space	1. Deactivate the paging space: **smit swapoff** 2. Remove the paging space: **smit rmps**

Note: If the paging space you are removing is the default dump device, you must change the default dump device to another paging space or logical volume before removing the paging space. To change the default dump device type the following command:

```
sysdumpdev -P -p /dev/new_dump_device
```

Resizing or Moving the hd6 Paging Space

This article discusses various ways to modify the hd6 paging space. The following procedures describe how to make the hd6 paging space smaller and how to move the hd6 paging space within the same volume group.

System managers and users sometimes want to *reduce* the default paging space in order to:

- Enhance storage system performance by forcing paging and swapping to other disks in the system that are less busy.
- Conserve disk space on hdisk0.

Moving hd6 to a different disk is another way to enhance storage system performance. Whether moving the paging space or reducing its size, the rationale is the same: move paging space activity to disks that are less busy. The installation default creates a paging logical volume (hd6) on drive hdisk0, that contains part or all of the busy **/** (root) and **/usr** file systems. If the minimum Inter Allocation policy is chosen, meaning that all of **/** and a large amount of **/usr** are on hdisk0, moving the paging space to a disk that is less busy significantly improves performance. Even if the maximum Inter Allocation policy is implemented and both **/** and **/usr** are distributed across multiple physical volumes, your hdisk2 (assuming three disks) likely contains fewer logical partitions belonging to the busiest file systems.

You can check your logical volume and file system distribution across physical volumes by typing the following command:

```
lspv -l hdiskX
```

Prerequisites

Be sure to read the following articles before attempting to move a paging space to a different disk:

- Paging Space Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- Managing Paging Spaces in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- Logical Volume Storage Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*

Making the hd6 Paging Space Smaller

The **chps** command provides a method for shrinking existing paging spaces, including the primary paging space and the primary and secondary dump device. Use this command by typing either `chps` *`PagingSpace`* or `smit chps`. The **chps** command involkes the **shrinkps** script. This script safely shrinks the paging space without leaving the system in an unbootable state.

> **Note:** The primary paging space is hardcoded in the boot record. Therefore, the primary paging space will always be activated when the system is restarted. **chps** is unable to deactivate the primary paging space.

The shrinkps script safely automates the process for reducing the size of a paging space. The shrinkps script:

1. Creates a temporary paging space in the same volume
2. Moves information to that temporary space
3. Creates a new, smaller paging space in the same volume, and
4. Removes the old paging space.

> **Note:** For this command to work, there must be enough free disk space (space not allocated to any logical volume) to create a temporary paging space. The size of the temporary paging space is equal to amount of space needed to hold all the paged out pages in the old paging space. The minimum size for a primary paging space is 32 MB. The minimum size for any other paging space is 16 MB.

Priority is given to maintaining an operational configuration. System checks can lead to immediate refusal to shrink the paging space. Errors occuring while the temporary paging space is being created, will exit the procedure and the system will revert to the original settings. Other problems are likely to provoke situations which will require intervention by the system administrator or possibly an immediate reboot. Some errors may prevent removal of the temporary paging space. This would normally require non-urgent attention from the administrator.

If an I/O error is detected on system backing pages or user backing pages by the **swapoff** command, an immediate shutdown is advised to avoid a possible system crash. At reboot the temporary paging space is active and an attempt can be made to stop and restart the applications which encountered the I/O errors. If the attempt is successful and the **swapoff** command is able to complete deactivation, the shrink procedure can be completed manually using the **mkps**, **swapoff** and **rmps** commands to create a paging space with the required size and to remove the temporary paging space.

> **Note:** Do not attempt to remove (using **rmps**) or reactivate (using **chps**) a deactivated paging space which was in the I/O ERROR state before the system restart. There is a risk that the disk space will be reused and may cause additional problems.

Moving the hd6 Paging Space within the Same Volume Group

Moving the default paging space from hdisk0 to a different disk within the same volume group is a fairly simple procedure because you do not have to shut down and reboot.

Type the following command to move the default (hd6) paging space from hdisk0 to hdisk2:

```
migratepv -l hd6 hdisk0 hdisk2
```

> **Note:** Moving a paging space with the name hd6 from rootvg to another volume group is not recommended because the name is hard-coded in several places, including the second phase of the boot process and the process that accesses the root volume group when booting from removable media. Only the paging spaces in rootvg are active during the second phase of the boot process, and having no paging space in rootvg could severely affect system boot performance. If you want the majority of paging space on other volume groups, it is better to make hd6 as small as possible (the same size as physical memory) and then create larger paging spaces on other volume groups (see “Adding and Activating a Paging Space” on page 75).

Chapter 8. Backup and Restore

This chapter contains the following procedures for backing up and restoring information:

- "Compressing Files"
- "Backing Up User Files or File Systems"
- "Backing Up Your System" on page 80
- "Restoring from Backup Image Individual User Files" on page 83

Compressing Files

Several methods exist for compressing a file system:

- Use the **-p** flag with the **backup** command.
- Use the **compress** or **pack** commands.

Files are compressed for the following reasons:

- Saving storage and archiving system resources:
  - Compress file systems before making backups to preserve tape space.
  - Compress log files created by shell scripts that run at night; it is easy to have the script compress the file before it exits.
  - Compress files that are not currently being accessed. For example, the files belonging to a user who is away for extended leave can be compressed and placed into a **tar** archive on disk or to a tape and later restored.
- Saving money and time by compressing files before sending them over a network.

Procedure

To compress the **foo** file and write the percentage compression to standard error, type:

```
compress -v foo
```

See the **compress** command for details about the return values but, in general, the problems encountered when compressing files can be summarized as follows:

- The command might run out of working space in the file system while compressing. Because the **compress** command creates the compressed files before it deletes any of the uncompressed files, it needs extra space-from 50% to 100% of the size of any given file.
- A file might fail to compress because it is already compressed. If the **compress** command cannot reduce the file size, it fails.

Backing Up User Files or File Systems

Two procedures can be used to back up files and file systems: the SMIT fast paths **smit backfile** or **smit backfilesys**, and the **backup** command.

For additional information about backing up user files or file systems, see "Backing Up User Files or File Systems" in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Prerequisites

- If you are backing up *inode* file systems that may be in use, unmount them first to prevent inconsistencies.

Attention: If you attempt to back up a mounted file system, a warning message is displayed. The **backup** command continues, but inconsistencies in the file system may occur. This warning does not apply to the root (**/**) file system.

- To prevent errors, make sure the backup device has been cleaned recently.

Backing Up User Files or File Systems Tasks		
Task	*SMIT Fast Path*	*Command or File*
Back Up User Files	**smit backfile**	1. Log in to your user account. 2. Backup: **find . -print | backup -ivf /dev/rmt0**
Back Up User File Systems	**smit backfilesys**	1. Unmount files systems that you plan to back up. For example: **umount all** or **umount /home /filesys1** 2. Verify the file systems. For example: **fsck /home /filesys1** 3. Back up by i-node. For example: **backup -5 -uf/dev/rmt0 /home/libr** 4. Restore the files using the following command:[1] **restore -t**

Note:

1. If this command generates an error message, you must repeat the entire backup.

Backing Up the System Image and User-Defined Volume Groups

Backing Up Your System

The following procedures describe how to make an installable image of your system. For more information about backing up the system, see "Backing Up the System Image and User-Defined Volume Groups" in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Prerequisites

Before backing up the rootvg volume group:

- All hardware must already be installed, including external devices, such as tape and CD-ROM drives.
- This backup procedure requires the **sysbr** fileset, which is in the BOS System Management Tools and Applications software package. Type the following command to determine whether the **sysbr** fileset is installed on your system:

  ```
  lslpp -l bos.sysmgt.sysbr
  ```

  If your system has the **sysbr** fileset installed, continue the backup procedures.

  If the **lslpp** command does not list the **sysbr** fileset, install it before continuing with the backup procedure. See Installing Optional Software and Service Updates in the *AIX 5L Version 5.1 Installation Guide* for instructions.

  ```
  installp -agqXd device bos.sysmgt.sysbr
  ```

  where `device` is the location of the software; for example,`/dev/rmt0` for a tape drive.

Before backing up a user-defined volume group:

- Before being saved, a volume group must be varied on and the file systems must be mounted.

Attention: Executing the **savevg** command results in the loss of all material previously stored on the selected output medium.

- Make sure the backup device has been cleaned recently to prevent errors.

Backing Up Your System Tasks		
Task	*SMIT Fast Path*	*Command or File*
Backing up the **rootvg** volume group	1. Log in as root. 2. Mount file systems for backup.[1] **smit mountfs** 3. Unmount any local directories that are mounted over another local directory. **smit umountfs** 4. Make at least 8.8MB of free disk space available in the **/tmp** directory.[2] 5. Back up. **smit mksysb** 6. Write-protect the backup media. 7. Record any backed-up root and user passwords.	1. Log in as root. 2. Mount file systems for backup.[1] See **mount** command. 3. Unmount any local directories that are mounted over another local directory. See **umount** command. 4. Make at least 8.8MB of free disk space available in the **/tmp** directory.[2] 5. Back up. See **mksysb** command. 6. Write-protect the backup media. 7. Record any backed-up root and user passwords.
Verify a Backup Tape[3]	**smit lsmksysb**	
Backing up a user-defined volume group[4]	**smit savevg**	1. Modify the file system size before backing up, if necessary.[5] **mkvgdata** *VGName* then edit **/tmp/vgdata/***VGName***/***VGName***.data** 2. Save the volume group. See the **savevg** command.

Notes:

1. The **mksysb** command does not back up file systems mounted across an NFS network.
2. The **mksysb** command requires this working space for the duration of the backup. Use the **df** command, which reports in units of 512-byte blocks, to determine the free space in the **/tmp** directory. Use the **chfs** command to change the size of the file system, if necessary.
3. This procedure lists the contents of a **mksysb** backup tape. The contents list verifies most of the information on the tape but does not verify that the tape can be booted for installations. The only way to verify that the boot image on a **mksysb** tape functions correctly is by booting from the tape.
4. If you want to exclude files in a user-defined volume group from the backup image, create a file named **/etc/exclude.***volume_group_name*, where *volume_group_name* is the name of the volume group that you want to back up. Then edit **/etc/exclude.***volume_group_name* and enter the patterns of file names that you do not want included in your backup image. The patterns in this file are input to the pattern matching conventions of the **grep** command to determine which files are excluded from the backup.
5. If you choose to modify the *VGName***.data** file to alter the size of a file system, you must not specify the **-i** flag or the **-m** flag with the **savevg** command, because the *VGName***.data** file is overwritten.

For more information about installing (or *restoring*) a backup image, see ″Installing BOS from a System Backup″ in the *AIX 5L Version 5.1 Installation Guide*.

Implementing Scheduled Backups

This procedure describes how to develop and use a script to perform a weekly full backup and daily incremental backups of user files. The script included in this procedure is intended only as a model and needs to be carefully tailored to the needs of the specific site.

Prerequisites

- The amount of data scheduled for backup cannot exceed one tape when using this script.
- Make sure the tape is loaded in the backup device before the **cron** command runs the script.
- Make sure the device is connected and available, especially when using scripts that run at night. Use the **lsdev -C | pg** command to check availability.
- Make sure the backup device has been cleaned recently to prevent errors.
- If you are backing up file systems that might be in use, unmount them first to prevent file system corruption.
- Check the file system before making the backup. Use the procedure "Verifying File Systems" on page 64 or run the **fsck** command.

Back Up File Systems Using the cron Command

This procedure describes how to write a **crontab** script that you can pass to the **cron** command for execution. The script backs up two user file systems, **/home/plan** and **/home/run**, on Monday through Saturday nights. Both file systems are backed up on one tape, and each morning a new tape is inserted for the next night. The Monday night backups are full archives (level 0). The backups on Tuesday through Saturday are incremental backups.

1. The first step in making the **crontab** script is to issue the **crontab-e** command. This opens an empty file where you can make the entries that are submitted to the **cron** script for execution each night (the default editor is **vi**). Type:

   ```
   crontab -e
   ```

2. The following example shows the six **crontab** fields. Field 1 is for the minute, field 2 is for the hour on a 24-hour clock, field 3 is for the day of the month, and field 4 is for the month of the year. Fields 3 and 4 contain an * (asterisk) to show that the script runs every month on the day specified in the `day/wk` field. Field 5 is for the day of the week, and field 6 is for the shell command being run.

   ```
   min hr day/mo mo/yr day/wk       shell command

   0   2    *     *      1          backup -0 -uf /dev/rmt0.1 /home/plan
   ```

   The command line shown assumes that personnel at the site are available to respond to prompts when appropriate. The `-0` (zero) flag for the `backup` command stands for level zero, or full backup. The `-u` flag updates the backup record in the **/etc/dumpdates** file and the `f` flag specifies the device name, a raw magnetic tape device 0.1 as in the example above. See rmt Special File in the *AIX 5L Version 5.1 Files Reference* for information on the meaning of extension .1 and other extensions (1-7).

3. Type a line similar to that in step 2 for each file system backed up on a specific day. The following example shows a full script that performs six days of backups on two file systems:

   ```
   0 2 * * 1 backup -0 -uf/dev/rmt0.1 /home/plan
   0 3 * * 1 backup -0 -uf/dev/rmt0.1 /home/run
   0 2 * * 2 backup -1 -uf/dev/rmt0.1 /home/plan
   0 3 * * 2 backup -1 -uf/dev/rmt0.1 /home/run
   0 2 * * 3 backup -2 -uf/dev/rmt0.1 /home/plan
   0 3 * * 3 backup -2 -uf/dev/rmt0.1 /home/run
   0 2 * * 4 backup -3 -uf/dev/rmt0.1 /home/plan
   0 3 * * 4 backup -3 -uf/dev/rmt0.1 /home/run
   0 2 * * 5 backup -4 -uf/dev/rmt0.1 /home/plan
   0 3 * * 5 backup -4 -uf/dev/rmt0.1 /home/run
   0 2 * * 6 backup -5 -uf/dev/rmt0.1 /home/plan
   0 3 * * 6 backup -5 -uf/dev/rmt0.1 /home/run
   ```

4. Save the file you created and exit the editor. The operating system passes the **crontab** file to the **cron** script.

Restoring from Backup Image Individual User Files

If you need to restore a backup image destroyed by accident, your most difficult problem is determining which of the backup tapes contains this file. The **restore -T** command can be used to list the contents of an archive. It is a good idea to restore the file in the **/tmp** directory so that you do not accidentally overwrite the user's other files.

If the backup strategy included incremental backups, then it is helpful to find out from the user when the file was most recently modified. This helps to determine which incremental backup contains the file. If this information cannot be obtained or is found to be incorrect, then start searching the incremental backups in reverse order (7, 6, 5, ...). For incremental file system backups, the **-i** flag (interactive mode) of the **restore** command is very useful in both locating and restoring the lost file. (Interactive mode is also useful for restoring an individual user's account from a backup of the **/home** file system.)

The procedures in the following table describe how to implement a level 0 (full) restoration of a directory or file system.

Prerequisites

Make sure the device is connected and available. To check availability, type:

```
lsdev -C | pg
```

Restoring from Backup Image Tasks		
Task	*SMIT Fast Path*	*Command or File*
Restore Individual User Files	**smit restfile**	See **restore** command.
Restoring a User File System	**smit restfilesys**	1. **mkfs /dev/hd1** 2. **mount /dev/hd1 /filesys** 3. **cd /filesys** 4. **restore -r**
Restoring a User Volume Group	**smit restvg**	See **restvg -q** command.

Chapter 9. System Environment

The system environment is primarily the set of variables that define or control certain aspects of process execution. They are set or reset each time a shell is started. From the system-management point of view, it is important to ensure the user is set up with the correct values at login. Most of these variables are set during system initialization. Their definitions are read from the **/etc/profile** file or set by default.

Topics covered in this chapter are:

Changing the System Date and Time

The system date and time is set with the **date** command.

Prerequisites

You must have root user authority to change the system date or time.

Procedure

The **date** command allows the date or time to specified in one of several different formats. One form of the **date** command is:

```
date mmddHHMM.SSyy
```

where `mm` is the month, `dd` is the day of the month, `HH` is the hour, `MM` is the minutes, `SS` is the seconds, and `yy` is the last two digits of the year.

Correcting an Inaccurate System Clock

The system clock records the time of system events, allows you to schedule system events (such as running hardware diagnostics at 3:00 a.m.), and tells when you first created or last saved files. To reset or reactivate an inaccurate clock, see:

- "Testing the System Battery"
- "Resetting the System Clock" on page 86

Testing the System Battery

If your system is losing track of time, the cause might be a depleted or disconnected battery. To determine the status of your system battery, type the following **diag** command:

```
diag -B -c
```

When the Diagnostics main menu appears, select the **Problem Determination** option. If the battery is disconnected or depleted, a problem menu will be displayed with a service request number (SRN). Record the SRN on Item 4 of the Problem Summary Form and report the problem to your hardware service organization.

If your system battery is operational, your system time might have been reset incorrectly because either the **date** or **setclock** command was run incorrectly or unsuccessfully. Refer to “Resetting the System Clock” to correct the problem.

Resetting the System Clock

Use the **date** command to set your system clock. Use the **setclock** command to set the time and date for a host on a network. Reset your system clock by either:

- “Using the date Command”
- “Using the setclock Command” on page 87

Using the date Command

The **date** command displays or sets the date and time. Enter the following command to determine your system’s date and time:

```
/usr/bin/date
```

> **Attention:** Do not change the date when the system is running with more than one user.

The following formats can be used when setting the date with the *Date* parameter:

- *mmddHHMM*[.*SSyy*] (default)
- *yymmddHHMM*[.*SS*]
- *ddmmHHMMyy*[.*SS*]

The variables to the *Date* parameter are defined as follows:

mm Specifies the month number.
dd Specifies the number of the day in the month.
HH Specifies the hour in the day (using a 24-hour clock).
MM Specifies the minute number.
SS Specifies the number of seconds.
yy Specifies the last two numbers of the year.

> **Note:** If the *yymmdd* format is specified, the value of the *yy* variable must be 88 to 99.

The **date** command writes the current date and time to standard output if called with no flags or with a flag list that begins with a **+** (plus sign). Otherwise, it sets the current date. Only a root user can change the date and time. The **date** command prints out the usage message on any unrecognized flags or input.

If you follow the **date** command with a + (plus sign) and a field descriptor, you can control the output of the command. You must precede each field descriptor with a **%** (percent sign). The system replaces the field descriptor with the specified value. Enter a literal % as %% (two percent signs). The **date** command copies any other characters to the output without change. The **date** command always ends the string with a new-line character.

Flags

-n Does not set the time globally on all machines in a local area network that have their clocks synchronized.
-u Displays or sets the time in Coordinated Universal Time (UTC).

Using the setclock Command

The **setclock** command sets the time and date for a host on a network. To determine your system's date and time, enter:

```
/usr/sbin/setclock
```

The **/usr/sbin/setclock** command gets the time from a network time server, and if run by a user with root user authority, sets the local time and date accordingly.

The **setclock** command takes the first response from the time server, converts the calendar clock reading found there, and shows the local date and time. If the **setclock** command is run by the root user, it calls the standard workstation entry points to set the system date and time.

If no time server responds, or if the network is not operational, the **setclock** command displays a message to that effect and leaves the date and time settings unchanged.

Note: Any host running the **inetd** daemon can act as a time server.

Parameter

TimeServer — The host name or address of a network host that services TIME requests. The **setclock** command sends a public network TIME service request to a time server host. If the *TimeServer* name is omitted, the **setclock** command sends the request to the default time server. The default time server in a DOMAIN environment is specified by the name server. Otherwise, the default time server is specified in the **/etc/hosts** file.

Changing the Message of the Day

The message of the day is displayed every time a user logs in to the system. It is a convenient way to communicate information to all users, such as installed software version numbers or current system news. The message of the day is contained in the **/etc/motd** file. To change the message of the day, simply edit that file.

Enabling Dynamic Processor Deallocation

You can turn the Dynamic Processor Deallocation **on** or **off** and, if the processor deallocation fails when enabled, you can restart it.

You can use SMIT or system commands. To perform these tasks, you must log in as **root**.

For additional information, see Enabling Dynamic Processor Deallocation in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

SMIT Fastpath Procedure

1. Type `smit system` at the system prompt, then press Enter.
2. In the **Systems Environment** window, select **Change / Show Characteristics of Operating System**.
3. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to work with the Dynamic Processor Deallocation:

- Use the **chdev** command to change the characteristics of the device specified. For information about using this command, see **chdev** in the *AIX 5L Version 5.1 Commands Reference, Volume 1*.
- If the processor deallocation fails for any reason, you can use the **ha_star** command to restart it after it has been fixed. For information about using this command, see **ha_star** in the *AIX 5L Version 5.1 Commands Reference, Volume 2*.
- Use the **errpt** command to generate a report of logged errors. For information about using this command, see **errpt** in the *AIX 5L Version 5.1 Commands Reference, Volume 2*.

Chapter 10. National Language Support

Many system variables are used to establish the language environment of the system. These variables and their supporting commands, files, and other tools, are referred to as National Language Support (NLS).

Topics covered in this chapter are:

Changing Your Locale

Changing the NLS Environment

You can customize your NLS environment. From the Users application of Web-based System Manager or from the Manage Language Environment screen in SMIT, you can:

- Choose the default language environment.
- Choose the keyboard map for the next system restart.
- Manage fonts.
- Convert the code set of message catalogs.
- Convert the code set of flat text files.

You can also use the **setmaps** command to set the code set map of a terminal.

For additional explanation, see National Language Support Overview in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Changing the Default Language Environment

To designate the default locale, which is a language-territory-code-set combination, set the **LANG** environment variable (the ″**LANG** = *name*″ string in the **/etc/environment** file). The default locale provides formats for default collation, character classification, case conversion, numeric and monetary formatting, date-and-time formatting, and affirmative or negative responses. The default locale includes reference to the code set.

Changing the NLS Environment with the localedef Command

If a special locale is desired (that is, a locale different from any of those provided), take the following steps with a user ID that allows read or write permissions (for example, root):

1. If you are using a locale source file named **gwm**, copy the provided locale source file that is closest to the desired locale to a file named **gwm.src**. This name cannot be the same as any previously defined locale. The system-defined locales are listed in Understanding Locale .

   ```
   cd /usr/lib/nls/loc
   cp en_GB.ISO8859-1.src gwm.src
   ```

2. Edit the newly created locale source file to change the locale variables to the desired values, by typing:

```
vi gwm.src
change d_fmt "%d%m%y" to d_fmt "%m-%d-%y"
```

3. Compile the locale definition source file, by typing:

   ```
   localedef -f ISO8859-1 -i gwm.src gwm
   ```

4. Set the **LOCPATH** environment variable to the directory containing the new locale file. The default for **LOCPATH** is **/usr/lib/nls/loc**. Type:

   ```
   LOCPATH=/usr/lib/nls/loc; export LOCPATH
   ```

   Note: All **setuid** and **setgid** programs ignore the **LOCPATH** environment variable.

5. Set the corresponding environment variable or variables, by typing:

   ```
   export LC_TIME=gwm
   ```

Creating a New Collation Order

Procedure

1. If you are using a locale source file named **gwm**, copy the provided locale source file that is closest to the desired character collation order to a file named **gwm.src**. This name cannot be the same as any previously defined locale. The system-defined locales are listed in Understanding Locale.

   ```
   cd /usr/lib/nls/loc

   cp en_GB.ISO8859-1.src gwm.src
   ```

2. Edit the newly created `gwm.src` file to change the lines that are associated within the **LC_COLLATE** category that is associated with the characters you want to change, by typing:

   ```
   vi gwm.src
      change
         <a>   <a>;<non-accent>;<lower-case>;IGNORE
         <b>   <b>;<non-accent>;<lower-case>;IGNORE
         <c>   <c>;<non-accent>;<lower-case>;IGNORE
         <d>   <d>;<non-accent>;<lower-case>;IGNORE
      to
         <a>   <d>;<non-accent>;<lower-case>;IGNORE
         <b>   <c>;<non-accent>;<lower-case>;IGNORE
         <c>   <b>;<non-accent>;<lower-case>;IGNORE
         <d>   <a>;<non-accent>;<lower-case>;IGNORE
   ```

3. Generate the new **gwm** file locale, by typing:

   ```
   localedef -f ISO08859-1 -i gwm.src gwm
   ```

4. Set the **LOCPATH** environment variable to the directory containing the new locale. If the new locale is in **/u/foo**, then type:

   ```
   LOCPATH=/u/foo:/usr/lib/nls/loc; export LOCPATH
   ```

   The default for **LOCPATH** is **/usr/lib/nls/loc**.

   Note: All **setuid** and **setgid** programs ignore the **LOCPATH** environment variable.

5. Change the **LC_COLLATE** environment variable to the name of the newly defined **gwm** locale binary, by typing:

   ```
   LC_COLLATE=gwm; export LC_COLLATE
   ```

   Any command now uses the collation order specified in the **gwm** locale. In the example in step 2, the characters `a-d` are sorted in reverse order by commands such as **ls** and **sort**.

Using the iconv Command

Any converter installed in the system can be used through the **iconv** command, which uses the **iconv** library. The **iconv** command acts as a filter for converting from one code set to another. For example, the following command filters data from PC Code (IBM-850) to ISO8859-1:

```
cat File | iconv -f IBM-850 -t ISO8859-1 | tftp -p - host /tmp/fo
```

The **iconv** command converts the encoding of characters read from either standard input or the specified file and then writes the results to standard output.

Also see the following topics in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*:

- Converters Introduction
- Understanding iconv Libraries

Using the Message Facility

To facilitate translation of messages into various languages and to make them available to a program based on a user's locale, it is necessary to keep messages separate from the program and provide them in the form of message catalogs that a program can access at run time. To aid in this task, the Message Facility provides commands and subroutines. Message source files containing application messages are created by the programmer and converted to message catalogs. These catalogs are used by the application to retrieve and display messages, as needed. Message source files can be translated into other languages and converted to message catalogs without changing and recompiling a program.

The Message Facility includes the following two commands for displaying messages with a shell script or from the command line:

dspcat	Displays all or part of a message catalog
dspmsg	Displays a selected message from a message catalog

These commands use the **NLSPATH** environment variable to locate the specified message catalog. The **NLSPATH** environment variable lists the directories containing message catalogs. These directories are searched in the order in which they are listed. For example:

```
NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lib/nls/msg/prime/%N
```

The `%L` and `%N` special variables are defined as follows:

%L Specifies the locale-specific directory containing message catalogs. The value of the **LC_MESSAGES** category or the **LANG** environment variable is used for the directory name. The **LANG**, **LC_ALL**, or **LC_MESSAGES** environment variable can be set by the user to the locale for message catalogs.

%N Specifies the name of the catalog to be opened.

If the **dspcat** command cannot find the message, the default message is displayed. You must enclose the default message in single-quotation marks if the default message contains **%*n*$** format strings. If the **dspcat** command cannot find the message and you do not specify a default message, a system-generated error message is displayed.

The following example uses the **dspcat** command to display all messages in the existing `msgerrs.cat` message catalog:

```
/usr/lib/nls/msg/$LANG/msgerrs.cat:
dspcat msgerrs.cat
```

The following output is displayed:

```
1:1 Cannot open message catalog %s
Maximum number of catalogs already open
1:2 File %s not executable
2:1 Message %d, Set %d not found
```

By displaying the contents of the message catalog in this manner, you can find the message ID numbers assigned to the msgerrs message source file by the **mkcatdefs** command to replace the symbolic identifiers. Symbolic identifiers are not readily usable as references for the **dspmsg** command, but using the **dspcat** command as shown can give you the necessary ID numbers.

The following is a simple shell script called **runtest** that shows how to use the **dspmsg** command:

```
if [ - x ./test ]
    ./test;
else
    dspmsg  msgerrs.cat -s 1 2 '%s NOT EXECUTABLE \n' "test";
    exit;
```

> **Note:** If you do not use a full path name, as in the preceding examples, be careful to set the **NLSPATH** environment variable so that the **dspcat** command searches the correct directory for the catalog. The **LC_MESSAGES** category or the value of the **LANG** environment variable also affects the directory search path.

Setting National Language Support for Devices

National Language Support (NLS) uses the locale setting to define its environment. The locale setting is dependent on the user's requirements for data processing and language that determines input and output device requirements. The system administrator is responsible for configuring devices that are in agreement with user locales.

- "Terminals (tty Devices)"
- "Printers"
- "Low-Function Terminals" on page 93

Terminals (tty Devices)

Use the **setmaps** command to set the terminal and code-set map for a given tty or pty. The **setmaps** file format defines the text of the code-set map file and the terminal map file.

The text of a code set map file is a description of the code set, including the type (single byte or multibyte), the memory and screen widths (for multibyte code sets), and the optional converter modules to push on the stream. The code set map file is located in the **/usr/lib/nls/csmap** directory and has the same name as the code set.

The terminal-map-file rules associate a pattern string with a replacement string. The operating system uses an input map file to map input from the keyboard to an application and uses an output map file to map output from an application to the display.

Printers

Virtual printers inherit the default code set of incoming jobs from the **LANG** entry in the **/etc/environment** file. A printer subsystem can support several virtual printers. If more than one virtual printer is supported, each can have a different code set. Three suggested printer subsystem scenarios are:

- The first scenario involves several queues, several virtual printers, and one physical printer. Each virtual printer has its own code set. The print commands specify which queue to use. The queue in turn specifies the virtual printer with the appropriate code set. In this scenario, the user needs to know which queue is attached to which virtual printer and the code set that is associated with each.

- The second scenario is similar to the first, but each virtual printer is attached to a different printer.
- The third scenario involves using the **qprt** print command to specify the code set. In this option, there are several queues available and one virtual printer. The virtual printer uses the inherited default code set.

Use the **qprt** command with the **-P-x** flags to specify the queue and code set. If the **-P** flag is not specified, the default queue is used. If the **-x** flag is not used, the default code set for the virtual printer is used.

Low-Function Terminals

Key Maps

Low-function terminals (LFTs) support single-byte code-set languages using key maps. An LFT key map translates a key stroke into a character string in the code set. A list of all available key maps is in the **/usr/lib/nls/loc** directory. LFT does not support languages that require multibyte code sets.

The default LFT keyboard setting and associated font setting are based on the language selected during installation. The possible default code sets are:

- ISO8859-1
- ISO8859-2
- ISO8859-5
- ISO8859-6
- ISO8859-7
- ISO8859-8
- ISO8859-9

There are several ways to change the default settings:

- To change the default font for next reboot, use the **chfont** command with the **-n** flag.
- To change the default keyboard for next reboot, use the **chkbd** command with the **-n** flag.

The **lsfont** and **lskbd** commands list all the fonts and keyboard maps that are currently available to the LFT.

Fonts

The LFT font libraries for all the supported code sets are in the **/usr/lpp/fonts** directory.

Changing the Language Environment

A number of system operations are affected by the language environment. Some of these operations include collation, time of day and date representation, numeric representation, monetary representation, and message translation. The language environment is determined by the value of the **LANG** environment variable, and you can change that value with the **chlang** command. The **chlang** command can be run from the command line or from SMIT.

Changing the Language Environment Task		
Task	*SMIT Fast Path*	*Command or File*
Change the Language Environment	**smit chlang**	**chlang** *Language*

Changing the Default Keyboard Map

NLS also enables you to specify the correct keyboard for the language you want to use. The operating system provides a number of keyboard maps for this purpose. You can change the default keyboard map for LFT terminals using Web-based System Manager (type `wsm`, then select `Devices`), the SMIT fast path, **smit chkbd**, or the **chkbd** command. The change does not go into effect until you restart the system.

National Language Support Commands and Files

National Language Support (NLS) provides several commands and files for system internationalization.

Converter Command

NLS provides a base for internationalization in which data can be changed from one code set to another. The following command can be used for this conversion:

iconv Converts the encoding of characters from one code set encoding scheme to another.

Input Method Command

An Input Method is a set of subroutines that translate key strokes into character strings in the code set specified by a locale. Input Method subroutines include logic for locale-specific input processing and keyboard controls (Ctrl, Alt, Shift, Lock, Alt Graphic). The following command allows for the customizing of input method mapping for the use of input method subroutines:

keycomp Compiles a keyboard mapping file into an input method keymap file.

For more information about these methods, see the Input Method Overview in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

Locale Commands and Files

NLS provides a database containing locale-specific rules for formatting data and an interface to obtain these rules.

Locale Commands

The following commands are provided for the creation and display of locale information:

locale Writes information about the current locale or all public locales

localedef Converts locale definition source files and character set description (charmap) source files to produce a locale database

Locale Source Files

The following files are provided for the specification of rules for formatting locale-specific data:

- **character set description (charmap)** — Defines character symbols as character encodings.
- **locale definition** — Contains one or more categories that describe a locale. The following categories are supported:

LC_COLLATE Defines character or string collation information.

LC_CTYPE Defines character classification, case conversion, and other character attributes.

LC_MESSAGES Defines the format for affirmative and negative responses.

LC_MONETARY Defines rules and symbols for formatting monetary numeric information.

LC_NUMERIC Defines a list of rules and symbols for formatting nonmonetary numeric information.

LC_TIME Defines a list of rules and symbols for formatting time and date information.

Message Facility Commands

The Message Facility consists of standard defined (X/Open) subroutines, commands, and value-added extensions to support externalized message catalogs. These catalogs are used by an application to retrieve and display messages, as needed. The following Message Facility commands create message catalogs and display their contents:

dspcat	Displays all or part of a message catalog
dspmsg	Displays a selected message from a message catalog
gencat	Creates and modifies a message catalog
mkcatdefs	Preprocesses a message source file for input to the **gencat** command
runcat	Pipes output from the **mkcatdefs** command to the **gencat** command

Chapter 11. Process Management

This chapter describes procedures that you, as the system administrator, can use to manage processes.

See “Chapter 11. Process Management” in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices* and see also *AIX 5L Version 5.1 System User’s Guide: Operating System and Devices* for basic information on managing your own processes; for example, restarting or stopping a process that you started or scheduling a process for a later time. The *AIX 5L Version 5.1 System User’s Guide: Operating System and Devices* also defines terms that describe processes, such as daemons and zombies.

Process Monitoring

The **ps** command is the primary tool for observing the processes in the system. Most of the flags of the **ps** command fall into one of two categories:

- Flags that specify which types of processes to include in the output
- Flags that specify which attributes of those processes are to be displayed

The most widely useful variants of **ps** for system-management purposes are:

ps -ef
Lists all nonkernel processes, with the userid, process ID, recent CPU usage, total CPU usage, and the command that started the process (including its parameters).

ps -fu *UserID*
Lists all of the processes owned by *UserID*, with the process ID, recent CPU usage, total CPU usage, and the command that started the process (including its parameters).

To identify the current heaviest users of CPU time, you could enter:

```
ps -ef | egrep -v "STIME|$LOGNAME" | sort +3 -r | head -n 15
```

This lists, in descending order, the 15 most CPU-intensive processes other than those owned by you.

For more specialized uses, the following two tables are intended to simplify the task of choosing **ps** flags by summarizing the effects of the flags.

Process Listed are:	**Process-Specifying Flags:**												
	-A	**-a**	**-d**	**-e**	**-G** **-g**	**-k**	**-p**	**-t**	**-U** **-u**	**a**	**g**	**t**	**x**
All processes	Y	-	-	-	-	-	-	-	-	-	Y	-	-
Not processes group leaders and not associated with a terminal	-	Y	-	-	-	-	-	-	-	-	-	-	-
Not process group leaders	-	-	Y	-	-	-	-	-	-	-	-	-	-
Not kernel processes	-	-	-	Y	-	-	-	-	-	-	-	-	-

Members of specified-process groups	-	-	-	-	Y	-	-	-	-	-	-	-	-
Kernel processes	-	-	-	-	-	Y	-	-	-	-	-	-	-
Those specified in process number list	-	-	-	-	-	-	Y	-	-	-	-	-	-
Those associated with tty(s) in the list	-	-	-	-	-	-	-	Y (*n* ttys)	-	-	-	Y (1 tty)	-
Specified user processes	-	-	-	-	-	-	-	-	Y	-	-	-	-
Processes with terminals	-	-	-	-	-	-	-	-	-	Y	-	-	-
Not associated with a tty	-	-	-	-	-	-	-	-	-	-	-	-	Y

Column:	**Column-Selecting Flags:**									
	Default1	**-f**	**-l**	**-U -u**	**Default2**	**e**	**l**	**s**	**u**	**v**
PID	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TTY	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TIME	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CMD	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USER	-	Y	-	-	-	-	-	-	Y	-
UID	-	-	Y	Y	-	-	Y	-	-	-
PPID	-	Y	Y	-	-	-	Y	-	-	-
C	-	Y	Y	-	-	-	Y	-	-	-
STIME	-	Y	-	-	-	-	-	-	Y	-
F	-	-	Y	-	-	-	-	-	-	-
S/STAT	-	-	Y	-	Y	Y	Y	Y	Y	Y
PIR	-	-	Y	-	-	-	Y	-	-	-
NI/NICE	-	-	Y	-	-	-	Y	-	-	-
ADDR	-	-	Y	-	-	-	Y	-	-	-
SZ/SIZE	-	-	Y	-	-	-	Y	-	Y	Y
WCHAN	-	-	Y	-	-	-	Y	-	-	-
RSS	-	-	-	-	-	-	Y	-	Y	Y
SSIZ	-	-	-	-	-	-	-	Y	-	-

%CPU	-	-	-	-	-	-	-	-	Y	Y
%MEM	-	-	-	-	-	-	-	-	Y	Y
PGIN	-	-	-	-	-	-	-	-	-	Y
LIM	-	-	-	-	-	-	-	-	-	Y
TSIZ	-	-	-	-	-	-	-	-	-	Y
TRS	-	-	-	-	-	-	-	-	-	Y
Environment (following the command)	-	-	-	-	-	Y	-	-	-	-

If **ps** is given with no flags or with a process-specifying flag that begins with a minus sign, the columns displayed are those shown for Default1. If the command is given with a process-specifying flag that does not begin with minus, Default2 columns are displayed. The **-u** or **-U** flag is both a process-specifying and column-selecting flag.

The following are brief descriptions of the contents of the columns:

PID Process ID
TTY Terminal or pseudo-terminal associated with the process
TIME Cumulative CPU time consumed, in minutes and seconds
CMD Command the process is running
USER Login name of the user to whom the process belongs
UID Numeric user ID of the user to whom the process belongs
PPID ID of the parent process of this process
C Recently used CPU time
STIME Time the process started, if less than 24 hours. Otherwise the date the process is started
F Eight-character hexadecimal value describing the flags associated with the process (see the detailed description of the **ps** command)
S/STAT Status of the process (see the detailed description of the **ps** command)
PRI Current priority value of the process
NI/NICE Nice value for the process
ADDR Segment number of the process stack
SZ/SIZE Number of working-segment pages that have been touched times 4
WCHAN Event on which the process is waiting
RSS Sum of the numbers of working-segment and code-segment pages in memory times 4
SSIZ Size of the kernel stack
%CPU Percentage of time since the process started that it was using the CPU
%MEM Nominally, the percentage of real memory being used by the process, this measure does not correlate with any other memory statistics
PGIN Number of page ins caused by page faults. Since all I/O is classified as page faults, this is basically a measure of I/O volume
LIM Always **xx**
TSIZ Size of the text section of the executable file
TRS Number of code-segment pages times 4
Environment Value of all the environment variables for the process

Altering Process-Priority

Basically, if you have identified a process that is using too much CPU time, you can reduce its effective priority by increasing its nice value with the **renice** command. For example:

```
renice +5 ProcID
```

The nice value of the *ProcID*'s would increase process from the normal 20 of a foreground process to 25. You must have root authority to reset the process *ProcID*'s nice value to 20. Type:

```
renice -5 ProcID
```

Terminating a Process

Use the **kill** command to end a process. The **kill** command sends a signal to the designated process. Depending on the type of signal and the nature of the program that is running in the process, the process might end or might keep running. The signals you send are:

SIGTERM (signal 15) is a request to the program to terminate. If the program has a signal handler for SIGTERM that does not actually terminate the application, this **kill** may have no effect. This is the default signal sent by **kill**.

SIGKILL (signal 9) is a directive to kill the process immediately. This signal cannot be caught or ignored.

Normally, it is desirable to issue SIGTERM rather than SIGKILL. If the program has a handler for SIGTERM, it can clean up and terminate in an orderly fashion. Type:

```
kill -term ProcessID
```

(The **-term** could be omitted.) If the process does not respond to the SIGTERM, type:

```
kill -kill ProcessID
```

Binding or Unbinding a Process

On multiprocessor systems, you can bind a process to a processor or unbind a previously bound process from:

- Web-based System Manager
- SMIT
- command line

> **Note:** While binding a process to a processor might lead to improved performance for the bound process (by decreasing hardware-cache misses), overuse of this facility could cause individual processors to become overloaded while other processors are underused. The resulting bottlenecks could reduce overall throughput and performance. During normal operations, it is better to let the operating system assign processes to processors automatically, distributing system load across all processors. Bind only those processes that you know can benefit from being run on a single processor.

Prerequisites

You must have root user authority to bind or unbind a process you do not own.

Binding or Unbinding a Process Tasks		
Task	*SMIT Fast Path*	*Command or File*
Binding a Process	**smit bindproc**	**bindprocessor -q**
Unbinding a Process	**smit ubindproc**	**bindprocessor -u**

Fixing Stalled or Unwanted Processes

Stalled or unwanted processes can cause problems with your terminal. Some problems produce messages on your screen that give information about possible causes.

To perform the following procedures, you must have either a second terminal, a modem, or a network login. If you do not have any of these, fix the terminal problem by rebooting your machine.

Choose the appropriate procedure for fixing your terminal problem:

- "Free a Terminal Taken Over by Processes"
- "Respond to Screen Messages" on page 102

Free a Terminal Taken Over by Processes

Identify and stop stalled or unwanted processes by doing the following:

1. Determine the active processes running on the screen by typing the following **ps** command:

   ```
   ps -ef | pg
   ```

   The **ps** command shows the process status. The **-e** flag writes information about all processes (except kernel processes), and the **f** flag generates a full listing of processes including what the command name and parameters were when the process was created. The **pg** command limits output to a single page at a time, so information does not quickly scroll off the screen.

   Suspicious processes include system or user processes that use up excessive amounts of a system resource such as CPU or disk space. System processes such as **sendmail**, **routed**, and **lpd** frequently become runaways. Use the **ps -u** command to check CPU usage.
2. Determine who is running processes on this machine by using the **who** command:

   ```
   who
   ```

   The **who** command displays information about all users currently on this system, such as login name, workstation name, date, and time of login.
3. Determine if you need to stop, suspend, or change the priority of a user process.

   Note: You must have root authority to stop processes other than your own. If you terminate or change the priority of a user process, contact the process owner and explain what you have done.

   - Stop the process using the **kill** command. For example:

     ```
     kill 1883
     ```

     The **kill** command sends a signal to a running process. To stop a process, specify the process ID (PID), which is 1883 in this example. Use the **ps** command to determine the PID number of commands.
   - Suspend the process and run it in the background by using the ampersand (&). For example:

     ```
     /u/bin1/prog1 &
     ```

     The **&** signals that you want this process to run in the background. In a background process, the shell does not wait for the command to complete before returning the shell prompt. When a process requires more than a few seconds to complete, run the command in background by typing an **&** at the end of the command line. Jobs running in the background appear in the normal **ps** command.
   - Change the priority of the processes that have taken over by using the following **renice** command:

     ```
     renice 20 1883
     ```

     The **renice** command alters the scheduling priority of one or more running processes. The higher the number, the lower the priority with 20 being the lowest priority.

     In the previous example, **renice** reschedules process number 1883 to the lowest priority. It will run when there is a small amount of unused processor time available.

Respond to Screen Messages

Respond to and recover from screen messages by doing the following:

1. Make sure the **DISPLAY** environment variable is set correctly. Use either of the following methods to check the **DISPLAY** environment:
   - Use the **setsenv** command to display the environment variables.

     ```
     setsenv
     ```

     The **setsenv** command displays the protected state environment when you logged in.

     Determine if the **DISPLAY** variable has been set. In the following example, the **DISPLAY** variable does not appear, which indicates that the **DISPLAY** variable is not set to a specific value.

     ```
     SYSENVIRON:
     NAME=casey
     TTY=/dev/pts/5
     LOGNAME=casey
     LOGIN=casey
     ```

     OR
   - Change the value of the **DISPLAY** variable. For example, to set it to the machine named `bastet` and terminal 0, enter:

     ```
     DISPLAY=bastet:0
     export DISPLAY
     ```

     If not specifically set, the **DISPLAY** environment variable defaults to `unix:0` (the console). The value of the variable is in the format *name*:*number* where *name* is the host name of a particular machine, and *number* is the X server number on the named system.
2. Reset the terminal to its defaults using the following **stty** command:

   ```
   stty sane
   ```

   The **stty sane** command restores the “sanity” of the terminal drivers. The command outputs an appropriate terminal resetting code from the **/etc/termcap** file (or **/usr/share/lib/terminfo** if available).
3. If the Return key does not work correctly, reset it by entering:

   ```
   ^J stty sane ^J
   ```

   The ^J represents the Ctrl-J key sequence.

RT_MPC and RT_GRQ

The use of multiple queues increases the processor affinity of threads, but there is a special situation where you might want to counteract this effect. When there is only one run queue, a thread that has been awakened (the waking thread) by another running thread (the waker thread) would normally be able to use the CPU immediately on which the waker thread was running. With multiple run queues, the waking thread may be on the run queue of another CPU which cannot notice the waking thread until the next scheduling decision. This may result in up to a 10 ms delay.

This is similar to scenarios in earlier releases of this operating system which migjht have occurred using the bindprocessor option. If all CPUs are constantly busy, and there are a number of interdependent threads waking up, there are two options available.

- The first option, which uses one run queue, is to set the environment variable RT_GRQ=ON which forces unbound selected threads to be dispatched off the global run queue.
- Alternatively, POWER-based platform users can choose the real time kernel option (type the command `bosdebug -R on` and then `bosboot`) and the RT_MPC=ON environment variable for selected processes.

It is essential to maintain a performance log of your systems to closely monitor the impact of any tuning you attempt. This option is not useful to Itanium-based platforms because the architecture does not perceive the result as a real-time kernel.

Chapter 12. Workload Manager

Workload Manager (WLM) is designed to give system administrators more control over how the scheduler and the virtual memory manager (VMM) allocate resources to processes. This can be used to prevent different classes of jobs from interfering with each other and to allocate resources based on the requirements of different groups of users.

WLM gives you the ability to create different classes of service for jobs, and specify attributes for those classes. These attributes specify minimum, optimum and maximum amounts of CPU, physical memory, and disk I/O bandwidth to be allocated to a class. The system administrator also defines class assignment rules used by WLM to assign jobs automatically to classes. These rules are based upon attributes of a process, such as the name of the user or group, the pathname of the applications executed, the type of process (that is, 32 bit or 64 bit), and the application tag.

WLM also provides isolation between user communities with very different system behaviors. This can prevent effective starvation of workloads with certain behaviors (for example, interactive or low CPU usage jobs) by workloads with other behaviors (for example, batch or high memory usage jobs).

Also, WLM ties into the accounting subsystem (see Accounting Overview in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*) allowing users to do resource usage accounting per WLM class in addition to the standard accounting per user or group.

Starting WLM

WLM is an optional service and must be started manually or automatically from **/etc/inittab**. The **wlmcntrl** command allows you to start and stop WLM.

All processes existing in the system before WLM is started are classified according to the newly loaded assignment rules, and are monitored by WLM.

Monitoring and Regulating Resource Allocation

WLM monitors and regulates the resource consumption at the class level. This means that WLM deals with the sum of the resources used by every process in the class.

Optionally, WLM can be started in a mode where it classifies new and existing processes and monitors the resource usage of the various classes, without attempting to regulate this usage. This mode is called the **passive** mode. The mode where WLM is fully enabled and does monitoring and regulation of resource utilization is called the **active** mode. The **passive** mode can be used when configuring WLM on a new system to verify the classification and assignment rules, and to establish a base line of resource utilization for the various classes when WLM does **not** regulate the CPU and memory allocation. This should give a basis for system administrators to decide how to apply the resource shares and resource limits (if needed) to favor critical applications and restrict less important work in order to meet their business goals.

In active mode, WLM attempts to keep active classes close to their targets. Since there are few constraints on the values of the various limits (as mentioned in Managing Resources with WLM in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*), the sum of any of the limits across all classes could far exceed 100%. In this case, if all of the classes are active, the limit cannot be reached by all classes. WLM regulates the CPU consumption by adjusting the scheduling priorities of the threads in the system according to how the class they belong to is performing, relative to its limits and target. This approach guarantees a CPU consumption averaged on a certain period of time, not the CPU consumption on very short intervals (for example, 10 ms ticks).

For example, if class A is the only one active, with a CPU minimum of 0% and a CPU target of 60 shares, then it gets 100% of the CPU. If class B, with a CPU minimum limit of 0% and a CPU target of 40 shares, becomes active, then class A's CPU utilization progressively decreases to 60% and class B's CPU utilization increases from 0 to 40%. The system stabilizes at 60% and 40% CPU utilization, respectively, in a matter of seconds.

This example supposes that there is no memory contention between the classes. Under regular working conditions, the limits you set for CPU and memory are interdependent. For example, a class may be unable to reach its target or even its minimum CPU allocation if the maximum limit on its memory usage is too low compared to its working set. Processes in the class wait to begin.

To help refine the class definition and class limits for a given set of applications, WLM provides the wlmstat reporting tool, which shows the amount of resource currently being used by each class. A graphical display tool, *wlmmon*, is also provided for system monitoring.

Specifying WLM Properties

The system administrator can specify the properties for the WLM subsystem by using either the Web-based System Manager graphical user interface, SMIT ASCII-oriented interface, the WLM command line interface, or by creating flat ASCII files. The Web-based System Manager and SMIT interfaces use the WLM commands to record the information in the same flat ASCII files. These files are named as follows:

classes	Class definitions
description	Configuration description text
limits	Class limits
shares	Class target shares
rules	Class assignment rules

These files are called the WLM property files. A set of WLM property files defines a WLM configuration. You can create multiple sets of property files, defining different configurations of workload management. These configurations are located in subdirectories of **/etc/wlm**. The WLM property files describing the superclasses of the *Config* configuration are the file's *classes*, *description*, *limits*, *shares* and *rules* in **/etc/wlm/Config**. Then, the property file's describing the subclasses of the superclass *Super* of this configuration are the file's *classes*, *limits*, *shares* and *rules* in directory **/etc/wlm/Config/Super**. Only the root user can star or stop WLM, or switch from one configuration to another.

The command to submit the WLM property files, **wlmcntrl**, and the other WLM commands allow users to specify an alternate directory name for the WLM properties files. This allows you to change the WLM properties without altering the default WLM property files.

A symbolic link, **/etc/wlm/current**, points to the directory containing the current configuration files. Update this link with the **wlmcntrl** command when you start WLM with a specified set of configuration files. The sample configuration files shipped with the operating system are in **/etc/wlm/standard**.

Defining Classes

In order to fully define a class, you must give it a name. You can also specify the values of the class attributes for which you want a value different from the system or user defined default. These attributes are the tier number, inheritance, and the name of the user or group of users authorized to manually assign processes to the class. In addition, when defining a superclass you can specify the name of the user or group of users authorized to perform the administration of the subclasses for this superclass. Next, you define the CPU, physical memory, disk I/O shares and resource limits, followed by the class assignment rules for this class. These rules are used by WLM to automatically assign processes to the class at exec time. The system administrator must provide a set of rules used to assign processes to one of the superclasses. For each superclass with user defined subclasses, either the system administrator or a superclass administrator authorized by the system administrator must provide rules to assign processes to one of the subclasses of the superclass.

Command Line Interfaces

WLM offers command-line interfaces, which allow system administrators to:

- Create, modify, and delete superclasses and subclasses, using the **mkclass**, **chclass**, and **rmclass** commands. These commands update the file's *classes*, *shares* and *limits*.
- Start, stop, and update WLM, using the **wlmcntrl** command.
- Check the WLM property files for a given configuration and determine to which class (superclass and subclass) a process with a given set of attributes is assigned using the **wlmcheck** command.
- Monitor the per-class resource utilization using the **wlmstat** (ASCII) command. Most of the performance tools, such as those started by the **svmon** and **topas** commands, have extensions to take into account the WLM classes and provide per-class and per-tier statistics using new command-line options.
- Flags in the **ps** command allow the user to display which class a process and its application tag is in. The **ps** command also allows the user to list all the processes belonging to a given superclass or subclass.
- There is no command line interface to manage the assignment rules. You must use the SMIT or Web-based System Manager administration tools, or a text editor.

Getting Started With Workload Manager

This example shows the different steps involved in creating and starting a new WLM configuration. It does not discuss how to determine the values of the shares and limits best suited for your set of business goals. Setting these values is system-, application-, and business-dependent and must be done on a case-by-case basis. WLM Concepts provides tips on how to determine the classification and resource control parameters.

The steps in the following example are completed using the WLM command-line interface. For each step, brief instructions describe how to complete each step using SMIT or the Web-based System Manager.

Step 1: Create the Configuration

Managing WLM configuration and administering the superclasses requires root authority. The first few steps are completed as root user. For more information on root authority, see WLM Concepts.

The easiest way to create a new configuration is by duplicating an existing configuration and then modifying the properties of the new configuration. WLM provides a sample configuration, called **template**, that defines the predefined superclasses Default, System, and Shared.

Create a new configuration, **new_config**, by first creating the **/etc/wlm/new_config** directory and then copying the files from the **/etc/wlm/template** directory:

> **Note:** You must be logged in as root user to perform this task.

```
cd /etc/wlm

cp -pr /etc/wlm/template new_config
```

Verify that the **new_config** directory is owned by the root user, has read, write, and execute permission only for owner, and has read and execute permission for group and other. For example:

```
ls -l /etc/wlm/new_config
total 40
-rw-r--r--   1 root    system       423 Jun 29 14:16 classes
-rw-r--r--   1 root    system        55 Jun 29 14:16 description
-rw-r--r--   1 root    system       430 Jun 29 14:16 limits
-rw-r--r--   1 root    system       496 Jun 29 14:16 rules
-rw-r--r--   1 root    system       404 Jun 29 14:16 shares
```

```
lsclass -d new_config
System
Default
Shared
```

The newly created configuration has a set of WLM property files describing the predefined superclasses System, Default, and Shared. Use a text editor to modify *description* to reflect the new configuration.

Using SMIT, for instance, to do the same thing, go to the **Workload Manager's** main menu (type **wlm** on the command line or from the SMIT main menu, select **Performance & Resource Scheduling** and then **Workload Management**). Then, select **Work on alternate configurations** and go to **Copy a configuration**. Provide **template** as the name of the configuration to copy and **new_config** as the name of the new configuration, and press the Enter key.

To continue working on the new configuration, go back to the Configurations menu, and select **Select a configuration**. Enter or select **new_config** as the configuration name, and press the Enter key. From this point on, the default configuration for your SMIT WLM session is **new_config** until you select another configuration from the Select a configuration menu, or until you exit SMIT. If you do not select a configuration, you will be working on the current configuration with the directory tree pointed to by **/etc/wlm/current**.

Using Web-based System Manager, you must also select the configuration whenever you work on a configuration other than **current**.

Step 2: Create Your Superclasses

Now create two superclasses with a basic set of attributes and show the delegated administration of subclasses.

For example, as root user, type the following on the command line:

```
mkclass -a inheritance=yes -a tier=1 -c shares=1 -m shares=1 \
-d new_config super1
```

This command creates a superclass named **super1** in the configuration **new_config** in superclass tier 1 with the *inheritance* attribute set to yes. **super1** is assigned one share of CPU and one share of memory. All the other attributes, resource entitlements, and limits are set to their default value. For additional information, see WLM Concepts.

To create another superclass, **super2**, in tier 1 with two shares of CPU and three shares of memory and delegate the administration of its subclasses to the user wlmu0, type the following on the command line:

```
mkclass -a tier=1 -a adminuser=wlmu0 -c shares=2 -m shares=3 \
     -d new_config super2
```

Type the following on the command line to verify the settings:

```
lsclass -d new_config
```

The results should read:

```
System
Default
Shared
super1
super2
root #
```

In this example, the two user-defined superclasses are added to three predefined superclasses created in Step 1.

To create the same superclasses in SMIT, select the configuration in Step 1, use the Add a class submenu to create **super1**. This menu allows you to create the superclass and set up the general characteristics of the class (attributes *description*, *inheritance*, *tier*, *authuser*/*authgroup*, *adminuser*/*admingroup*, and *rset*). Then from the Change/Show Characteristics of a class menu, select**resource management** (CPU, memory, and disk I/O) to set up the entitlements listed above.

Repeat these steps for **super2**. Web-based System Manager requires similar steps.

Step 3: Create Superclass Assignment Rules

Now create a set of assignment rules to assign processes to these superclasses.

There is no command-line interface to add, modify, or delete assignment rules. Use SMIT or Web-based System Manager to modify assignment rules. With SMIT with the configuration still active, select **Class assignment rules** -> **List all Rules** to see what is already in the file, then **Create a new Rule** for each rule that you want to create.

After creating the two rules, type the following on the command line to verify the results:

```
cat /etc/wlm/new_config/rules
```

The results should be similar to the following:

```
* class resvd user       group application  type  tag
super1   -    wlmu[3-6]    -       -         -     -
super2   -    wlmu[0-2]    -       -         -     -
System   -    root         -       -         -     -
Default  -    -            -       -         -     -
```

The new rules assign all processes with a real user ID of wlmu3, wlmu4, wlmu5, or wlmu6 to **super1**, and the processes with a real user ID of wlmu0, wlmu1, or wlmu2 to **super2**.

WLM matches processes by comparing them to the rules in the order that they appear in the file and then assigns the process to the class corresponding to the first rule that is matched. In the preceding example, a process with a real user ID of wlmu1 will be assigned to **super2**.

When we added our rules, the rules file already contained the assignment rules for the System and Default predefined superclasses.

If the same process used a real user ID of wlmu1, it would be assigned to the Default superclass.

Step 4: Start Workload Manager

All steps up to this point modified WLM property files. Even if we had been working on the current configuration and if WLM was already started, the new classes would not exist in the WLM kernel data structures and the new rules would not be available to the operating system.

The new configuration or changes to the current configuration are loaded into the WLM kernel data structures when WLM is started or when WLM is updated or refreshed. Then WLM starts classifying processes and managing resources according to the rules and policies defined in the new current configuration.

The **wlmcntrl** command does extensive processing on the WLM configuration files before handing the data down to the kernel. The **wlmcntrl** command processes the wildcards and pattern-matching characters in the user name, group name, and application file name fields of the rules file. In the case of the rule for **superclass2**, for instance, we specified wlmu[0-2]. The **wlmcntrl** command would expand the list to wlmu0, wlmu1, and wlmu2, and pass the corresponding UIDs, for instance 221, 222, and 223, to the kernel. This is also true for any specified group names. For application file path names, **wlmcntrl** also handles wildcard expansion to build a list of names. After that, prior to passing the data to the kernel, it would try to access every file and get an identification of each file in a format easier to manage by the kernel.

In the following example, WLM is not running. Start WLM on the new configuration using the **wlmcntrl** command, by typing the following on the command line:

```
wlmcntrl -d new_config
wlmcntrl -q
```

The following message appears on the command line:

```
WLM is running
```

All existing processes are classified according to the rules defined above. To see how the processes are classified, use the **ps** command as follows:

```
ps -e -o pid,ppid,user,class,pri,args
```

The output should be similar to the following:

```
PID    PPID    USER CLASS        PRI COMMAND
    1     0    root System        83 /etc/init
 8634  9860    root System        83 /usr/sbin/inetd
 8958  9860    root System        83 /usr/sbin/hostmibd
 9332     1    root System        83 /usr/sbin/syncd 60
 9606     1    root System        83 /usr/lib/errdemon
 9860     1    root System        83 /usr/sbin/srcmstr
10180  9860    root System        83 /usr/sbin/portmap
11376  9860    root System        83 /usr/sbin/snmpd
11962  9860    root System        83 /usr/sbin/biod 6
12208  9860    root System        83 /usr/sbin/syslogd
12408  9860    root System        83 sendmail: rejecting connections on port
12768     1    wlmu0 super2      159 /tmp/test12
12942  9860    root System        83 /usr/sbin/dpid2
13158     1    root System        83 /usr/ccs/bin/shlap
13432  9860    root System        83 /usr/sbin/rpc.lockd
13682  9860    daemon Default     60 /usr/sbin/rpc.statd
13942     1    root System        83 -ksh
14198     1    root System        83 /usr/sbin/cron
14456     1    root System        83 /usr/sbin/uprintfd
14730  9860    root System        83 /usr/sbin/writesrv
15004  9860    root System        83 /usr/sbin/qdaemon
15224     1    root System        83 /usr/bin/AIXPowerMgtDaemon
15742     1    root System        83 /usr/sbin/getty /dev/tty1
16256     1    root System        83 /usr/lpp/diagnostics/bin/diagd
16788     1    wlmu1 super2      159 /tmp/test14
17062     1    wlmu0 super2      159 /tmp/test2
17802     1    wlmu1 super2      159 /tmp/test15
18318     1    wlmu2 super2      159 /tmp/test19
18834     1    wlmu3 super1      235 /tmp/test9
19350     1    wlmu3 super1      235 /tmp/test0
19866     1    wlmu3 super1      235 /tmp/test1
20382     1    wlmu4 super1      235 /tmp/test11
20898     1    wlmu4 super1      235 /tmp/test4
21414     1    wlmu5 super1      235 /tmp/test7
21930     1    wlmu6 super1      235 /tmp/test7
22446     1    wlmu6 super1      235 /tmp/test17
22962     1    wlmu10 Default     85 /tmp/test17
23478     1    wlmu10 Default     85 /tmp/test8
23750 13942    root System        84 ps -e -o pid,ppid,user,class,pri,args
```

In the above output, processes are assigned according to the following:

- Processes with the user ID of root are in the System class
- Processes with the user ID of wlmu0, wlmu1, or wlmu2 are in **super2**

- Processes with the user ID of wlmu3, wlmu4, wlmu5, or wlmu6 are in **super1**
- Processes with other user IDs (in this example, wlmu10 and daemon) are in the Default class

The **-c** flag for the **ps** command displays all processes for a given class. To list all the processes that belong to the superclass **super1**, type the following on the command line:

```
ps -l -c super1
```

The output should look similar to the following:

```
F S UID   PID  PPID  C PRI NI ADDR      SZ    WCHAN    TTY TIME CMD
240001 A 224 18834    1  84 235 20 3402ed    68            0  7:24 test9
240001 A 224 19350    1  85 235 20 3c02ef    68            0  7:19 test0
240001 A 224 19866    1  85 235 20 4402f1    68            0  7:15 test1
240001 A 223 20382    1  84 235 20 4c02f3    68            0  7:07 test11
240001 A 223 20898    1  85 235 20 5402f5    68            0  6:58 test4
240001 A 222 21414    1  85 235 20 5c02f7    68            0  6:42 test7
240001 A 221 21930    1  84 235 20 6402f9    68            0  6:14 test7
240001 A 221 22446    1  85 235 20 6c02fb    68            0  6:05 test17
```

With WLM running, use the **wlmstat** command to list the per-class resource utilization statistics:

```
wlmstat
```

The output should look similar to the following:

```
       CLASS CPU MEM BIO
Unclassified   0   0   0
   Unmanaged   0   0   0
     Default   8   0   0
      Shared   0   0   0
      System   0   0   0
      super1  33   0   0
      super2  21   0   0
```

The programs *testXX* are CPU loops, so memory and disk I/O have no output.

Step 5: Create and Manage Subclasses

Up to this point, all steps were done as root user. Only root can create a new configuration, create and manage superclasses, start and stop WLM, switch between active and passive mode, and change the current configuration.

When creating a superclass for a given configuration, the system administrator working as root user can delegate the authority to create and manage subclasses to a user or group and refresh the WLM kernel data pertaining to the subclasses managed.

For superclass **super2**, this authority has been delegated to user wlmu0 (attribute *adminuser* of the superclass **super1** of the configuration **new_config**).

Log in as wlmu0 and type the following on the command line:

```
mkclass -a tier=0 -a authuser=wlmu2 -c shares=10 -d new_config -S super2 sub1
```

This command creates a subclass of superclass **super2** named sub1, in subclass tier 0, with ten shares of CPU and gives user wlmu2 the authority to manually assign processes to **super2.sub1**.

> **Note: super2.sub1** is the fully qualified name of the subclass and uniquely identifies the subclass for a given configuration. Subclasses in different superclasses can have the same short name.

To create the subclass **super2.sub1** in tier 3, with 20 shares of CPU, type the following on the command line:

```
mkclass -a tier=3 -c shares=20 -d new_config -S super2 sub2
```

For superclasses, all the attributes, resource entitlements, and limits not explicitly specified are assigned the system default value.

The major differences between superclasses and subclasses are in the scope of the resource entitlements and limits:

- At the superclass level, the system administrator distributes a portion of the total system resources to each superclass.
- At the subclass level, the ″superclass administrator″ (the system administrator or someone with delegated authority) redistributes among the subclasses whatever resources have been allocated to the superclass between the subclasses.

To verify what has been defined up to this point, type the following on the command line:

```
lsclass -d new_config -r
```

The output should look similar to the following:

```
System
Default
Shared
super1
super2
super2.Default
super2.Shared
super2.sub1
super2.sub2
wlmu0 $
```

Use the **-r** flag of the **lsclass** command to list both superclasses and subclasses.

To create subclasses using SMIT, first set the focus on the superclass with which you want to work. To do this, select the Work on alternate configurations/Select a configuration menu. Select **new_config** -> **Work on a set of Subclasses**, then select the superclass **super2**. At any point during your SMIT session, you can verify which configuration or superclass you are working with by selecting the **Show current focus** menu. Web-based System Manager has similar options and requirements.

After you select the desired configuration and superclass, create the subclasses using the same Add a class and Change/Show Characteristics of a class menus used for superclasses.

> **Note:** The WLM configuration **new_config** is the active configuration pointed to by **/etc/wlm/current**, so you do not need to select **new_config** in SMIT (or Web-based System Manager). It is, however, good practice to always select the configuration you wish to work with whenever you have several WLM configurations in **/etc/wlm**. If the system administrator or a **cron**-initiated script switches the WLM configuration in the middle of your SMIT or Web-based System Manager session, you might end up with part of your changes in one configuration and the rest in another configuration.

As with the superclasses, for processes to be assigned to one of the new subclasses, a set of assignment rules must be provided.

Step 6: Create Subclass Assignment Rules

Use either SMIT or the Web-based System Manager to create subclass assignment rules. First, set the appropriate focus by selecting **new_config** and **super2**. The assignment rules for subclasses use the same process attributes and have the same format. Here are the rules we have entered:

```
cat /etc/wlm/new_config/super2/rules
* class resvd user group application type tag
sub1 - wlmu1
sub2 - wlmu2
```

The automatic assignment works by comparing a process attribute against the values in the superclass assignment rules file for the active (current) configuration to determine in which superclass the process will be assigned. Then, if there are subclasses, the process attributes are compared against the values in the subclasses rules file to determine the subclass.

For a subclass rule to be effective, it must be compatible with its superclass's rules. For example, in our case, according to the superclass rules, a process is assigned to **super2** if its real UID is wlmu0, wlmu1, or wlmu2.

If we had decided that a process of this superclass would be assigned to a given subclass when its real UID is wlmu5, no process assigned to **super2** would satisfy this condition. This subclass would therefore remain empty.

Now that the subclass definitions and the corresponding assignment rules are created, you can activate the new subclasses. Recall that the changes take place only in the configuration files. The new classes do not become active until the changes are communicated to the kernel.

To view the WLM statistics at this point, type the following on the command line:

```
wlmstat
```

Notice in the following example output that the subclasses are not yet displayed.

```
           CLASS CPU MEM BIO
    Unclassified   0   0   0
       Unmanaged   0   0   0
         Default   8   0   0
          Shared   0   0   0
          System   0   0   0
          super1  33   0   0
          super2  21   0   0
```

Step 7: Update WLM

The **wlmcntrl** command passes the class definitions to the kernel. With WLM already active, you can update the WLM kernel data structures using the **-u** flag. In addition, as a superclass administrator, you can only update the data corresponding to the subclasses of this superclass. Because you are not logged in as root user, the **wlmcntrl** command does not start or stop WLM, or load a new configuration, so a superclass administrator cannot affect other superclasses.

To update the superclass, type the following on the command line:

```
wlmcntrl -u -S super2
```

To view the updated WLM kernel data structures with the new subclasses, type the following on the command line:

```
wlmstat -a
```

The output should be similar to the following:

```
           CLASS CPU MEM BIO
    Unclassified   0   0   0
       Unmanaged   0   0   0
         Default   8   0   0
          Shared   0   0   0
          System   0   0   0
          super1  33   0   0
          super2  19   0   0
super2.Default    12   0   0
 super2.Shared     0   0   0
   super2.sub1     5   0   0
   super2.sub2     2   0   0
```

Using the **-a** flag displays the subclass resource usage as a percentage of the total system resources. In this case, the combined processes in **super2** consume 19% of the CPU time and these 19% are decomposed in 12% in the Default subclass, 5% in sub1, and 2% in sub2. Without the **-a** flag, the percentage shown for the subclasses is a percentage of the resource consumed by the superclass. To view the resource consumed as a percentage of superclass, type `wlmstat` on the command line and press the Enter key. The result should look similar to the following:

```
           CLASS CPU MEM BIO
    Unclassified   0   0   0
       Unmanaged   0   0   0
         Default   8   0   0
          Shared   0   0   0
          System   0   0   0
          super1  33   0   0
          super2  19   0   0
super2.Default    63   0   0
 super2.Shared     0   0   0
   super2.sub1    26   0   0
   super2.sub2    11   0   0
```

This output shows that Default subclass accounts for 63% of the CPU consumed by the superclass, sub1 for 26%, and sub2 for 11%. Recall that the shares and limits for a subclass are relative to the superclass entitlements and not to the total amount of the resource available on the system.

To view the **ps** output now that the subclasses are active, type the following on the command line:

```
ps -e -o pid,ppid,user,class,pri,args | grep super2
```

The output should be similar to the following:

```
12768     1   wlmu0 super2.Default 170 /tmp/test12
16788     1   wlmu1 super2.sub1    159 /tmp/test14
17062     1   wlmu0 super2.Default 170 /tmp/test2
17802     1   wlmu1 super2.sub1    159 /tmp/test15
18318     1   wlmu2 super2.sub2    207 /tmp/test19
23782 13942   wlmu0 super2.Default 168 -ksh
24032 23782   wlmu0 super2.Default 168 grep super2
25040 23782   wlmu0 super2.Default 169 ps -e -o pid,ppid,user,class,pri,args
```

Examine the WLM property files that we have just created in the **/etc/wlm/new_config** directory:

```
-rw-r--r-- 1 root   system  112 Jul  2 17:56   classes
-rw-r--r-- 1 root   system   55 Jun 29 14:16   description
-rw-r--r-- 1 root   system   31 Jun 29 16:35   limits
-rw-r--r-- 1 root   system  544 Jun 29 14:27   rules
-rw-r--r-- 1 root   system   78 Jun 29 16:35   shares
drwxr-xr-x 2 wlmu0  system  512 Jun 29 15:20   super2
-rw-r--r-- 1 wlmu0  staff    72 Jun 29 14:57   super2/rules
-rw-r--r-- 1 wlmu0  staff     0 Jun 29 14:55   super2/limits
-rw-r--r-- 1 wlmu0  staff    40 Jun 29 14:55   super2/shares
-rw-r--r-- 1 wlmu0  staff    98 Jun 29 14:55   super2/classes
```

Directly under **/etc/wlm/new_config**, the WLM property files for the superclasses have write permission only for root user. Under **/etc/wlm/new_config/super2**, the WLM property files for the subclasses of the superclass **super2** have write permission for wlmu0. This is expected because wlmu0 was designated as superclass administrator for **super2**. The owner and permissions would be the same if root user had created the subclasses. If the system administrator had designated a group as superclass administrator using the class attribute *admingroup*, then the group ID for the files would be set accordingly and the files would have write permission for the group. This can become complex when the system administrator changes a superclass administrator (by changing *adminuser*, for instance), but the **chclass** command changes the file ownership and permission automatically.

After you have created your first test configuration, you can experiment with the passive and active modes of WLM, change shares, and set limits. Examine how the system reacts using the**wlmstat** command and experiment with other features of WLM, such as the manual assignment of processes.

SMIT, Web-based System Manager, and the command line interfaces all perform the steps necessary to manage WLM configurations. Functions of WLM that are not supported by all three interfaces include:

- The **cron** facility and the WLM command-line interfaces enable the system administrator to activate different WLM configurations depending on the time of day or day of the week. There is no SMIT or Web-based System Manager support for this functionality.
- SMIT and Web-based System Manager both offer menus to create and name resource sets for use with WLM to restrict some classes to a subset of the system resources or a subset of the processors available on the system. System administrators must use either SMIT or Web-based System Manager to define resource sets. The corresponding menus in SMIT and WLM are part of the Performance & Resource Scheduling menu. This submenu is called **Resource Set Management** (see “Resource Sets Management”).
- Setting specific default values for the attributes in the stanza files **classes**, **shares**, and **limits** is not supported by SMIT, Web-based System Manager, or the command line interfaces. Administrators must use a text editor to manually modify the stanza files.

Resource Sets Management

WLM uses the concept of resource sets (or *rsets*) to restrict the processes in a given class to a subset of the system’s physical resources. In WLM, the physical resources managed are the memory and the processors. A valid resource set is composed of memory and at least one processor.

Using SMIT or Web-based System Manager, a system administrator can define and name resource sets containing a subset of the resources available on the system. Then, using the WLM administration interfaces, root user or a designated superclass administrator can use the name of the resource set as the **rset** attribute of a WLM class. From then on, every process assigned to this WLM class is dispatched only on one of the processors in the resource set, effectively separating workloads for the CPU resource.

All of the current systems have only one memory domain shared by all the resource sets, so this method does not physically separate workloads in memory.

Rset Registry

The **rset** registry services enable system administrators to define and name resource sets so that they can then be used by other users or applications. To alleviate the risks of name collisions, the registry supports a two-level naming scheme. The name of a resource set is in the form *name_space***/***rset_name*. Both the *namespace* and *rset_name* can each be 255 characters in length, are case-sensitive, and may contain only uppercase and lowercase letters, numbers, underscores, and periods (**.**). The *namespace* of **sys** is reserved by the operating system and used for **rset** definitions that represent the resources of the system.

The **rset** definition names are unique within the registry name space. Adding a new **rset** definition to the registry using the same name as an existing **rset** definition causes the existing definition to be replaced with the new definition, given the proper permission and privilege. Only root can create, modify, and delete resource sets and update the in-core **rset** data base, using SMIT or Web-based System Manager.

Each **rset** definition has an owner (user ID), group (group ID), and access permissions associated with it. These are specified at the time the **rset** definition is created and exist for the purpose of access control. As is the case for files, separate access permissions exist for the owner, group and others that define whether read and/or write permission has been granted. Read permission allows an **rset** definition to be retrieved while write permission allows an rset definition to be modified or removed.

System Administrator defined **rset** definitions are kept in the **/etc/rsets** stanza file. The format of this file is not described, and users must manipulate **rsets** through the SMIT or Web-based System Manager interfaces to prevent future potential compatibility problems if the file format is modified. As is the case for WLM class definitions, the **rset** definitions must be loaded into kernel data structures before they can be used by WLM.

Rather than giving an extensive definition of resource sets and how to create them from basic building blocks called *system RADs* (Resource Access Domains), the following example details what is in a resource set and how to create new one.

Creating a Resource Set

The following example is on a 24-way system. The system administrator wants to create a resource set containing processors 0 to 5, and use it in WLM configuration to restrict all processes of a superclass to these six processors. This example uses SMIT, but the same steps can be done with Web-based System Manager.

The first step is to create and name the resource set. The system administration gets to the Resource Set Management menu either from the initial menu by selecting **Performance & Resource Scheduling** and then **Resource Set Management** or by using the fast path `smit rset`.

The **Manage Resource Set Database** option is used to create, modify, or delete **rset**. Before selecting **Manage Resource Set Database**, select **List All System RADs** to see what building blocks are available from which to create the resource sets:

```
COMMAND STATUS
Command: OK           stdout: yes          stderr: no
Before command completion, additional instructions may appear below.
T  Name              Owner   Group   Mode    CPU  Memory  Resources
r  sys/sys0          root    system  r-----   24   98298  sys/sys0
r  sys/node.00000    root    system  r-----   24   98298  sys/sys0
r  sys/mem.00000     root    system  r-----    0   98298  sys/mem.00000
r  sys/cpu.00023     root    system  r-----    1       0  sys/cpu.00023
r  sys/cpu.00022     root    system  r-----    1       0  sys/cpu.00022
r  sys/cpu.00021     root    system  r-----    1       0  sys/cpu.00021
r  sys/cpu.00020     root    system  r-----    1       0  sys/cpu.00020
r  sys/cpu.00019     root    system  r-----    1       0  sys/cpu.00019
r  sys/cpu.00018     root    system  r-----    1       0  sys/cpu.00018
r  sys/cpu.00017     root    system  r-----    1       0  sys/cpu.00017
r  sys/cpu.00016     root    system  r-----    1       0  sys/cpu.00016
r  sys/cpu.00015     root    system  r-----    1       0  sys/cpu.00015
r  sys/cpu.00014     root    system  r-----    1       0  sys/cpu.00014
r  sys/cpu.00013     root    system  r-----    1       0  sys/cpu.00013
r  sys/cpu.00012     root    system  r-----    1       0  sys/cpu.00012
r  sys/cpu.00011     root    system  r-----    1       0  sys/cpu.00011
r  sys/cpu.00010     root    system  r-----    1       0  sys/cpu.00010
r  sys/cpu.00009     root    system  r-----    1       0  sys/cpu.00009
r  sys/cpu.00008     root    system  r-----    1       0  sys/cpu.00008
r  sys/cpu.00007     root    system  r-----    1       0  sys/cpu.00007
r  sys/cpu.00006     root    system  r-----    1       0  sys/cpu.00006
r  sys/cpu.00005     root    system  r-----    1       0  sys/cpu.00005
r  sys/cpu.00004     root    system  r-----    1       0  sys/cpu.00004
r  sys/cpu.00003     root    system  r-----    1       0  sys/cpu.00003
r  sys/cpu.00002     root    system  r-----    1       0  sys/cpu.00002
r  sys/cpu.00001     root    system  r-----    1       0  sys/cpu.00001
r  sys/cpu.00000     root    system  r-----    1       0  sys/cpu.00000
```

As mentioned earlier, **sys/sys0** represents the whole system (in this case, a 24-way SMP with 96GB of memory). This set is what processes in those WLM classes that do not specify a **rset** attribute potentially have access to. Later, we will select the memory and some of the CPUs when creating our resource set.

Select **Manage Resource Set Database**, then select **Add a Resource Set to the Database**. From the resulting screen, enter or select the **Name Space** and **Resource Set Name** and then select the other attributes of the resource sets. In our case, we are creating a new namespace and resource set, so we enter the character strings for the **Name Space** and **Resource Set Name** fields.

Fill in the other fields by selecting from lists. For the **Resources** field, select from a list of the System RADs. In this case, select the lines corresponding to the memory and CPUs 0 to 5 (sys/cpu.00000 to sys.cpu.00005). Remember that only processor sets are supported. Press Enter after the selections to create a new rset named **admin/proc0_5**.

At this point, a new **rset** is created in **/etc/rsets**. To use the new **rset**, add it into the kernel data structures by selecting **Reload Resource Set Database**. This menu gives you the option to reload the data base `now`, `at next boot` or `both`. The first time you create a new resource set, select `both` so that your administrator-defined resource sets are loaded after each reboot and can be used by WLM. After that, you would probably select `now`.

Now that we have our new resource set, we will use it in WLM using the **new_config** defined in the previous article.

We want to go back to the definition of the superclass super1 and set up the **rset** attribute to use the new **rset**. Using SMIT, go to the **Workload Manager's** main menu (fast path **smit wlm**), then to **Work on alternate configurations** and on to **Select a configuration** and select **new_config**. We then go back to the main menu and from there to **Change / Show Characteristics of a class** and on to **General characteristics of a class**. Enter or select **super1** as the class name and press Enter to display the class attributes.

Scroll to the **rset** field, press F4 to get the list of available **rsets**, and select the newly created **admin/proc0_5**. After you have selected the new **rset** and committed the modification, the **classes** file on disk is changed.

After starting (or updating if it was already running) WLM with the new class definition as explained in the previous article, the following is a quick test to show the effect of the resource set on **super1**:

- We start 90 CPU loops (program executing an infinite loop) in class **super1**.
- We get a **wlmstat** output similar to the following:

  ```
  root # wlmstat
             CLASS CPU MEM BIO
      Unclassified   0   0   0
         Unmanaged   0   0   0
           Default   8   0   0
            Shared   0   0   0
            System   0   0   0
            super1  25   0   0
            super2   0   0   0
  super2.Default     0   0   0
   super2.Shared     0   0   0
     super2.sub1     0   0   0
     super2.sub2     0   0   0
  root #
  ```

  This output shows that the 90 CPU bound processes, which otherwise unconstrained would take up 100% of the CPU (almost four times over if it were possible), use just 25% because they are limited to run on CPUs 0 to 5.
- Use the SMIT **rset** menus to verify what resource set a process (identified by its PID) has access to. In our case, find one of our loop processes. For example:

  ```
       UID   PID  PPID   C    STIME    TTY  TIME CMD
     wlmu3 11234     1  95 15:11:45      0  3:28 loop
     ...     ...     ...     ...
  ```

Go to the **Show a Process Partition** entry of the **rset** SMIT menu. Enter the PID of the process we are interested in (or select it from the list of processes displayed with F4 key) and press Enter. For example:

```
                                 COMMAND STATUS
Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.
CPU  Memory  Resources
  6   98298  sys/mem.00000 sys/cpu.00005 sys/cpu.00004 sys/cpu.00003
             sys/cpu.00002 sys/cpu.00001 sys/cpu.00000
```

Selecting a process from a class without a specified **rset** attribute (here the **init** process) shows the following default resource set:

```
CPU  Memory  Resources
 24   98298  sys/sys0
```

Using **rsets** is an effective way to isolate workloads from one another as far as the CPU is concerned. By separating two different workloads into two classes and giving each class a different subset of the CPUs, you can make sure that the two workloads will never compete for CPU with one another. Of course, they still compete for physical memory and I/Os.

Chapter 13. System Resource Controller and Subsystems

This chapter contains procedures for starting and stopping, tracing, and obtaining status of the System Resource Controller (SRC) subsystems.

Topics covered this chapter are:

Starting the System Resource Controller

The System Resource Controller (SRC) is started during system initialization with a record for the **/usr/sbin/srcmstr** daemon in the **/etc/inittab** file. The default **/etc/inittab** file already contains such a record, so this procedure might be unnecessary. You can also start the SRC from the command line, a profile, or a shell script, but there are several reasons for starting it during initialization:

- Starting the SRC from the **/etc/inittab** file allows the **init** command to restart the SRC if it stops for any reason.
- The SRC is designed to simplify and reduce the amount of operator intervention required to control subsystems. Starting the SRC from any source other than the **/etc/inittab** file is counterproductive to that goal.
- The default **/etc/inittab** file contains a record for starting the print scheduling subsystem (**qdaemon**) with the **startsrc** command. Typical installations have other subsystems started with **startsrc** commands in the **/etc/inittab** file as well. Because the **srcmstr** command requires the SRC be running, removing the **srcmstr** daemon from the **/etc/inittab** file causes these **startsrc** commands to fail.

See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- Reading and writing the **/etc/inittab** file requires root user authority.
- The **mkitab** command requires root user authority.
- The **srcmstr** daemon record must exist in the **/etc/inittab** file.

Procedure

Note: This procedure is necessary only if the **/etc/inittab** file does not already contain a record for the **srcmstr** daemon.

1. Make a record for the **srcmstr** daemon in the **/etc/inittab** file using the **mkitab** command. For example, to make a record identical to the one that appears in the default **/etc/inittab** file, type:

   ```
   mkitab -i fbcheck srcmstr:2:respawn:/usr/sbin/srcmstr
   ```

   The **-i fbcheck** flag ensures that the record is inserted before all subsystems records.
2. Tell the **init** command to reprocess the **/etc/inittab** file by typing:

   ```
   telinit q
   ```

   When **init** revisits the **/etc/inittab** file, it processes the newly entered record for the **srcmstr** daemon and starts the SRC.

Starting or Stopping a Subsystem, Subsystem Group, or Subserver

Use the **startsrc** command to start a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver. The **startsrc** command can be used:

- From the **/etc/inittab** file so the resource is started during system initialization
- From the command line
- With SMIT.

When you start a subsystem group, all of its subsystems are also started. When you start a subsystem, all of its subservers are also started. When you start a subserver, its parent subsystem is also started if it is not already running.

Use the **stopsrc** command to stop an SRC resource such as a subsystem, a group of subsystems, or a subserver. When you stop a subsystem, all its subservers are also stopped. However, when you stop a subserver, the state of its parent subsystem is not changed.

Both the **startsrc** and **stopsrc** commands contain flags that allow requests to be made on local or remote hosts.See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- To start or stop an SRC resource, the SRC must be running. The SRC is normally started during system initialization. The default **/etc/inittab** file, which determines what processes are started during initialization, contains a record for the **srcmstr** daemon (the SRC). To see if the SRC is running, type **ps -A** and look for a process named **srcmstr**.
- The user or process starting an SRC resource must have root user authority. The process that initializes the system (**init** command) has root user authority.
- The user or process stopping an SRC resource must have root user authority.

Starting/Stopping a Subsystem Tasks		
Task	*SMIT Fast Path*	*Command or File*
Start a Subsystem	**smit startssys**	**/bin/startsrc -s** *SubsystemName* OR edit **/etc/inittab**
Stop a Subsystem	**smit stopssys**	**/bin/stopsrc -s** *SubsystemName*

Displaying the Status of a Subsystem or Subsystems

Use the **lssrc** command to display the status of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

All subsystems can return a short status report that includes which group the subsystem belongs to, whether the subsystem is active, and what its process ID (PID) is. If a subsystem does not use the signals communication method, it can be programmed to return a long status report containing additional status information.

The **lssrc** command provides flags and parameters for specifying the subsystem by name or PID, for listing all subsystems, for requesting a short or long status report, and for requesting the status of SRC resources either locally or on remote hosts.

See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Displaying the Status of Subsystems Tasks		
Task	*SMIT Fast Path*	*Command or File*
Display the status of a subsystem (long format)	**smit qssys**	**lssrc -l -s** *SubsystemName*
Display the status of all subsystems	**smit lsssys**	**lssrc -a**
Display the status of all subsystems on a particular host		**lssrc -h***HostName* **-a**

Refreshing a Subsystem or Subsystem Group

Use the **refresh** command to tell a System Resource Controller (SRC) resource such as a subsystem or a group of subsystems to refresh itself.

The **refresh** command provides flags and parameters for specifying the subsystem by name or PID. You can also use it to request a subsystem or group of subsystems be refreshed, either locally or on remote hosts. See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- The SRC must be running. See "Starting the System Resource Controller" on page 119 for details.
- The resource you want to refresh must not use the signals communications method.
- The resource you want to refresh must be programmed to respond to the refresh request.

Refreshing a Subsystem or Subsystem Group		
Task	**SMIT Fast Path**	**Command or File**
Refresh a Subsystem	**smit refresh**	**refresh -s Subsystem**

Turning On or Off Subsystem, Subsystem Group, or Subserver Tracing

Use the **traceson** command to turn on tracing of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

Use the **tracesoff** command to turn off tracing of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

The **traceson** and **traceoff** commands can be used to remotely turn on or turn off tracing on a specific host. See the **srcmstr** command for the configuration requirements for supporting remote SRC requests.

Prerequisites

- To turn the tracing of an SRC resource either on or off , the SRC must be running. See "Starting the System Resource Controller" on page 119 for details.
- The resource you want to trace must not use the signals communications method.
- The resource you want to trace must be programmed to respond to the trace request.

Turning On/Off Subsystem, Subsystem Group, or Subserver Tasks		
Task	*SMIT Fast Path*	*Command or File*
Turn on Subsystem Tracing (short format)	**smit tracessyson**	**traceson -s Subsystem**

Turning On/Off Subsystem, Subsystem Group, or Subserver Tasks		
Turn on Subsystem Tracing (long format)	**smit tracessyson**	**traceson -l -s Subsystem**
Turn off Subsystem Tracing	**smit tracessysoff**	**tracesoff -s Subsystem**

Chapter 14. System Accounting

The system accounting utility allows you to collect and report on individual and group use of various system resources.

Topics covered in this chapter are:

Setting Up an Accounting System

Prerequisites

You must have root authority to complete this procedure.

Procedure

The following is an overview of the steps you must take to set up an accounting system. Refer to the commands and files noted in these steps for more specific information.

1. Use the **nulladm** command to ensure that each file has the correct access permission: read (r) and write (w) permission for the file owner and group and read (r) permission for others by typing:

   ```
   /usr/sbin/acct/nulladm wtmp pacct
   ```

   This provides access to the **pacct** and **wtmp** files.
2. Update the **/etc/acct/holidays** file to include the hours you designate as prime time and to reflect your holiday schedule for the year.

   > **Note:** Comment lines can appear anywhere in the file as long as the first character in the line is an asterisk (*).

   a. To define prime time, fill in the fields on the first data line (the first line that is not a comment), using a 24-hour clock. This line consists of three 4-digit fields, in the following order:
      - Current year
      - Beginning of prime time (*hhmm*)
      - End of prime time (*hhmm*)

Leading blanks are ignored. You can enter midnight as either 0000 or 2400.

For example, to specify the year 2000, with prime time beginning at 8:00 a.m. and ending at 5:00 p.m., enter:

```
2000  0800  1700
```

b. To define the company holidays for the year on the next data line. Each line contains four fields, in the following order:
   - Day of the year
   - Month
   - Day of the month
   - Description of holiday

   The day-of-the-year field contains the number of the day on which the holiday falls and must be a number from 1 through 365 (366 on leap year). For example, February 1st is day 32. The other three fields are for information only and are treated as comments.

   A two-line example follows:

```
  1  Jan  1  New Year's Day
332  Nov 28  Thanksgiving Day
```

3. Turn on process accounting by adding the following line to the **/etc/rc** file or by deleting the comment symbol (#) in front of the line if it exists:

```
/usr/bin/su - adm -c /usr/sbin/acct/startup
```

   The **startup** procedure records the time that accounting was turned on and cleans up the previous day's accounting files.
4. Identify each file system you want included in disk accounting by adding the following line to the stanza for the file system in the **/etc/filesystems** file:

```
account = true
```

5. Specify the data file to use for printer data by adding the following line to the queue stanza in the **/etc/qconfig** file:

```
acctfile = /var/adm/qacct
```

6. As the adm user, create a **/var/adm/acct/nite**, a **/var/adm/acct/fiscal**, a and **/var/adm/acct/sum** directory to collect daily and fiscal period records:

```
su - adm
cd /var/adm/acct
mkdir nite fiscal sum
exit
```

7. Set daily accounting procedures to run automatically by editing the **/var/spool/cron/crontabs/root** file to include the **dodisk**, **ckpacct**, and **runacct** commands. For example:

```
0 2 * * 4 /usr/sbin/acct/dodisk
5 * * * * /usr/sbin/acct/ckpacct
0 4 * * 1-6 /usr/sbin/acct/runacct
              2>/var/adm/acct/nite/accterr
```

   The first line starts disk accounting at 2:00 a.m. (`0 2`) each Thursday (4). The second line starts a check of the integrity of the active data files at 5 minutes past each hour (`5 *`) every day (`*`). The third line runs most accounting procedures and processes active data files at 4:00 a.m. (`0 4`) every Monday through Saturday (`1-6`). If these times do not fit the hours your system operates, adjust your entries.

   Note: You must have root user authority to edit the **/var/spool/cron/crontabs/root** file.
8. Set the monthly accounting summary to run automatically by including the **monacct** command in the **/var/spool/cron/crontabs/root** file. For example, type:

```
15 5 1 * * /usr/sbin/acct/monacct
```

Be sure to schedule this procedure early enough to finish the report. This example starts the procedure at 5:15 a.m. on the first day of each month.

9. To submit the edited **cron** file, type:

```
crontab /var/spool/cron/crontabs/root
```

Generating System Accounting Reports

Once accounting has been configured on the system, daily and monthly reports are generated. The **runacct** command produces the daily reports and the **monact** command produces the monthly reports.

Daily Accounting Reports

To generate a daily report, use the **runacct** command. This command summarizes data into an ASCII file named **/var/adm/acct/sum/rprtMMDD**. **MMDD** specifies the month and day the report is run. The report covers the following:

- Daily Report
- Daily Usage Report
- Daily Command Summary
- Monthly Total Command Summary
- Last Login

Daily Report

The first line of the Daily Report begins with the start and finish times for the data collected in the report, a list of system-level events including any existing shutdowns, reboots, and run-level changes. The total duration is also listed indicating the total number of minutes included within the accounting period (usually 1440 minutes, if the report is run every 24 hours). The report contains the following information:

LINE	Console, tty, or pty In use
MINUTES	Total number of minutes the line was in use
PERCENT	Percentage of time in the accounting period that the line was in use
# SESS	Number of new login sessions started
# ON	Same as **# SESS**
# OFF	Number of logouts plus interrupts made on the line

Daily Usage Report

The Daily Usage Report is a summarized report of system usage per user ID during the accounting period. Some fields are divided into prime and non-prime time, as defined by the accounting administrator in the **/usr/lib/acct/holidays** directory. The report contains the following information:

UID	User ID
LOGIN NAME	User name
CPU (PRIME/NPRIME)	Total CPU time for all of the user's processes in minutes
KCORE (PRIME/NPRIME)	Total memory used by running processes, in kilobyte-minutes
CONNECT (PRIME/NPRIME)	Total connect time (how long the user was logged in) in minutes
DISK BLOCKS	Average total amount of disk space used by the user on all filesystems for which accounting is enabled
FEES	Total fees entered with **chargefee** command
# OF PROCS	Total number of processes belonging to this user
# OF SESS	Number of distinct login sessions for this user
# DISK SAMPLES	Number of times disk samples were run during the accounting period. If no DISK BLOCKS are owned the value will be zero

Daily Command Summary

The Daily Command Summary report shows each command executed during the accounting period, with one line per each unique command name. The table is sorted by TOTAL KCOREMIN (described below), with the first line including the total information for all commands. The data listed for each command is cumulative for all executions of the command during the accounting period. The columns in this table include the following information:

COMMAND NAME	Command that was executed
NUMBER CMDS	Number of times the command executed
TOTAL KCOREMIN	Total memory used by running the command, in kilobyte-minutes
TOTAL CPU-MIN	Total CPU time used by the command in minutes
TOTAL REAL-MIN	Total real time elapsed for the command in minutes
MEAN SIZE-K	Mean size of memory used by the command per CPU minute
MEAN CPU-MIN	Mean numbr of CPU minutes per execution of the command
HOG FACTOR	Measurement of how much the command hogs the CPU while it is active. It is the ratio of **TOTAL CPU-MIN** over **TOTAL REAL-MIN**
CHARS TRNSFD	Number of characters transferred by the command with system reads and writes
BLOCKS READ	Number of physical block reads and writes performed by the command

Monthly Total Command Summary

The Monthly Total Command Summary , created by the **monacct** command, provides information about all commands executed since the previous monthly report. The fields and information mean the same as those in the Daily Command Summary.

Last Login

The Last Login report displays two fields for each user ID. The first field is YY-MM-DD and indicates the most recent login for the specified user. The second field is the name of the user account. A date field of 00-00-00 indicates that the user ID has never logged in.

Fiscal Accounting Reports

The Fiscal Accounting Reports generally collected monthly by using the **monacct** command. The report is stored in **/var/adm/acct/fiscal/fiscrptMM** where **MM** is the month that the **monacct** command was executed. This report includes information similar to the daily reports summarized for the entire month.

Generating Reports on System Activity

To generate a report on system activity, use the **prtacct** command. This command reads the information in a total accounting file (**tacct** file format) and produces formatted output. Total accounting files include the daily reports on connect time, process time, disk usage, and printer usage.

Prerequisites

The **prtacct** command requires an input file in the **tacct** file format. This implies that you have an accounting system set up and running or that you have run the accounting system in the past. See “Setting Up an Accounting System” on page 123 for guidelines.

Procedure

Generate a report on system activity by entering:

```
prtacct -f Specification -v Heading File
```

`Specification` is a comma-separated list of field numbers or ranges used by the **acctmerg** command. The optional `-v` flag produces verbose output where floating-point numbers are displayed in higher precision notation. *Heading* is the title you want to appear on the report and is optional. *File* is the full path name of the total accounting file to use for input. You can specify more than one file.

Summarizing Accounting Records

To summarize raw accounting data, use the **sa** command. This command reads the raw accounting data, usually collected in the **/var/adm/pacct** file, and the current usage summary data in the **/var/adm/savacct** file, if summary data exists. It combines this information into a new usage summary report and purges the raw data file to make room for further data collection.

Prerequisites

The **sa** command requires an input file of raw accounting data such as the **pacct** file (process accounting file). To collect raw accounting data, you must have an accounting system set up and running. See "Setting Up an Accounting System" on page 123 for guidelines

Procedure

The purpose of the **sa** command is to summarize process accounting information and to display or store that information. The simplest use of the command displays a list of statistics about every process that has run during the life of the **pacct** file being read. To produce such a list, type:

```
/usr/sbin/sa
```

To summarize the accounting information and merge it into the summary file, type:

```
/usr/sbin/sa -s
```

The **sa** command offers many additional flags that specify how the accounting information is processed and displayed. See the **sa** command description for more information.

Starting the runacct Command

Prerequisites

1. You must have the accounting system installed.
2. You must have root user or adm group authority.

Notes:

1. If you call the **runacct** command with no parameters, the command assumes that this is the first time that the command has been run today. Therefore, you need to include the *mmdd* parameter when you restart the **runacct** program, so that the month and day are correct. If you do not specify a state, the **runacct** program reads the **/var/adm/acct/nite/statefile** file to determine the entry point for processing. To override the **/var/adm/acct/nite/statefile** file, specify the desired state on the command line.
2. When you perform the following task, you might need to use the full path name **/usr/sbin/acct/runacct** rather than the simple command name, **runacct**.

Procedure

To start the **runacct** command, type the following:

```
nohup runacct 2> \
/var/adm/acct/nite/accterr &
```

This entry causes the command to ignore all **INTR** and **QUIT** signals while it performs background processing. It redirects all standard error output to the **/var/adm/acct/nite/accterr** file.

Restarting the runacct Command

Prerequisites

1. You must have the accounting system installed.
2. You must have root user or adm group authority.

> **Note:** The most common reason why the **runacct** command can fail are because:
> - The system goes down
> - The **/usr** file system runs out of space
> - The **/var/adm/wtmp** file has records with inconsistent date stamps.

Procedure

If the **runacct** command is unsuccessful, do the following:

1. Check the **/var/adm/acct/nite/active** *mmdd* file for error messages.
2. If both the active file and lock files exist in **acct/nite**, check the **accterr** file, where error messages are redirected when the **cron** daemon calls the **runacct** command.
3. Perform any actions needed to eliminate errors.
4. Restart the **runacct** command.
5. To restart the **runacct** command for a specific date, type the following:

   ```
   nohup runacct 0601 2>> \
   /var/adm/acct/nite/accterr &
   ```

   This restarts the **runacct** program for June 1 (`0601`). The **runacct** program reads the **/var/adm/acct/nite/statefile** file to find out with which state to begin. All standard error output is appended to the **/var/adm/acct/nite/accterr** file.
6. To restart the **runacct** program at a specified state, for example, the MERGE state, type the following:

   ```
   nohup runacct 0601 MERGE 2>> \
   /var/adm/acct/nite/accterr &
   ```

Showing System Activity

You can display formatted information about system activity with the **sar** command.

Prerequisites

To display system activity statistics, the **sadc** command must be running.

> **Note:** The typical method of running the **sadc** command is to place an entry for the **sa1** command in the root **crontab** file. The **sa1** command is a shell-procedure variant of the **sadc** command designed to work with the **cron** daemon.

Procedure

To display basic system-activity information, type:

```
sar 2 6
```

where the first number is the number of seconds between sampling intervals and the second number is the number of intervals to display. The output of this command looks something like this:

```
    arthurd 2 3 000166021000    05/28/92

14:03:40    %usr    %sys    %wio   %idle
14:03:42       4       9       0      88
14:03:43       1      10       0      89
```

```
14:03:44       1      11       0      88
14:03:45       1      11       0      88
14:03:46       3       9       0      88
14:03:47       2      10       0      88

Average        2      10       0      88
```

The **sar** command also offers a number of flags for displaying an extensive array of system statistics. To see all available statistics, use the **-A** flag. For a list of the available statistics and the flags for displaying them, see the **sar** command.

> **Note:** To have a daily system activity report written to **/var/adm/sa/sa***dd*, include an entry in the root **crontab** file for the **sa2** command. The **sa2** command is a shell procedure variant for the **sar** command designed to work with the **cron** daemon.

Showing System Activity While Running a Command

You can use the **time** and **timex** commands to display formatted information about system activity while a particular command is running.

Prerequisites

The **-o** and **-p** flags of the **timex** command require that system accounting be turned on.

Procedure

- To display the elapsed time, user time, and system execution time for a particular command, type:

  ```
  time CommandName
  ```

  OR

  ```
  timex CommandName
  ```
- To display the total system activity (all the data items reported by the **sar** command) during the execution of a particular command, type:

  ```
  timex -s CommandName
  ```

The **timex** command has two additional flags. The **-o** flag reports the total number of blocks read or written by the command and all of its children. The **-p** flag lists all of the process accounting records for a command and all of its children.

Showing Process Time

You can display formatted reports about the process time of active processes with the **ps** command or of finished processes with the **acctcom** command.

Prerequisites

The **acctcom** command reads input in the total accounting record form (**acct** file format). This implies that you have process accounting turned on or that you have run process accounting in the past. See “Setting Up an Accounting System” on page 123 for guidelines.

Display the Process Time of Active Processes

The **ps** command offers a number of flags to tailor the information displayed. To produce a full list of all active processes except kernel processes, type:

```
ps -ef
```

Another useful variation displays a list of all processes associated with terminals. Type:

```
ps -al
```

Both of these usages display a number of columns for each process, including the current CPU time for the process in minutes and seconds.

Display the Process Time of Finished Processes

The process accounting functions are turned on with the **startup** command, which is typically started at system initialization with a call in the **/etc/rc** file. When the process accounting functions are running, a record is written to **/var/adm/pacct** (a total accounting record file) for every finished process that includes the start and stop time for the process. You can display the process time information from a **pacct** file with the **acctcom** command. This command has a number of flags that allow flexibility in specifying which processes to display.

For example, to see all processes that ran for a minimum number of CPU seconds or longer, use the **-O** flag, type:

```
acctcom -O 2
```

This displays records for every process that ran for at least 2 seconds. If you do not specify an input file, the **acctcom** command reads input from the **/var/adm/pacct** directory.

Showing CPU Usage

You can display formatted reports about the CPU usage by process or by user with a combination of the **acctprc1**, **acctprc2**, and **prtacct** commands.

Prerequisites

The **acctprc1** command requires input in the total accounting record form (**acct** file format). This implies that you have process accounting turned on or that you have run process accounting in the past. See “Setting Up an Accounting System” on page 123 for guidelines.

Show CPU Usage for Each Process

To produce a formatted report of CPU usage by process, type:

```
acctprc1 </var/adm/pacct
```

This information will be useful in some situations, but you might also want to summarize the CPU usage by user. The output from this command is used in the next procedure to produce that summary.

Show CPU Usage for Each User

1. Produce an output file of CPU usage by process by typing:

   ```
   acctprc1 </var/adm/pacct >out.file
   ```

   The **/var/adm/pacct** file is the default output for process accounting records. You might want to specify an archive **pacct** file instead.
2. Produce a binary total accounting record file from the output of the previous step by typing:

   ```
   acctprc2 <out.file >/var/adm/acct/nite/daytacct
   ```

   Note: The **daytacct** file is merged with other total accounting records by the **acctmerg** command to produce the daily summary record, **/var/adm/acct/sum/tacct**.
3. Display a formatted report of CPU usage summarized by user by typing:

   ```
   prtacct </var/adm/acct/nite/daytacct
   ```

Showing Connect Time Usage

You can display the connect time of all users, of individual users, and by individual login with the **ac** command.

Prerequisites

The **ac** command extracts login information from the **/var/adm/wtmp** file, so this file must exist. If the file has not been created, the following error message is returned:

```
No /var/adm/wtmp
```

If the file becomes too full, additional **wtmp** files are created; you can display connect-time information from these files by specifying them with the **-w** flag.

Procedure

- To display the total connect time for all users, type:

  ```
  /usr/sbin/acct/ac
  ```

  This command displays a single decimal number that is the sum total connect time, in minutes, for all users who have logged in during the life of the current **wtmp** file.
- To display the total connect time for one or more particular users, type:

  ```
  /usr/sbin/acct/ac User1 User2 ...
  ```

  This command displays a single decimal number that is the sum total connect time, in minutes, for the user or users you specified for any logins during the life of the current **wtmp** file.
- To display the connect time by individual user plus the total connect time, type:

  ```
  /usr/sbin/acct/ac -p User1 User2 ...
  ```

  This command displays as a decimal number for each user specified equal to the total connect time, in minutes, for that user during the life of the current **wtmp** file. It also displays a decimal number that is the sum total connect time for all the users specified. If no user is specified in the command, the list includes all users who have logged in during the life of the **wtmp** file.

Showing Disk Space Utilization

You can display disk space utilization information with the **acctmerg** command.

Prerequisites

To display disk space utilization information, the **acctmerg** command requires input from a **dacct** file (disk accounting). The collection of disk-usage accounting records is performed by the **dodisk** command. Placing an entry for the **dodisk** command in a **crontabs** file is part of the procedure described in “Setting Up an Accounting System” on page 123 .

Procedure

To display disk space utilization information, type:

```
acctmerg -a1 -2,13 -h </var/adm/acct/nite/dacct
```

This command displays disk accounting records, which include the number of 1 KB blocks utilized by each user.

Note: The **acctmerg** command always reads from standard input and can read up to nine additional files. If you are not piping input to the command, you must redirect input from one file; the rest of the files can be specified without redirection.

Showing Printer Usage

You can display printer or plotter usage accounting records with the **pac** command.

Prerequisites

- To collect printer usage information, you must have an accounting system set up and running. See "Setting Up an Accounting System" on page 123 for guidelines.
- The printer or plotter for which you want accounting records must have an `acctfile=` clause in the printer stanza of the **/etc/qconfig** file. The file specified in the `acctfile=` clause must grant read and write permissions to the root user or printq group.
- If the **-s** flag of the **pac** command is specified, the command rewrites the summary file name by appending **_sum** to the path name specified by the `acctfile=` clause in the **/etc/qconfig** file. This file must exist and grant read and write permissions to the root user or printq group.

Procedure

- To display printer usage information for all users of a particular printer, type:

  ```
  /usr/sbin/pac -PPrinter
  ```

  If you do not specify a printer, the default printer is named by the **PRINTER** environment variable. If the **PRINTER** variable is not defined, the default is **lp0**.
- To display printer usage information for particular users of a particular printer, type:

  ```
  /usr/sbin/pac -PPrinter User1 User2 ...
  ```

The **pac** command offers other flags for controlling what information gets displayed.

Fixing tacct Errors

If you are using the accounting system to charge user for system resources, the integrity of the **/var/adm/acct/sum/tacct** file is quite important. Occasionally, mysterious **tacct** records appear that contain negative numbers, duplicate user numbers, or a user number of 65,535.

Prerequisites

You must have root user or adm group authority.

Patch a tacct File

1. Move to the **/var/adm/acct/sum** directory by typing:

   ```
   cd /var/adm/acct/sum
   ```
2. Use the **prtacct** command to check the total accounting file, **tacctprev**, by typing:

   ```
   prtacct tacctprev
   ```

   The **prtacct** command formats and displays the **tacctprev** file so that you can check connect time, process time, disk usage, and printer usage.
3. If the **tacctprev** file looks correct, change the latest **tacct .***mmdd* file from a binary file to an ASCII file. In the following example, the **acctmerg** command converts the **tacct.***mmdd* file to an ASCII file named `tacct.new`:

   ```
   acctmerg -v < tacct.mmdd > tacct.new
   ```

> **Note:** The **acctmerg** command with the **-a** flag also produces ASCII output. The **-v** flag produces more precise notation for floating-point numbers.

The **acctmerg** command is used to merge the intermediate accounting record reports into a cumulative total report (**tacct**). This cumulative total is the source from which the **monacct** command produces the ASCII monthly summary report. Since the **monacct** command procedure removes all the **tacct.***mmdd* files, you recreate the **tacct** file by merging these files.

4. Edit the **tacct.new** file to remove the bad records and write duplicate user number records to another file by typing:

   ```
   acctmerg -i < tacct.new > tacct.mmdd
   ```
5. Create the **tacct** file again by typing:

   ```
   acctmerg tacctprev < tacct.mmdd > tacct
   ```

Fixing wtmp Errors

The **/var/adm/wtmp**, or ″who temp″ file, might cause problems in the day-to-day operation of the accounting system. When the date is changed and the system is in multiuser mode, date change records are written to the **/var/adm/wtmp** file. When a date change is encountered, the **wtmpfix** command adjusts the time stamps in the **wtmp** records. Some combinations of date changes and system restarts may slip past the **wtmpfix** command and cause the **acctcon1** command to fail and the **runacct** command to send mail to the **root** and **adm** accounts listing incorrect dates.

Prerequisites

You must have root user or adm group authority.

Procedure

1. Move to the **/var/adm/acct/nite** directory by typing:

   ```
   cd /var/adm/acct/nite
   ```
2. Convert the binary **wtmp** file to an ASCII file that you can edit by typing:

   ```
   fwtmp < wtmp.mmdd > wtmp.new
   ```

   The **fwtmp** command converts **wtmp** from binary to ASCII.
3. Edit the ASCII **wtmp.new** file to delete damaged records or all records from the beginning of the file up to the needed date change by typing:

   ```
   vi wtmp.new
   ```
4. Convert the ASCII **wtmp.new** file back to binary format by typing:

   ```
   fwtmp -ic < wtmp.new > wtmp.mmdd
   ```
5. If the **wtmp** file is beyond repair, use the **nulladm** command to create an empty **wtmp** file. This prevents any charges in the connect time.

   ```
   nulladm wtmp
   ```

   The **nulladm** command creates the file specified with read and write permissions for the file owner and group, and read permissions for other users. It ensures that the file owner and group are **adm**.

Fixing General Accounting Problems

You might encounter several different problems when using the accounting system. You might need to resolve file ownership and permissions problems.

This section describes how to fix general accounting problems:

- “Fixing Incorrect File Permissions” on page 134

- “Fixing Errors”
- “Fixing Errors Encountered When Running the runacct Command” on page 135
- “Updating an Out-of-Date Holidays File” on page 137

Prerequisites

You must have root user or adm group authority.

Fixing Incorrect File Permissions

To use the accounting system, file ownership and permissions must be correct. The **adm** administrative account owns the accounting command and scripts, except for **/var/adm/acct/accton** which is owned by root.

1. To check file permissions using the **ls** command, type:

   ```
   ls -l /var/adm/acct

   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/fiscal
   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/nite
   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/sum
   ```

2. Adjust file permissions with the **chown** command, if necessary. The permissions are 755 (all permissions for owner and read and execute permissions for all others). Also, the directory itself should be write-protected from others. For example:

   a. Move to the **/var/adm/acct** directory by typing:

      ```
      cd /var/adm/acct
      ```

   b. Change the ownership for the **sum**, **nite**, and **fiscal** directories to **adm** group authority by typing:

      ```
      chown adm sum/* nite/* fiscal/*
      ```

      To prevent tampering by users trying to avoid charges, deny write permission for others on these files. Change the **accton** command group owner to **adm**, and permissions to 710, that is, no permissions for others. Processes owned by **adm** can execute the **accton** command, but ordinary users can not.

3. The **/var/adm/wtmp** file must also be owned by **adm**. If **/var/adm/wtmp** is owned by root, you will see the following message during startup:

   ```
   /var/adm/acct/startup: /var/adm/wtmp: Permission denied
   ```

   To correct the ownership of **/var/adm/wtmp**, change ownership to the **adm** group by typing the following command:

   ```
   chown adm /var/adm/wtmp
   ```

Fixing Errors

Processing the **/var/adm/wtmp** file night produce some warnings mailed to root. The **wtmp** file contains information collected by **/etc/init** and **/bin/login** and is used by accounting scripts primarily for calculating connect time (the length of time a user is logged in). Unfortunately, date changes confuse the program that processes the **wtmp** file. As a result, the **runacct** command sends mail to root and adm complaining of any errors after a date change since the last time accounting was run.

1. Determine if you received any errors.

   The **acctcon1** command outputs error messages that are mailed to adm and root by the **runacct** command. For example, if the **acctcon1** command stumbles after a date change and fails to collect connect times, adm might get mail like the following mail message:

   ```
   Mon Jan 6 11:58:40 CST 1992
   acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
   new: Mon Jan 6 11:57:59 1992
   ```

```
acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
new: Mon Jan 6 11:57:59 1992
acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
new: Mon Jan 6 11:57:59 1992
```

2. Adjust the **wtmp** file by typing:

   ```
   /usr/sbin/acct/wtmpfix wtmp
   ```

   The **wtmpfix** command examines the **wtmp** file for date and time-stamp inconsistencies and corrects problems that could make **acctcon1** fail. However, some date changes slip by **wtmpfix**. See "Fixing wtmp Errors" on page 133.
3. Run accounting right before shutdown or immediately after startup.

   Using the **runacct** command at these times minimizes the number of entries with bad times. The **runacct** command continues to send mail to the root and adm accounts, until you edit the **runacct** script, find the `WTMPFIX` section, and comment out the line where the file log gets mailed to the **root** and **adm** accounts.

Fixing Errors Encountered When Running the runacct Command

The **runacct** command processes files that are often very large. The procedure involves several passes through certain files and consumes considerable system resources while it is taking place. That is why the **runacct** command is normally run early in the morning when it can take over the machine and not disturb anyone.

The **runacct** command is a scrip divided into different stages. The stages allow you to restart the command where it stopped, without having to rerun the entire script.

When the **runacct** encounters problems, it sends error messages to different destinations depending on where the error occurred. Usually it sends a date and a message to the console directing you to look in the **active***MMDD* file (such as **active0621** for June 21st) which is in the **/usr/adm/acct/nite** directory. When the **runacct** command aborts, it moves the entire **active** file to **active***MMDD* and appends a message describing the problem.

1. Review the following error message tables for errors you have encountered when running the **runacct** command.

   Notes:

   1. The abbreviation *MMDD* stands for the month and day, such as 0102 for January 2. For example, a fatal error during the CONNECT1 process on January 2 creates the file **active0102** containing the error message.
   2. The abbreviation ″SE message″ stands for the standard error message such as:

      ```
      ********* ACCT ERRORS : see active0102 *********
      ```

Preliminary State and Error Messages from the runnacct Command

State	Command	Fatal?	Error Message	Destinations
pre	**runacct**	yes	`* 2 CRONS or ACCT PROBLEMS * ERROR: locks found, run aborted`	console, mail, active
pre	**runacct**	yes	`runacct: Insufficient space in /usr (` *nnn* blks); Terminating procedure	console, mail, active

pre	**runacct**	yes	SE message; ERROR: acctg already run for 'date': check lastdate	console, mail, active*MMDD*
pre	**runacct**	no	* SYSTEM ACCOUNTING STARTED *	console
pre	**runacct**	no	restarting acctg for 'date' at STATE	console active, console
pre	**runacct**	no	restarting acctg for 'date' at state (argument $2) previous state was STATE	active
pre	**runacct**	yes	SE message; Error: runacct called with invalid arguments	console, mail, active*MMDD*

States and Error Messages from the runacct Command				
State	**Command**	**Fatal?**	**Error Message**	**Destinations**
SETUP	**runacct**	no	ls -l fee pacct* /var/adm/wtmp	active
SETUP	**runacct**	yes	SE message; ERROR: turnacct switch returned rc=error	console, mail, active*MMDD*
SETUP	**runacct**	yes	SE message; ERROR: SpacctMMDD already exists file setups probably already run	active*MMDD*
SETUP	**runacct**	yes	SE message; ERROR: wtmpMMDD already exists: run setup manually	console, mail, active*MMDD*
WTMPFIX	**wtmpfix**	no	SE message; ERROR: wtmpfix errors see xtmperrorMMDD	active*MMDD*, wtmperror*MMDD*
WTMPFIX	**wtmpfix**	no	wtmp processing complete	active
CONNECT1	**acctcon1**	no	SE message; (errors from acctcon1 log)	console, mail, active*MMDD*
CONNECT2	**acctcon2**	no	connect acctg complete	active
PROCESS	**runacct**	no	WARNING: accounting already run for pacct*N*	active
PROCESS	**acctprc1 acctprc2**	no	process acctg complete for SpacctNMMDD	active
PROCESS	**runacct**	no	all process actg complete for date	active
MERGE	**acctmerg**	no	tacct merge to create dayacct complete	active

FEES	**acctmerg**	no	`merged fees OR no fees`	active
DISK	**acctmerg**	no	`merged disk records OR no disk records`	active
MERGEACCT	**acctmerg**	no	`WARNING: recreating sum/tacct`	active
MERGEACCT	**acctmerg**	no	`updated sum/tacct`	active
CMS	**runacct**	no	`WARNING: recreating sum/cms`	active
CMS	**acctcms**	no	`command summaries complete`	active
CLEANUP	**runacct**	no	`system accounting completed at 'date'`	active
CLEANUP	**runacct**	no	`*SYSTEM ACCOUNTING COMPLETED*`	console
<wrong>	**runacct**	yes	`SE message; ERROR: invalid state, check STATE`	console, mail, active*MMDD*

Note: The label `<wrong>` in the previous table does not represent a state, but rather a state other than the correct state that was written in the state file **/usr/adm/acct/nite/statefile**.

Summary of Message Destinations	
Destination	**Description**
console	The **/dev/console** device
mail	Message mailed to **root** and **adm** accounts
active	The **/usr/adm/acct/nite/active** file
activeMMDD	The **/usr/adm/acct/nite/active***MMDD* file
wtmperrMMDD	The **/usr/adm/acct/nite/wtmperror***MMDD* file
STATE	Current state in **/usr/adm/acct/nite/statefile** file
fd2log	Any other error messages

Updating an Out-of-Date Holidays File

The **acctcon1** command (started from the **runacct** command) sends mail to the **root** and **adm** accounts when the **/usr/lib/acct/holidays** file gets out of date. The holidays file is out of date after the last holiday listed has passed or the year has changed.

Update the out-of-date holidays file by editing the **/var/adm/acct/holidays** file to differentiate between prime and nonprime time.

Prime time is assumed to be the period when your system is most active, such as workdays. Saturdays and Sundays are always nonprime times for the accounting system, as are any holidays that you list.

The holidays file contains three types of entries: comments, the year and prime-time period, and a list of holidays as in the following example:

```
* Prime/Non-Prime Time Table for Accounting System
*
*   Curr       Prime            Non-Prime
*   Year       Start            Start
```

```
    1992       0830            1700
*
*   Day of     Calendar        Company
*   Year       Date            Holiday
*
*   1          Jan 1           New Year's Day
*   20         Jan 20          Martin Luther King Day
*   46         Feb 15          President's Day
*   143        May 28          Memorial Day
*   186        Jul 3           4th of July
*   248        Sep 7           Labor Day
*   329        Nov 24          Thanksgiving
*   330        Nov 25          Friday after
*   359        Dec 24          Christmas Eve
*   360        Dec 25          Christmas Day
*   361        Dec 26          Day after Christmas
```

The first noncomment line must specify the current year (as four digits) and the beginning and end of prime time, also as four digits each. The concept of prime and nonprime time only affects the way that the accounting programs process the accounting records.

If the list of holidays is too long, the **acctcon1** command generates an error, and you will need to shorten your list. You are safe with 20 or fewer holidays. If you want to add more holidays, just edit the holidays file each month.

Displaying Locking Activity

You can display system locking activity with the **locktrace** command.

Procedure

Show locking activity by typing:

```
locktrace 2 6
```

Where the first number specifies the number of seconds between sampling intervals, and the second number is the number of samples to display. If no parameters are given, a single report covering a one second period is displayed. The report output is similar to:

```
Subsys   Name                Ocn   Ref/s   %Ref   %Block   %Sleep
-----------------------------------------------------------------
PROC     PROC_LOCK_CLASS      2    1442    3.06    6.98     0.75
PROC     PROC_INT_CLASS       1    1408    2.98    5.86     1.77
IOS      IOS_LOCK_CLASS       4     679    1.44    5.19     2.29
```

The **locktrace** command can filter its output depending on a number of conditions. This allows you to limit the reports to the most active locks, or to those locks that are causing the most contention. Limiting the number of locks that are analyzed, reduces the system resources required to generate the locking reports.

Chapter 15. The Common Desktop Environment

With the Common Desktop Environment, you can access networked devices and tools without having to be aware of their location. You can exchange data across applications by simply dragging and dropping objects.

System administrators find many tasks that previously required complex command line syntax can now be done more easily and similarly from platform to platform. They can also maximize their investment in existing hardware and software by configuring centrally and distributing applications to users. They can centrally manage the security, availability, and interoperability of applications for the users they support.

> **Note:** The Common Desktop Environment (CDE) 1.0. Help volumes, web-based documentation, and hardcopy manuals might refer to the desktop as Common Desktop Environment, the AIXwindows desktop, the Common Desktop Environment, CDE 1.0, or simply, the desktop.

Topics covered in this chapter are:

- "Starting and Stopping the Common Desktop Environment"
- "Modifying Desktop Profiles" on page 140
- "Adding and Removing Displays and Terminals for Common Desktop Environment" on page 140
- "Customizing Display Devices for Common Desktop Environment" on page 142

Starting and Stopping the Common Desktop Environment

You can set up the system so that Common Desktop Environment comes up automatically when you start the system, or you can start Common Desktop Environment manually. You must log in as root to perform each of these tasks.

- "Enabling and Disabling Desktop Autostart"
- "Starting Common Desktop Environment Manually"
- "Stopping Common Desktop Environment Manually" on page 140

Enabling and Disabling Desktop Autostart

You may find it more convenient to set up your system to start Common Desktop Environment automatically when the system is turned on. You can do this through the Web-based System Manager (type `wsm`, then select `System`), through the System Management Interface Tool (SMIT), or from a command line.

Prerequisite

You must have root user authority to enable or disable desktop auto-start.

Starting/Stopping the Common Desktop Environment Automatically Tasks		
Task	*SMIT Fast Path*	*Command or File*
Enabling the Desktop Auto-Start [1]	**smit dtconfig**	**dtconfig -e**
Disabling the Desktop Auto-Start [1]	**smit dtconfig**	**dtconfig -d**

[1] **Note:** Restart the machine after completing this task.

Starting Common Desktop Environment Manually

You can start Common Desktop Environment manually.

Start the Desktop Login Manager Manually

1. Log in to your system as root.
2. At the command line, type:

   ```
   /usr/dt/bin/dtlogin -daemon
   ```

A **Desktop Login** screen is displayed. When you log in, you will start a desktop session.

Stopping Common Desktop Environment Manually

You can stop Common Desktop Environment manually.

Stop the Login Manager Manually

When you manually stop the login manager, all X-servers and desktop sessions that the login manager started are stopped.

1. Open a terminal emulator window and log in as root.
2. Obtain the process ID of the Login Manager by typing the following:

   ```
   cat /var/dt/Xpid
   ```

3. Stop the Login Manager by typing:

   ```
   kill -term process_id
   ```

Modifying Desktop Profiles

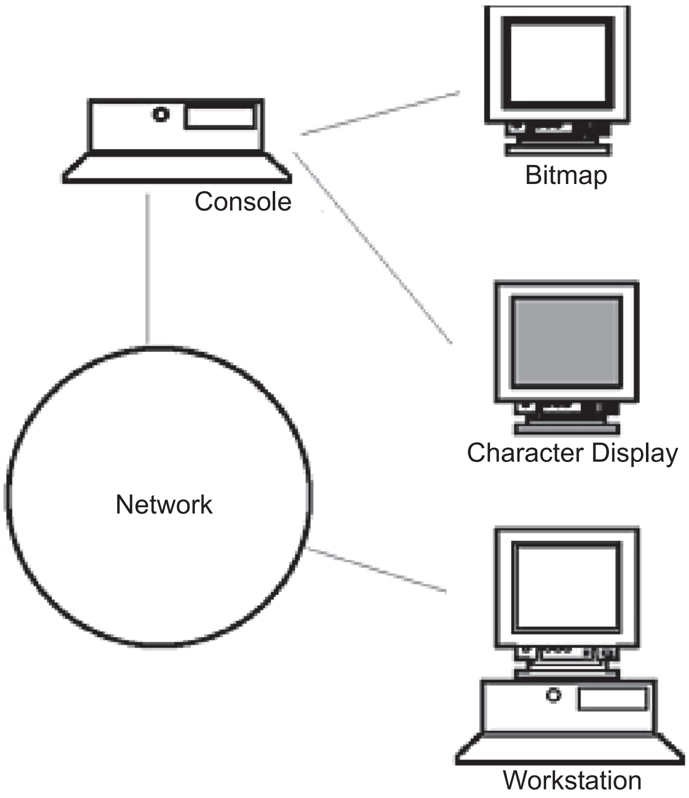
When a user logs in to the desktop, the shell environment file (**.profile** or **.login**) is not automatically read. The desktop runs the X-server before the user logs in, so the function provided by the **.profile** file or the **.login** file must be provided by the desktop's login manager.

User-specific environment variables are set in */Home Directory/* **.dtprofile**. A template for this file is located in **/usr/dt/config/sys.dtprofile**. Place variables and shell commands in **.dtprofile** that apply only to the desktop. Add lines to the end of the **.dtprofile** to incorporate the shell environment file.

System-wide environment variables can be set in Login Manager configuration files. For details on configuring environment variables, see the *Common Desktop Environment 1.0: Advanced User's and System Administrator's Guide*.

Adding and Removing Displays and Terminals for Common Desktop Environment

The login manager can be started from a system with a single local bitmap or graphics console. Many other situations are also possible, however (see the following figure). You can start Common Desktop Environment from:



- Local consoles
- Remote consoles
- Bitmap and character-display
- Xterminal systems running on a host system on the network

An Xterminal system consists of a display device, keyboard, and mouse that runs only the Xserver. Clients, including Common Desktop Environment, are run on one or more host systems on the networks. Output from the clients is directed to the Xterminal display.

The following Login Manager configuration tasks support many possible configurations.

- "Removing a Local Display"
- "Adding an ASCII or Character-Display Terminal" on page 142

Using a Workstation as an Xterminal

From a command line, type:

```
/usr/bin/X11/X -query hostname
```

The X server of the workstation acting as an Xterminal must:

- Support XDMCP and the **-query** command-line option.
- Provide xhost permission (in **/etc/X*.hosts**) to the terminal host.

Removing a Local Display

To remove a local display, remove its entry in the Xservers file in the **/usr/dt/config** directory.

Adding an ASCII or Character-Display Terminal

A character-display console is a configuration in which the console is not a bitmap device.

Adding an ASCII or Character-Display Console if No Bitmap Display Is Present

1. If the **/etc/dt/config/Xservers** file does not exist, copy the **/usr/dt/config/Xervers** file to the **/etc/dt/config** directory.
2. If you have to copy Xservers to**/etc/dt/config**, you must change the **Dtlogin.servers:** line in **/etc/dt/config/Xconfig** to:

   ```
   Dtlogin*servers: /etc/dt/config/Xservers
   ```
3. Comment out the line in **/etc/dt/config/Xservers** that starts the Xserver. This will disable the Login Option Menu.

   ```
   # * Local local@console /path/X :0
   ```
4. Reread the Login Manager configuration files.

Adding a Character-Display Console if a Bitmap Display Exists

1. If the **/etc/dt/config/Xservers** file does not exist, copy the **/usr/dt/config/Xservers** file to the **/etc/dt/config** directory.
2. If you have to copy Xservers to **/etc/dt/config**, you must change the **Dtlogin.servers:** line in **/etc/dt/config/Xconfig** to:

   ```
   Dtlogin*servers: /etc/dt/config/Xservers
   ```
3. Edit the line in**/etc/dt/config/Xservers** that starts the Xserver to read:

   ```
   * Local local@none /path/X :0
   ```
4. Reread the Login Manager configuration files.

Customizing Display Devices for Common Desktop Environment

You can configure Common Desktop Environment Login Manager to run on systems with two or more display devices.

When a system includes multiple displays, the following configuration requirements must be met:

- A server must be started on each display.
- No Windows mode must be configured for each display.

It might be necessary or desirable to use different dtlogin resources for each display.

It may also be necessary or desirable to use different systemwide environment variables for each display device.

Starting the Server on Each Display Device

1. If the **/etc/dt/config/Xservers** file does not exist, copy the **/usr/dt/config/Xservers** file to the **/etc/dt/config** directory.
2. If you have to copy Xservers to **/etc/dt/config**, you must change the **Dtlogin.servers:** line in **/etc/dt/config/Xconfig** to:

   ```
   Dtlogin*servers: /etc/dt/config/Xservers
   ```
3. Edit **/etc/dt/config/Xservers** to start an X server on each display device.

Syntax

The general syntax for starting the server is:

```
DisplayName DisplayClass DisplayType [ @ite ] Command
```

Only displays with an associated Internal Terminal Emulator (ITE) can operate in No Windows mode. No Windows mode temporarily disables the desktop for the display and runs a getty process if one is not already started. This allows you to log in and perform tasks not possible under Common Desktop Environment. When you log out, the desktop is restarted for the display device. If a getty is not already running on a display device, Login Manager starts one when No Windows mode is initiated.

Default configuration

When ite is omitted, display:0 is associated with the ITE (/dev/console).

Specifying a Different Display as ITE

- On the ITE display, set ITE to the character device.
- On all other displays, set ITE to none.

Examples

The following entries in the **Xserver** file start a server on three local displays on `sysaaa:0`. Display `:0` will be the console (ITE).

```
sysaaa:0 Local local /usr/bin/X11/X :0
sysaaa:1 Local local /usr/bin/X11/X :1
sysaaa:2 Local local /usr/bin/X11/X :2
```

On host sysbbb, the bitmap display `:0` is not the ITE; the ITE is associated with device **/dev/ttyi1**. The following entries in the **Xserver** file start servers on the two bitmap displays with No Windows Mode enabled on `:1`.

```
sysaaa:0 Local local@none /usr/bin/X11/X :0
sysaaa:1 Local local@ttyi1 /usr/bin/X11/X :1
```

Specifying the Display Name in Xconfig

You cannot use regular hostname:0 syntax for the display name in **/etc/opt/dt/Xconfig**.

- Use underscore in place of the colon.
- In a fully qualified host name, use underscores in place of the periods.

Example

```
Dtlogin.claaa_0.resource: value
Dtlogin.sysaaa_prsm_ld_edu_0.resource: value
```

Using Different Login Manager Resources for Each Display

1. If the **/etc/dt/config/Xconfig** file does not exist, copy the **/usr/dt/config/Xconfig** file to the **/etc/dt/config directory**.
2. Use the resources resource in **/etc/dt/config/Xconfig** to specify a different resource file for each display (this file is the equivalent to **/etc/opt/dt/Xresources**):

   ```
   Dtlogin.DisplayName.resources: path/file
   ```
3. Create each of the resource files specified in the **Xconfig** file.
4. In each file, place the dtlogin resources for that display.

Example

The following lines in the **Xconfig** file specify different resource files for three displays:

```
Dtlogin.sysaaa_0.resources: /etc/opt/dt/Xresources0
Dtlogin.sysaaa_1.resources: /etc/opt/dt/Xresources1
Dtlogin.sysaaa_2.resources: /etc/opt/dt/Xresources2
```

Running Different Scripts for Each Display

1. If the **/etc/dt/config/Xconfig** file does not exist, copy the **/usr/dt/config/Xconfig** file to the **/etc/dt/config** directory.

2. Use the startup, reset, and setup resources in **/etc/dt/config/Xconfig** to specify different scripts for each display (these files are run instead of **Xstartup**, **Xreset**, and **Xsetup.** file):

   ```
   Dtlogin*DisplayName*sarttup: /path/file
   Dtlogin*DisplayName*startup: /path/file
   Dtlogin*DisplayName*startup: /path/file
   ```

The startup script is run as root after the user has logged in, before the Common Desktop Environment session is started.

The script **/etc/dt/config/Xreset** can be used to reverse the setting made in the **Xstartup** file. The **Xreset** file runs when the user logs out.

Example

The following lines in the **Xconfig** file specify different scripts for two displays.

```
Dtlogin.sysaaa_0*startup:   /etc/opt/dt/Xstartup0
Dtlogin.sysaaa_1*startup:    /etc/opt/dt/Xstartup1
Dtlogin.sysaaa_0*setup:      /etc/opt/dt/Xsetup0
Dtlogin.sysaaa_1*setup:      /etc/opt/dt/Xsetup1
Dtlogin.sysaaa_0*reset:      /etc/opt/dt/Xreset0
Dtlogin.sysaaa_1*reset:      /etc/opt/dt/Xreset1
```

Setting Different Systemwide Environment Variables for Each Display

1. If the **/etc/dt/config/Xconfig** file does not exist, copy the **/usr/dt/config/Xconfig** file to the **/etc/dt/config** directory.
2. Set the environment resource in **/etc/dt/config/Xconfig** separately for each display:

   ```
   Dtlogin*DisplayName*environment: value
   ```

The following points apply to environment variables for each display:

- Separate variable assignments with a space or tab.
- Do not use the environment resource to set TZ and LANG.
- There is no shell processing within the **Xconfig** file.

Example

The following lines in the **Xconfig** file set variables for two displays.

```
Dtlogin*syshere_0*environment:EDITOR=vi SB_DISPLAY_ADDR=0xB00000
Dtlogin*syshere_1*environment: EDITOR=emacs \
         SB_DISPLAY_ADDR=0xB00000
```

Chapter 16. Documentation Library Service

The Documentation Library Service allows you to read, search, and print online HTML documents. It provides a library application that displays in your web browser. Within the library application, you can click on links to open documents for reading. You can also type words into the search form in the library application. The library service searches for the words and presents a search results page that contains links that lead to the documents that contain the target words. Starting with AIX 5.1 you can also download printable versions of books by using the ″Print Tool″ button in the Documentation Library Service GUI.

To launch the library application, type the **docsearch** command or select the CDE help icon, click on the **Front Panel Help** icon, then click on the **Documentation Library** icon.

The documentation search service allows you to access only the documents on your documentation server that are registered with the library and that have been indexed. You cannot read or search the internet or all the documents on your computer. Indexing creates a specially compressed copy of a document or collection of documents. It is this index that is searched rather than the original documents. This technique provides significant performance benefits. When a phrase you are searching for is found in the index, the documentation search service presents a results page that contains links to select and open the document that contains the search phrase.

You can register HTML documents of your own company into the library so that all users can access and search the documents using the library application. Before your documents can be searched, you must create indexes of the documents. For more information on adding your own documents to the library, see "Documents and Indexes" on page 153 .

With the exception of the library search engine, the library's components are installed with the base operating system. To use the library service, it must be configured. You can configure a computer to be a documentation server and install documents on that computer; or you can configure a computer to be a client that gets all of its documents from a documentation server. If the computer is to be a documentation server, the search engine and documentation must also be manually installed.

The library service must be fully configured because it is the library service for the operating system manuals and the Web-based System Manager documentation. Even if you do not need the operating system manuals, you should still configure the documentation library service because it is expected that other applications may use it as the library function for their own online documentation. For instructions on how to install and configure the documentation library service, see Installing and Configuring the Documentation Library Service and Online Documentation in *AIX Version 4.3 Installation Guide*.

The rest of this chapter contains information on changing the configuration of the library service after installation, adding or removing your own documents from the library, and problem determination.

Changing the Configuration of the Documentation Library Service

This section provides information about changing the configuration of the Documentation Library Service after it has been initially installed and configured. For instructions on how to set up the library service for the first time on a computer, see Installing the Online Documentation in *AIX Version 4.3 Installation Guide*.

The following topics are covered in this section:

- "Viewing the Current Configuration" on page 146
- "Changing the Default Remote Documentation Library Service of a Client Computer" on page 146
- "Selecting the Documentation Search Server for a Single User" on page 147
- "Converting a Client System to a Documentation Server System" on page 148
- "Disabling or Uninstalling the Documentation Library Service" on page 148

- “Converting a Standalone Documentation Server into a Public Documentation Remote Server” on page 149
- “Changing the Default Browser” on page 150
- “Changing the Web Server Software on A Documentation Server” on page 150
- “Changing the Documentation Language” on page 151

Viewing the Current Configuration

This process shows the default system documentation server settings. If users have specified different settings in the **.profile** file in their home directories, they are not affected by the default settings.

You can view the configuration of the documentation library service by using either of the system management tools (Web-based System Manager or SMIT).

Using Web-based System Manager

1. Change to the root user.
2. At the command line, type: `wsm`, then double-click on **System Environment**.
3. In the System Environments window, double-click on **Settings**.
4. When the contents are displayed, double-click on the **Default Browser** icon. This shows the current command that is used to launch the default browser that displays the library application.

   Double-click on the **Documentation Server** icon to view the current settings for the documentation server for this computer.

Using SMIT

1. Change to the root user.
2. At the command line, type: `smit web_configure`
3. From the Web Configuration menu, select **Show Documentation and Search Server** to display the current configuration information.

Changing the Default Remote Documentation Library Service of a Client Computer

This configuration process changes the default system documentation server. If users have specified a different server in their own **.profile** file in their home directories, they will not be affected by the default settings.

You can view the configuration of the documentation library service by using either of the system management tools (Web-based System Manager or SMIT).

Using Web-based System Manager

1. Change to the root user.
2. At the command line, type: `wsm`, then double-click on **System Environment**.

   This opens the **System Environments** container.
3. In the System Environments window, double-click on the **Settings** icon to open it, then double-click on **Documentation Server**.
4. Click on the **Remote server host name** radio button, then type the name of the documentation server computer in the field to the right. This is the server computer that contains the documents that you want this client computer to be able to access and search.
5. In the **Server port** field, type the port number the web server software is using. The most commonly used port is 80. An exception is the Lite NetQuestion web server, which **must** use port 49213. Your client computer will now be reconfigured to use the new server.

Using SMIT

1. Change to the root user.
2. On a command line, type: `smit web_configure`

3. From the web configuration screen, select **Change Documentation and Search Server**. From the List menu, select **Remote computer**.
4. In **NAME of remote documentation server**, type the name or IP address of the new server and the appropriate port number. The reconfiguration is complete when the output window shows the message `Documentation server configuration completed`.

Selecting the Documentation Search Server for a Single User

All users on a computer do not have to use the same documentation server. The system administrator sets the default server for users, but users can choose to use a different server. There are two ways users can specify the documentation server they want to use:

- “Changing the Personal Default Documentation Server”
- “Manually Going to a Documentation Server”

Changing the Personal Default Documentation Server

A user’s default documentation server is the documentation server that is used when he or she starts the Documentation Library Service. System administrators set up a default server for all users logged into a system. A user who does not want to use the default documentation server can specify a different personal default documentation server.

To specify their own personal default documentation server, users can do the following:

1. Insert the following two lines in the **.profile** file in their home directory:

   ```
   export DOCUMENT_SERVER_MACHINE_NAME=servername
   export DOCUMENT_SERVER_PORT=portnumber
   ```
2. Replace *servername* with the name of the documentation search server computer they want to use.
3. Replace *portnumber* with the number of the port that the web server on the server uses. In most cases this will be 80. An exception is the Lite NetQuestion web server, which **must** use port 49213.
4. Log out, then log back in to activate the changes.

Once these two lines are placed in the **.profile** file in their home directory, changes that the system administrator makes to the system-wide default settings do not affect these users. If these users want to resume using the system-wide default server, they can remove the two lines inserted in step 1 from their profile, log out, then log back in.

Manually Going to a Documentation Server

When users do not want to change their default documentation server but want to use the documents on another documentation server, they can type the following into the URL location field of his browser:

```
http://server_name[:port_number]/cgi-bin/ds_form
```

This opens into their browser the library application from the document server with the server_name given in the URL. The *port_number* only needs to be entered if the port is different from 80. (80 is the standard port number for most webservers; an exception is the Lite NetQuestion web server which uses port 49213).

In the following example, if a user wants to search the documents on a document server named `hinson`, and the web server on `hinson` uses the standard port 80, the user can enter the following URL:

```
http://hinson/cgi-bin/ds_form
```

A library application would open in the user’s browser to display the documents registered on the server `hinson`. Once the library application from a document server is displayed in the user’s browser, the user can create a bookmark that goes back to the server. The system administrator of a web server can also create a web page that contains links to all the different documentation servers in an organization.

Converting a Client System to a Documentation Server System

In this case, you have a client computer that is using a remote documentation server to access documents. You want to convert this client computer to be a documentation server so that the documents stored on this computer can be read and searched by the users on this computer or by remote users.

See the Installing and Configuring the Documentation Library Service and Installing Documentation in *AIX Version 4.3 Installation Guide* for instructions for installing and configuring a documentation service. Choose the procedures that configure a system as a documentation server.

Disabling or Uninstalling the Documentation Library Service

Use one of the following procedures:

- "Temporarily Disabling a Server"
- "Permanently Uninstalling a Server" on page 149

Temporarily Disabling a Server

There are several different techniques:

- On the documentation server, turn off the web server software or turn off the web server access permissions for all or some users.

  If you are using the Lite NetQuestion web server software, it is automatically restarted each time you reboot the computer. To turn off the Lite NetQuestion web server until the next reboot, kill the **httpdlite** process. To prevent the web server software from being automatically restarted each time the computer reboots, edit the **/etc/inittab** file and remove or comment out the following line:

  ```
  httpdlite:2:once:/usr/IMNSearch/httpdlite -r \
  /etc/IMNSearch/httpdlite/httpdlite.conf >/dev/console 2>&1
  ```

  To restore automatic startup of the lite server, reinsert or uncomment the same line in **/etc/inittab**.

  To manually start the Lite NetQuestion server, type the following command (there is a single space before and after the **-r** flag):

  ```
  /usr/IMNSearch/httpdlite/httpdlite -r /etc/IMNSearch/httpdlite/httpdlite.conf
  ```

- To disable the library service but leave the web server functioning, go to the CGI directory of the web server. Find the file names **ds_form**, **ds_rslt**, and **ds_print**. Turn off these files' execution permissions. This turns off access to all the documentation library service functions. An error message is displayed whenever users try to access the library service on this documentation server.
- To disable the searching of a specific index without removing the documents or index from the documentation sever, unregister the index.

  Note: To re-register the index, you must record the index registry information before you remove it.

  To delete an index:

  1. Login as the root user or library administrator.
  2. Type the following command at a command line:

     ```
     /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -l -x index_name
     ```

     where *index_name* is replaced with the name of the index.
  3. Write the index name, document path, and title.
  4. Type the following command to delete the index:

     ```
     /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -d -x index_name
     ```

  If you ever want to re-register this same index, you must complete the following steps:

  1. Login as the root user or library administrator.
  2. Type the following command at a command line:

```
/usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -c -x index_name -sp \
document path -ti "title"
```

where you insert the index name, document path, and title values you recorded previously.

Permanently Uninstalling a Server

If you are sure you want to permanently remove the documentation library service functions, do the following:

> **Note:** In each of the following steps make sure you uninstall using SMIT instead of deleting software. Deleting does not correctly clean up the system.

1. Uninstall the documentation library service package (*bos.docsearch*). If you want this computer to be a client of another search server, leave the Docsearch Client software installed and just uninstall the Docsearch Server component.
2. Uninstall the documentation service search engine (IMNSearch package). Uninstall both **IMNSearch.bld** (**NetQuestion Index Buildtime**), and **IMNSearch.rte** (**NetQuestion Search Runtime**).
3. Uninstall the web server software if it is not being used for some other purpose.

   > **Note:** If you are using the Lite NetQuestion web server software, you can remove it by uninstalling the fileset **IMNSearch.rte.httpdlite** (**NetQuestion Local HTTP Daemon**).
4. Uninstall the documentation and indexes.

   > **Note:** The operating system documents can be read directly from the documentation CDs by opening the readme file in the top directory of the CDs. However, the search functions will not work.
5. Unregister any indexes that were not automatically unregistered during the uninstall process. This will included any indexes that you manually registered.

To unregister an index:

1. Login as the root user or a search administrator.
2. At the command line, type the following:

   ```
   rm -r /usr/docsearch/indexes/index name
   ```

   where *index name* is the name of the index you want to remove.

All of the documentation server functions should now be disabled. If the users of this computer were using this computer as their documentation server, start SMIT and change the name of the default documentation server to another computer. See “Changing the Default Remote Documentation Library Service of a Client Computer” on page 146.

Converting a Standalone Documentation Server into a Public Documentation Remote Server

The difference between a stand alone documentation server and a public remote server is that the remote server allows people on other machines to access and search the documents stored on the remote server. After a standalone server is connected to a network, modify the web server software’s security configuration controls to allow users on other computers to access the documents on this computer. Consult the web server documentation for instructions on how to alter these access permissions.

> **Note:** If you are using the Lite NetQuestion web server software for your standalone documentation server, you must replace the lite server with a more full-functioned web server software package that can serve remote users. The lite web server can only serve local users. After you install the new server you must reconfigure the documentation service to use the new server. For more instructions on reconfiguration, see “Changing the Web Server Software on A Documentation Server” on page 150.

Changing the Default Browser

This procedure changes the default browser that is used by applications that use the **defaultbrowser** command to open a browser window. The default browser is the browser that is launched when users use the **docsearch** command or the Documentation Library icon on the Help subpanel in the CDE desktop. You can change the default browser by using either of the system management tools, Web-based System Manager (see "Using Web-based System Manager") or SMIT (see "Using SMIT").

Using Web-based System Manager

1. Change to the root user on the client computer.
2. On a command line, type: `wsm`, then double-click on **System Environment**.

   to open the **System Environments** container.
3. In the System Environments window, double-click on the **Settings** icon to open it.
4. In **Settings**, double-click on the **Default Browser** icon.
5. In the Browser command field, type the command that launches the browser that you want to be the default browser for all users on this computer. Include any flags that are required when a URL is included in the command. For example, if you type `wonderbrowser -u http://www.ibm.com` at a command line to open your wonderbrowser with the www.ibm.com page open inside, type `wonderbrowser -u` in this field. Many browsers (for example, Netscape) do not require a flag.
6. Click **OK**. You can now close Web-based System Manager. The browser change will take effect the next time users log back into the computer.

Using SMIT

1. Change to root user.
2. On a command line, type:

   ```
   smit web_configure
   ```
3. From the `Web Configuration` screen, select **Change/Show Default Browser**. On the next screen, type in the field the command that launches your new web browser. Include any flags that are required when a URL is included in the command. For example, if you type:

   ```
   wonderbrowser -u http://www.ibm.com
   ```

   to open your wonderbrowser with the www.ibm.com page open inside, you would type `wonderbrowser -u` in the field. Many browsers (for example, Netscape) do not require a flag. The browser change will take effect the next time users log back into the computer.

Changing the Web Server Software on A Documentation Server

Use the following procedure if you have already configured a documentation server and you now want to change the web server software that it is using.

1. Uninstall the current web server.
2. Install the new web server. For instructions see Install the Web Server Software in the *AIX Version 4.3 Installation Guide*.
3. Configure and start your new web server software. Consult the documentation that came with your web server software and configure and start your web server software. Write down the full pathnames of the web server directories where the server starts looking for HTML documents and CGI programs. If you are going to use the Lite NetQuestion web server or the IBM HTTP Webserver, and you installed them in their default location, you can skip this step. Also, some web servers might not automatically create these directories. If not, you must create them before you continue.

   If your computer is going to serve documents to remote users, you must also configure your web server software to allow access from the users and remote computers that are using this computer as their documentation search server.

Note: If you are using the Lite NetQuestion web server software you do not need to do this step because the lite server can only be used for standalone documents services. It does not support access by remote users.

4. Reconfigure the documentation library service to use the new web server by using either of the system management tools, Web-based System Manager (see "Using Web-based System Manager") or SMIT (see "Using SMIT").

Using Web-based System Manager

1. Change to the root user.
2. On the command line, type: `wsm`, then double-click on **System Environments**.
3. In the System Environments window, double-click on the **Settings** icon to open it.
4. Next, double-click on the **Documentation Server** icon. In this dialog, the **This computer server** radio button is already selected.
5. To the right of the heading **Location of documents and CGI programs**, select your new web server software. If the name of your webserver software is not listed, select **Other**.

   Note: If your web server software is listed by name, but you installed it in a non-default location on your system, or if you set up the web servers to use non-standard locations for their cgi-bin or HTML directories, you must select **Other**.
6. If you selected **Other**, type in the full pathname of the CGI and Documents directories. If you selected one of the default web server packages, skip to the next step.
7. In the **Server port** field, type the port number the web server software is using. The standard default port is 80. An exception is the Lite NetQuestion server, which must use port 49213.
8. Click **OK**. The documentation service on this computer is now reconfigured to use the new webserver software. Any users who were logged in when configuration was completed must log out, and then log back in to reactivate the library service.

Using SMIT

1. Change to the root user.
2. On the command line, type:

   ```
   smit web_configure
   ```
3. From the `Web Configuration` screen, select **Change Documentation and Search Server**.
4. In the `Documentation and Search Server` dialog, select **local - this computer** for server location. From the `Web Server Software` screen, select **List**, then choose the web server software you are using.
5. Enter the full pathnames of the directories and choose the appropriate port number. The standard default port is 80. An exception is the Lite NetQuestion server, which must use port 49213. SMIT now configures your system. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service.

Changing the Documentation Language

By default, if a user opens the library using the **docsearch** command, the **Documentation Library** icon in the Common Desktop Environment, or the **Base Library** icon, the library application displays in the same language as the current locale of the user's client computer. However, there may be reasons that users want to see the documentation in a language other than current default locale of the computer. The documentation language can be changed for all users on a computer, or it can be changed for a single user.

Notes:

1. These techniques do not affect the language that is used if you are opening a document or search form from an HTML link inside a document. These techniques only affect what language is used when you use the desktop icons or the **docsearch** command.
2. Before a computer can serve documents in a language, the locale (language environment) for that language and the library service messages for the language must be installed on the

documentation server. For instructions, see Chapter 7. Installing and Configuring Documentation Library Service and Online Documentation in *AIX Version 4.3 Installation Guide*.

Changing the Default Documentation Language for All Users

To change the default documentation language for all users on a computer, the system administrator (as **root**) can use the Web-based System Manager (see “Using Web-based System Manager:”) or SMIT (see “Using SMIT:”).

Using Web-based System Manager:

1. Change to the root user.
2. On the command line, type: `wsm`, then double-click on **System Environment**.
3. In the `System Environments` window, double-click on the **Settings** icon to open it.
4. In the next view, double-click on the **Documentation Server** icon.
5. Scroll down until you see the **Start Up Web Page** language field, then select your new language.
6. Click **OK**. The documentation service on this computer is now reconfigured to use the new language default. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service with the new default language.

Using SMIT:

1. Change to root user.
2. At the command line, type:
   ```
   smit web_configure
   ```
3. From the web configuration screen, select the `Change/Show Documentation Language` choice.
4. In the **Language** dialog, select the new language. The documentation service on the computer is now reconfigured to use the new language default. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service with the new default language.

To Change Documentation Language for a Single User

A system administrator might assign a single user a documentation language that is different than the default language of the user’s computer. This is done by running the following command as **root**:

```
/usr/bin/chdoclang [-u UID|username] locale
```

where *locale* is replaced by the locale that will be the new language and *username* is replaced with the user’s username. Locale names can be found in the Language Support Table.

Running the command as described adds the following line to the user’s **$HOME/.profile** file:

```
export DOC_LANG=<locale>
```

where *locale* is the locale that will be the new default documentation viewing and searching language.

For example, to change the documentation language of user **fred** to be Spanish (es_ES), type the following command:

```
/usr/bin/chdoclang -u fred es_ES
```

> **Note:** If the `DOC_LANG` environment variable is defined in a user’s **.profile**, it takes precedence over any global `DOC_LANG` setting in the **/etc/environment** file on the user’s computer. Also, for the Common Desktop Environment (CDE), you must uncomment the `DTSOURCEPROFILE=true` line in the **$HOME/.dtprofile** file, which causes the **$HOME/.profile** file to be read during CDE login. The change to a user’s documentation language takes effect the next time the user logs out and then logs back in.

To Remove a Documentation Language Setting

If the documentation language has been set, you can delete the setting. To delete the global system default documentation language setting, run the following command as **root**:

```
/usr/bin/chdoclang -d
```

To delete a single user's language setting, run the following command:

```
/usr/bin/chdoclang -d [UID|username]
```

For example, to remove the user **fred**'s personal language setting to use the system default language, run the following command:

```
/usr/bin/chdoclang -d fred
```

Documents and Indexes

This section covers system management operations on documents and indexes for the documentation search service:

- "Registering Documents for Online Searching"
- "Deleting or Uninstalling Documents" on page 154
- "Updating Documents" on page 154
- "Moving Documents" on page 154
- "Security" on page 155

Registering Documents for Online Searching

Not all documents on a documentation server can be read and searched within the library service application. Two things must occur before a document can be accessed using the Documentation Library Service:

1. The document and its index must be created or installed on the document server.
2. The document and its index must be registered with the library service.

You can register documents two ways:

- If an application ships prebuilt indexes for its documents, you can register the indexes automatically when you install them on your system.
- You can manually create indexes for documents that are already on the server and then manually register the indexes.

This section provides an overview of the steps to register a document and create an index of the document. When you are ready to actually do this work, see the chapter on the documentation library service in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs* for the detailed instructions on completing these steps.

1. Write your document in HTML.
2. Create the index of the document.
3. If you are an application developer who is creating this index for inclusion in an installp package, see the chapter on the documentation library service in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*. Follow the steps to include the index in your installation package and do automatic registration of your indexes during your package's post-installation process.

   If you are the system administrator of a documentation server, the next step is to register the new indexes on the server.
4. Now register the index. After your indexes are registered, they are displayed for reading and searching in the global Documentation Library Service application that is launched by typing the **docsearch** command or by opening the **Documentation Library Service** icon in the CDE Desktop. You can also create your own custom library application that only shows a subset of all registered documents on a documentation sever. For example, you might want a library application that only shows accounting documents. For instructions, see the chapter on the documentation library service in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

For detailed instructions on creating and registering a document and index, see Creating Indexes of your Documentation in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

Deleting or Uninstalling Documents

If a document and its index were automatically registered when an application was installed on the documentation server, you must use normal software uninstall tools of the operating system to remove the document. If you simply delete a registered document or its index, it will still be registered with the library service. This generates error messages during searches since the search service still tries to search the missing index.

Note: If you uninstall a package and it does not correctly remove all of its indexes, use the following procedure to clean up your system.

If you want to delete a document that was manually registered by the system administrator, follow the instructions in Removing Indexes in Your Documentation in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

Updating Documents

If the contents of a document change, the index of the document must be updated to reflect the changes to the contents of the document. If you are installing an updated application and it automatically registers its documents, it automatically updates the old indexes with the new ones. If you are updating a document that a user created, you have to manually update the index for the document.

1. Unregister and delete the old index. You **cannot** just delete an index. This leaves the search service corrupted. Follow the procedure in Removing Indexes in Your Documentation in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.
2. Rebuild the index. See Building the Index in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs* for more information.

Moving Documents

Do not move application documents that were automatically installed with an application. For example, do not move operating system base documentation after it is installed. If you move automatically registered documents, the search service is unable to find the documents and errors occur.

You can move documents that you wrote and manually indexed and registered. However, when you move a document, you must tell the search service how that document path has changed so that the service can find the document.

The first part of a document path is stored in the index registration table, and the last part is stored inside the index for that document. There are two methods for changing a document path depending on which part of the path you are changing.

To determine which method you need to use, as root (or a member of the **imnadm** group:

1. Type:

   ```
   /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -l -x index_name
   ```

   where *index_name* is replaced with the name of the index that contains the documents you want to move.

   The output of the command looks similar to:

   ```
   Index index_name - index_title,
   documents in: path
   function completed
   ```

The *path* in the output shows you the part of your document path that is stored in the registration table. If you are only changing the names of directories that are listed within the *path*, you can use the first move method in the following. Write down the current *index_name*, *index_title*, and *path*. Then skip to the next numbered step to change this part of the document path.

However, if you need to change any part of the path that is lower (to the right) of the part of the path shown in the output, you must update the index instead. This is because the lower part of the path is stored inside the index. To update the index, go back to the “Updating Documents” on page 154 section and complete all the instructions in that section. Also, go to that section if you need to make changes in both the upper and lower parts of the document path. In either case, you do not need to do any other steps in this section.

2. To change the upper part of the document path in the index registration table, type the following command:

```
/usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -u -x index_name -sp \
path -ti "index_title"
```

Note: There must be a trailing slash (/) in the *path*.

In the above commands replace the *path* part of the command with the new path where you moved your document. Replace *index_name* and *index_title* with the values you wrote down from the output of the command in the first step.

For example, if your documents are in the **acctn3en English** index and the index title is ″Accounting Documents″, you can move the document tree from the **/doclink/en_US/engineering** directory into the **/doc_link/en_US/accounting** directory by typing the following:

```
/usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -u -x acctn3en -sp \
/doc_link/en_US/accounting/ -ti "Accounting Documents"
```

Note: If you need to, you can change the index title by typing a new title in the previous command. You **cannot** change the *index_name*.

Changing the document’s library service location is now complete. If you have not already done so, you can now move your documents. Next, test your changes by searching for a word that is inside the moved documents. The document’s link in the search results page correctly displays the document.

Security

Follow your normal security procedures for the documents on the documentation server. In addition, a documentation server also has the added security elements of the document indexes and the web server software.

Indexes are treated as files that include a list of all the words in the original documents. If the documents contain confidential information, then the indexes themselves are treated with the same care as the documents.

There are three levels of security you can set up for indexes:

- **No Restrictions**

  By default, the permissions on the indexes directory are set so that all web server users can both search and read all index files.
- **Search, but not read**

  All web server users can search inside indexes for key words, but cannot open an index file to directly read its contents. This makes it more difficult for users to obtain confidential data, but a person can sometimes still gain a lot of information just by knowing if certain key words are inside a document. Assuming you store all your indexes in the standard location, you can set this level of security by setting the permissions of the **/usr/docsearch/indexes** directory. It is set to the user:group **imnadm:imnadm** with all permissions for others disabled so that only members of the imnadm search administration group can read the index files. To set these permissions type the following two commands:

```
chown -R imnadm:imnadm /usr/docsearch/indexes
```

```
chmod -R o-rwx /usr/docsearch/indexes
```

> **Note:** The user imnadm must always be able to read and execute the directory where you store indexes. This is because the search engine runs as user **imnadm** when it searches inside indexes.

- **No search, no read**

  This is done by setting the permissions as in ″Search, but not read″ to prevent reading of index files. In addition, a user’s permission to use the search service web server is disabled (this prevents searches). The user is unable to search indexes because the web server does not let the user open the search form. This security level is set up using the administration functions in your web server software to turn off a user’s permission to use the web server. See the documentation that came with your web server to determine how to configure your web server software to prevent access by specific users.

Advanced Topics

Search Service Administrators Authority

Only root and members of the **imnadm** (IMN administration) user group have the authority to perform administrative tasks for the Documentation Library Service. This includes tasks such as creating document indexes, registering indexes, and unregistering indexes. If you want users to be able to perform these functions, add them to the **imnadm** group using one of the administration tools.

> **Note:** If you add users to the **imnadm** group, they are able to read the contents of all indexes on the system. See “Security” on page 155 for more information.

Creating Custom Library Applications

When you open the global library application, all documents that are registered with the global view set are displayed. You might want to create a custom library application that only shows a subset of the documents on a documentation server. For example, you may want to put a ″library″ or ″search″ link inside the ″Project X Plan″ HTML document. When a user clicks on one of these links, a library opens and displays a list of the documents for Project X. You can then read or search these documents.

For instructions on how to create your own custom library applications, see the chapter on the documentation library service in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs* for more information.

Problem Determination

This section contains discussions of two different types of problems:

- “Problems That Don’t Generate Error Messages” on page 157
- “Error Message Listings” on page 157

> **Note:** If you receive an error message when using the documentation search service, and your web browser is using a cache, that error message page is stored in your web browser cache. This means that even if you fix the problem that caused the error, the error message continues to be displayed if you repeat the exact same search that caused the error in the first place. Therefore, it is important that you clear out the contents of the browser cache before you retest the search after you have done a fix. Usually, there is a **clear cache** function in the `Options` screen of the browser.

Problems That Don’t Generate Error Messages

- **When the search form is displayed it is not in the correct language.**

  The language of the search form is possibly being set by the document that is opening the search form. For example, if the document was written in Spanish, the author may have specified that when the Search link in the document is clicked, the search service provides the search form in Spanish. Look at the Search link and see if it is specifying a language.

  The web server software might not be reading the locale value correctly. Try restarting your web server to see if it picks up the correct locale.

Error Message Listings

- **ds_form: Error**

  ```
  There was a request to open a viewset named 'XXX'. Either there is no viewset
  named 'XXX', or there is no configuration file named '/usr/docsearch/views
  /<locale>/XXX/config' for the viewset. If you want to continue now, you
  can use the generic search page, which will allow you to search all volumes.

  Use generic page
  ```

  This error occurs when the search form is passed a viewset name and that viewset does not exist or is not readable by the user **imnadm**.

  In this message XXX indicates the name of the viewset. If the viewset given in the message does not match the name of the desired viewset, edit the HTML link being used to call the search form and change the viewset given.

- **ds_form: Error EhwStartSession 70**

  ```
  There was a problem communicating with the search program.

  Retry your search. If you repeatedly get this error, contact the system administrator of the search
  server computer. They may want to try restarting the search program.
  ```

  This error occurs if the search engine is not running.

  To start the search engine, you must be root or a member of the group **imnadm**. To start the search engine type:

  ```
  itess -start search
  ```

- **ds_form: Error**

  ```
  The search page is not available in the requested language 'xx_XX'.
  ```

  This error occurs if the CGIs are passed a language for which the documentation server does not have the locale installed.

  In this message xx_XX is the language for which there was no locale installed. If it is available, the locale for the language can be installed. Otherwise, specify a language for which there is a locale installed by using the *lang* parameter.

- **ds_form: Error EhwSearch 77**

  ```
  An error occurred when attempting to open or read an index file.
  Contact the system administrator of the search server computer.
  ```

  This error occurs if the file permissions for an index are incorrectly set on files or directories that are part of that index.

  Where *indexname* is the name of an index, the index files, or links to them, can be found in:

  ```
  /usr/docsearch/indexes/indexname/data
  /usr/docsearch/indexes/indexname/work
  ```

Make sure all index file permissions adhere to the following rules:

- All index files and directories are readable by the user **imnadm**.
- The work directory and all files in it are writable by the user **imnadm**.
- In the data directory the **iteadmtb.dat** and **iteiq.dat** files are writable.
- All index files and directories have **imnadm** as owner and group.

- **ds_rslt: Error EhwSearch 32**

  ```
  The search program reported an unexpected error condition.
  ```

  The most likely cause of this error is that the file permissions for one or more indexes are incorrectly set.

  Where *indexname* is the name of an index, the index files, or links to them, can be found in:

  ```
  /usr/docsearch/indexes/indexname/data
  /usr/docsearch/indexes/indexname/work
  ```

  - All index files and directories are readable by the user **imnadm**.
  - The work directory and all files in it are writable by the user **imnadm**.
  - In the data directory the **iteadmtb.dat** and **iteiq.dat** files are writable.
  - All index files and directories have **imnadm** as owner and group.

- **ds_rslt: Error EhwSearch 8**

  ```
  One or more of the indexes for the selected volumes contain errors that make them unsearchable.

  Error 76 in index indexname

  The requested function is in error.

  Contact the system administrator of the search server computer.
  ```

  This error occurs when one or more of the indexes being searched needs to be reset.

  To reset an index you must be root or a member of the group **imnadm**. Reset the index with the **itectrix** command by typing:

  ```
  /usr/IMNSearch/bin/itectrix -s server -x indexname -reset
  ```

- **ds_rslt: Error EhwSearch 76**

  ```
  The requested function is in error.

  Contact the system administrator of the search server computer.
  ```

  This error occurs when all of the indexes being searched need to be reset.

  To reset an index you must be root or a member of the group **imnadm**. Reset the index with the **itectrix** command by typing:

  ```
  /usr/IMNSearch/bin/itectrix -s server -x indexname -reset
  ```

- **Cannot run ds_form**

  A web server error message saying it cannot run **ds_form**. The exact wording of the message varies across different web server software. For example, the message might say something like:

  ```
  ds_form is not an executable
  ```

  or

  ```
  Cannot locate ds_form
  ```

The web server software cannot find the search service **ds_form** CGI program because the server has not been configured correctly. See “Changing the Configuration of the Documentation Library Service” on page 145 to make sure that the Documentation Library Service is installed and configured correctly on the server computer.

Chapter 17. Power Management

Note: The information in this section is specific to POWER-based.

Power Management is a technique that enables hardware and software to minimize system power consumption. It is especially important for products that operate with batteries and desktop products.

See Power Management Limitation Warnings in the *AIX 5L Version 5.1 System User's Guide: Operating System and Devices*, which contains important information for all Power Management users.

Prerequisites

You must have root user authority to perform most Power Management tasks.

Procedures

You can use the following tools to perform the Power Management tasks in the following table:

- the System Management Interface Tool (SMIT)
- commands
- the Power Management application

Power Management Tasks			
Task	*SMIT Fast Path*	*Command or File*	*PM Application*
Enable Events	**smit pmEnable**	**pmctrl -e -a enable**	**/usr/lpp/x11/bin/xpowerm**
Disable Events	**smit pmEnable**	**pmctrl -e -a full_on**	**/usr/lpp/x11/bin/xpowerm**
Configure Power Management	**smit pmConfigConfigure**	**mkdev -l pmc0**	
Unconfigure Power Management	**smit pmConfigUnconfigure**	**rmdev -l pmc0**	
Start System State Transition	**smit pmState**	**pmctrl -e -a suspend**	**/usr/lpp/x11/bin/xpowerm**
Change/Show Parameters	**smit pmData**	**pmctrl**	**/usr/lpp/x11/bin/xpowerm**
Change Timer Setting	**smit pmTimer**	**pmctrl**	**/usr/lpp/x11/bin/xpowerm**
Change Display Power Management	**smit pmDisplaySelect**	**pmctrl**	**/usr/lpp/x11/bin/xpowerm**
Change Idle Time for Each Device	**pmDevice**	**pmctrl**	**/usr/lpp/x11/bin/xpowerm**
Show Battery Information	**smit pmBatteryInfo**	**battery**	**/usr/lpp/x11/bin/xpowerm**
Discharge Power Management Battery	**smit pmBatteryDischarge**	**battery -d**	**/usr/lpp/x11/bin/xpowerm**

Chapter 18. Devices

Devices include hardware components such as, printers, drives, adapters, buses, and enclosures, as well as pseudo-devices, such as the error special file and null special file. This section provides procedures for the following tasks:

- “Preparing to Install a Device”
- “Installing a SCSI Device” on page 164
- “Installing an IDE Device” on page 170
- “Configuring a Read/Write Optical Drive” on page 174
- “Managing Hot Plug Connectors” on page 174
- “Working with Device Problems” on page 183

See “Chapter 18. Devices” in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices* for an overview and additional device information.

Preparing to Install a Device

Installing devices on your system consists of identifying where the device is to be attached, connecting the device physically, and configuring the device with Web-based System Manager, the Configuration Manager, or SMIT.

Devices fall into two categories: SCSI and non-SCSI devices. The installation procedures have basic similarities, but the SCSI device installation requires additional steps for identifying the location code and SCSI address of the device. See “Installing a SCSI Device” on page 164 for more information about installing SCSI devices.

Procedure

This section documents installation tasks that are common to all devices. Because of the wide variety of devices that you can install on your system, only a general procedure is provided. See the installation instructions shipped with the specific device.

> **Note:** The following procedure requires a shutdown of your system to install the device. Not all device installations require a shutdown of your system. Refer to the documentation shipped with the specific device.

1. Stop all applications running on the system unit and shut down the system unit using the **shutdown** command.
2. Turn off the system unit and all attached devices.
3. Unplug the system unit and all attached devices.
4. Connect the new device to the system using the procedure described in the setup and operator guide for the device.
5. Plug in the system unit and all attached devices.
6. Turn on all the attached devices leaving the system unit turned off.
7. Turn on the system unit when all the devices complete power-on self-tests (POST).

The Configuration Manager automatically scans the attached devices and configures any new devices it detects. The new devices are configured with default attributes and recorded in the customized configuration database placing the device in **Available** state.

You can manually configure a device using Web-based System Manager (`wsm`, then select `Devices`), or the SMIT fast path, **smit dev**, if you need to customize the device attributes or if the device is one that the Configuration Manager cannot configure automatically (see the device documentation that shipped with the device for specific configuration requirements).

Installing a SCSI Device

This section outlines the procedure used to install a SCSI device on your system. The procedure has been divided into several tasks that must be performed in order.

Prerequisites

- There must be at least one unused SCSI address on a SCSI controller on the system.
- If you are updating the product topology diskettes, you need the Product Topology System diskette which is kept with important records for the system, and the Product Topology Update diskette which is shipped with the device.
- You must have access to the operator guide for your system unit.
- Verify that the interface of the device is compatible with the interface of the SCSI controllers on the system unit. SCSI controllers with single-ended interfaces (identified as type 4-X in the *About Your Machine* document shipped with your system unit) only supports devices intended to connect to single-ended interfaces, not devices intended to connect to differential interfaces.

  The following list shows the SCSI I/O controller types:

TYPE #	INTERFACE TYPE
4-1	Single-ended, Narrow
4-2	Differential, Narrow, Fast
4-4	Single-ended, Narrow, Fast
4-6	Differential, Wide, Fast
4-7	Single-ended, Wide, Fast
4-C	Differential, Wide, Fast

  With appropriate cabling, you can attach:

  – Narrow devices to narrow or wide adapters

  – Wide devices to narrow or wide adapters

  – Slow devices to slow or fast adapters

  – Fast devices to slow or fast adapters

  You cannot attach:

  – Differential devices to single-ended adapters

  – Single-ended devices to differential adapters

Task 1 - Determine the Number and Location of the SCSI Controllers

Determine how many SCSI controllers are attached to your system unit and where the SCSI controllers are located. A SCSI controller might be in an adapter slot or built into the system planar. If your system has a SCSI-2 Fast/Wide Adapter/A or a SCSI-2 Differential Fast/Wide Adapter/A, remember that it has two SCSI controllers (SCSI buses). Thus, two SCSI controllers might be found in an adapter slot or built into the system planar.

You can obtain this information three different ways:

- Inspecting your system unit. This method can be used anytime.
- Using a software configuration command. This method is available only when the operating system has been installed on the system unit.

- Using the *About Your Machine* document shipped with your system unit. This method is valid only for initial setup and installation of a new system unit.

Inspecting the System Unit

Look for SCSI I/O controllers in the adapter slots in the back of the system unit. The adapter slots are marked with numbers one, two, and so on. Single-ended SCSI I/O controllers in adapter slots are labeled `4-X`. SCSI I/O controllers are typically located in adapter slot one for desktop models or in adapter slot eight for floor models.

If you find the letters SCSI molded into the back of the system unit next to a cable connector, the system unit has a SCSI I/O controller built into the system planar. The connector labeled SCSI is the location to connect the built-in SCSI controller.

Using a Software Configuration Command

This method applies to a system that already has the operating system installed.

To list the SCSI I/O controllers on the system, type the following commands:

```
lscfg -l scsi*
lscfg -1 vscsi*
```

Examine the list of SCSI controllers that are displayed. The following sample display from the **lscfg -l scsi*** command shows three SCSI I/O controllers. Controller scsi0 is located in adapter slot one. The adapter slot number is the fourth digit in the location value. Controller scsi1 is located in adapter slot two. Controller scsi2, with location value 00-00-0S, is built into the system planar and does not have a slot number.

```
DEVICE    LOCATION      DESCRIPTION

scsi0     00-01         SCSI I/O Controller
scsi1     00-02         SCSI I/O Controller
scsi2     00-00-0S      SCSI I/O Controller
              |  |
    4th digit is  A location code of the format 00-00-XX
    the adapter  means the controller is contained on the
    slot number  planar and does not have a slot number.
```

The following is a sample display from the **lscfg -l vscsi*** command. A SCSI-2 Fast/Wide Adapter/A or a SCSI-2 Differential Fast/Wide Adapter/A adapter is located in adapter slot 3, and the listing shows the two buses on this adapter— one internal and one external. The vscsi0 device is connected to the internal bus. This is indicated by the `0` in the sixth digit of the location code. The vscsi1 device is connected to the external bus, which is denoted by the `1` in the sixth digit.

```
DEVICE      LOCATION      DESCRIPTION

vscsi0      00-03-00      SCSI I/O Controller Protocol Device
vscsi1      00-03-01      SCSI I/O Controller Protocol Device
                   |
                   A ′1' in the 6th digit means the device
                   is connected to the fast/wide external
                   bus; a ′0' means the device
                   is connected to the internal bus.
```

Initial Setup

Use the *About Your Machine* document to determine the SCSI I/O controllers on the system if the device is being installed during initial setup.

> **Note:** Incorrect results are produced if controllers have been added after the system was shipped from the factory.

1. Determine the SCSI I/O controllers installed in adapter slots by scanning the listings from the *About Your Machine* document. The following is a sample entry for a SCSI I/O controller located in an adapter slot:

```
Slot  Adapters                               Type      P/N

1     SCSI I/O Controller                     4-1      31G9729
2     SCSI-2 Differential Fast/Wide Adapter/A  4-6      71G2594
3     SCSI-2 Fast/Wide Adapter/A              4-7      71G2589
```

2. Determine whether the system unit has a SCSI controller built into the planar board. A built-in SCSI I/O controller is standard on some system units. Your system unit has a built-in SCSI controller if there is a connector labeled SCSI on the back of the system unit or the *About Your Machine* document shows an internal media SCSI device with a blank slot number. The following is a sample entry from an *About Your Machine* document that shows an internal 400 MB SCSI disk driver:

   ```
   BAY  INTERNAL MEDIA DEVICES   ADDRESS     SLOT   P/N

        -400 MB SCSI Disk Drive  SCSI_ID=0          73F8955
   ```

Task 2 - Select a SCSI Controller and a SCSI Address on the Controller

After identifying the SCSI controllers attached to the system unit, select the SCSI I/O controller you want to connect the device to. This SCSI I/O controller should have at least one SCSI address that is not already assigned to another device.

Determine what SCSI addresses are not already assigned to another device by viewing information about the devices already connected to the SCSI controllers.

You can use two methods to select a SCSI I/O controller and a SCSI address on the controller that is not already assigned to another device:

- Using a software configuration command if the operating system is already installed on the system unit.
- Using the *About Your Machine* document for initial setup and installation of a new system unit.

Using a Software Configuration Command

This method applies to a system that already has the operating system installed.

1. Type the following command to list all the currently defined SCSI devices:

   ```
   lsdev -C -s scsi -H
   ```

2. Examine the list of devices already assigned to SCSI addresses on the SCSI controllers. Each row in this display shows the logical name, status, location, and description of a SCSI device. The location for each device begins with the location of the controller that the device is connected. The seventh digit of each location field is the SCSI ID or SCSI address for the device. In the following sample, the SCSI I/O controller with address `00-01`, has three devices with SCSI addresses 0, 1, and 2 attached. The SCSI I/O controller with location `00-02` has one device, with SCSI address 2 attached. The SCSI I/O controller with location `00-00-0S`, that is built into the system planar, has one device with SCSI address 1 attached.

   ```
   name     status       location       description

   hdisk0   Available    00-01-00-0,0   320MB SCSI Disk Drive
   hdisk1   Available    00-01-00-1,0   320MB SCSI Disk Drive
   rmt0     Available    00-01-00-2,0   2.3GB 8mm Tape Drive
   cdo      Defined      00-02-00-2,0   CD ROM Drive
   rmt1     Available    00-00-0S-1,0   2.3GB 8mm Tape Drive
                                  |
                             SCSI address (7th digit)
   ```

3. Typically, SCSI I/O controllers support up to seven devices, with SCSI addresses `0` through `6`. If the SCSI I/O controller supports wide SCSI, it supports up to `15` devices per SCSI bus, with addresses ranging from 0 through `15`, excluding `7`. Combine this and the information displayed by the previous command to create a list of unassigned SCSI addresses on each controller. The following is one possible way of writing this list with the sample information.

```
Position of SCSI controller      Unassigned SCSI addresses

Adapter slot 1                   3, 4, 5, 6
Adapter slot 2                   0, 1, 3, 4, 5, 6
Built into system planar         0, 2, 3, 4, 5, 6
Adapter slot 3 (external)        0, 1, 2, 3, 4, 5, 6,
                                 8, 9, 10, 11, 12, 13, 14, 15
Adapter slot 3 (internal)        0, 1, 2, 3, 4, 5, 6,
                                 8, 9, 10, 11, 12, 13, 14, 15
```

Note: `7` is the default SCSI ID value for SCSI adapters. The default SCSI ID can be changed for most of the supported SCSI I/O controllers.

4. Select an unassigned SCSI address on one of the controllers, and record the SCSI address and the controller position for later use.

Initial Setup

Use the *About Your Machine* document to determine the devices assigned to the SCSI I/O controllers on the system if the device is being installed during initial setup.

Note: Incorrect results are produced if controllers have been added after the system was shipped from the factory.

1. Determine the SCSI devices assigned to SCSI addresses on the SCSI controllers by examining ″Internal Media Devices.″ The following is a sample listing from the *About Your Machine* document where the built-in SCSI I/O controller has one device attached and the SCSI I/O controller in adapter slot 1 has two devices attached:

```
BAY  INTERNAL MEDIA DEVICES   ADDRESS    SLOT   P/N

     -400 MB SCSI Disk Drive  SCSI_ID=0         73F8955
C    -320 MB SCSI Disk Drive  SCSI_ID=0  AS 1   93X2355
D    -320 MB SCSI Disk Drive  SCSI_ID=1  AS 1   93x2355
```

2. Create a list of unassigned SCSI addresses on each controller. The following is one possible way of writing this list with the sample *About Your Machine* document:

```
Position of SCSI controller     Unassigned SCSI addresses

Built into system planar        1, 2, 3, 4, 5, 6
Adapter slot 1                  2, 3, 4, 5, 6
```

3. Select an unassigned SCSI address on one of the controllers and record the SCSI address and the controller position for later use.

Task 3 - Setting Up the Hardware

Prerequisites

- Do not begin this task until you have selected and recorded the:
  - Position of the SCSI I/O controller where the device will be connected (either built-in or identified by an adapter slot number).
  - SCSI address for the device.
- Determine the physical position on the system unit to connect the selected SCSI controller. For example, locate adapter slot 1 on your system unit and the position of the built-in SCSI adapter. Refer to the operator guide for help.

Procedure

1. Shut down the system unit using the **shutdown** command after stopping all applications that are currently running. To stop the system immediately without notifying other users, type:

```
shutdown -F
```

2. Wait for the message `Halt Completed` or a similar message to appear.
3. Turn off the system unit and all attached devices.

4. Unplug the system unit and all attached devices.
5. Make the physical connections following the procedure described in the setup and operator guide.

   Note: Do not power on the system unit; proceed to the next task.

Task 4 - Add the Device to the Customized Configuration Database

This task makes the device known to the system. During system unit startup, the operating system reads the current configuration and detects new devices. A record of each new device is added to the customized configuration database and each device is given default attributes.

If the device is being installed on a new system unit, the operating system must be installed. Instructions for installing the operating system are included in the installation guide for the operating system.

Follow this procedure to add a device to the customized configuration database:

1. Plug in the system unit and all attached devices.
2. Turn on all the devices, but leave the system unit turned off.
3. Turn on the system unit when all the attached devices have completed power-on self-tests (POSTs).

   Note: The startup process automatically detects and records the device in the customized configuration database.
4. Confirm that the device was added to the customized configuration database using Web-based System Manager (type `wsm`, then select `Devices`), or the SMIT fast path, **smit lsdtmscsi**. A list of all defined devices is displayed. Look at the location field for the SCSI adapter and SCSI address values of the device you just installed.

Task 5 - Verify the System (Optional)

This task is not required for installing a device, but it is recommended.

For additional information about this task, review ″Using the System Verification Procedure″ in the operator guide for the system unit.

Prerequisite

1. Shut down the system unit by stopping all application programs running on the system unit. Enter the `shutdown -F` command and wait for the `Halt Completed` message.
2. Turn off the system unit.

Procedure

1. Set the key mode switch to the Service position.
2. Turn on the system unit.
3. Press Enter when DIAGNOSTICS OPERATING INSTRUCTIONS is displayed.
4. Select **DIAGNOSTIC ROUTINES** and press Enter.
5. Select **System Verification** and press Enter.
6. Select the resource corresponding to the device being installed and press Enter.
7. Follow the instructions for the diagnostic routine for your particular device.
8. Wait for the test to end. A successful test ends with the TESTING COMPLETE menu and a message stating that `No trouble was found`. An unsuccessful test ends with a message stating that `A PROBLEM WAS DETECTED` and includes a service request number (SRN). If the test failed, record the SRN and report the problem to your service representative.
9. Press Enter.
10. Press F3 several times until you return to the DIAGNOSTIC OPERATING INSTRUCTIONS.

11. Skip to Task 6, item 3 if you are updating the topology diskettes. Otherwise, continue with this procedure.
12. Press F3 to shut down the system unit.
13. Set the key mode switch to the Normal position, and press the Reset button when you are ready to resume normal operations.

Task 6 - Update the Product Topology Diskettes (Optional)

Product topology diskettes keep an electronic record of what is attached to your system. This task is performed during the initial installation of any device that has a Product Topology Update diskette.

For additional information about updating product topology diskettes, review the information on using the diagnostics and service aids in the operator guide.

Prerequisites

1. Obtain the Product Topology System diskette that is shipped with the system unit and the Product Topology Update diskette that is shipped with the new device.
2. Shut down the system unit by stopping all application programs running on the system by typing the `shutdown -F` and waiting for a `Halt Completed` message.
3. Turn off the system unit.

Procedure

1. For Microchannel systems, set the key mode switch to the Service position.
2. Turn on the system unit.
3. Press Enter when the DIAGNOSTICS OPERATING INSTRUCTIONS menu is displayed.
4. Select **Service Aid** and press Enter.
5. Select **Product Topology** and press Enter.
6. Select **Device Installation, ECs and MESs** and press Enter.
7. Follow the instructions on your display.
8. When the question `Do you have any update diskettes that have not been loaded?` displays, answer `Yes`, and insert the Product Topology Update diskette.
9. Follow the instructions on your display.
10. If the EC AND MES UPDATES menu (screen 802311) is displayed and asks for data you do not have, use the listed function key to commit.
11. Follow the instructions for your display.
12. When the PRODUCT TOPOLOGY SERVICE AID menu (screen number 802110) is displayed, press F3 several times until you return to the DIAGNOSTIC OPERATING INSTRUCTIONS menu.
13. Press F3 once more from the DIAGNOSTIC OPERATING INSTRUCTIONS menu to shut down the system unit.
14. Remove the diskette.
15. Set the key mode switch to the Normal position, and press the Reset button when you are ready to resume normal operations.
16. Return the Product Topology System diskette to its normal storage location.
17. Return the Product Topology Update diskette.
    a. For customers within the United States of America, place the Product Topology Update diskette into the self-addressed prepaid mailer provided and mail it.
    b. For customers outside the United States of America, place the Product Topology Update diskette into the self-addressed prepaid mailer provided and return it to your service representative. *Do not mail it*.

Task 7 - Customize the Attributes for the Device (Optional)

Default attributes are assigned to a supported device when it is added to the customized configuration database. These attributes are appropriate for typical use of the device. Change the device attributes when the device you are installing is not supported or when you need to customize part of the device operation. For example, you might need to change your tape drive to write tapes in a lower-density format.

To customize the attributes for a device, use Web-based System Manager (type `wsm`, then select `Devices`), or the SMIT fast path, **smit dev**.

Installing an IDE Device

This section outlines the procedure used to install an IDE device on your system. The procedure has been divided into several tasks that must be performed in order.

Prerequisites

- You must have access to the operator's guide for your system unit and the installation guide for the device to be installed. The documentation must identify how to set the IDE device jumper to configure the device to either the master or slave setting.
- There must be at least one unused IDE device ID on an IDE adapter on the system.
- If you are updating the product topology diskettes, you need the Product Topology System diskette which is kept with important records for the system, and the Product Topology Update diskette which is shipped with the device.
- Verify that the interface of the device is compatible with the interface of the IDE controllers on the system unit.
- There are two classifications for IDE devices, ATA and ATAPI. ATA are disk devices and ATAPI are CD-ROM or tape devices. Up to two devices are allowed to be connected to each IDE controller, one master and one slave. Typically an IDE adapter has two controllers, which allows up to four IDE devices to be attached.

  With appropriate cabling, you can attach any of the following device combinations to a single controller:

  - 1 ATA device as master
  - 1 ATAPI device as master
  - 2 ATA devices as master and slave
  - 1 ATA device as master and 1 ATAPI device as slave
  - 2 ATAPI devices as master and slave

  You cannot attach the following:

  - 1 ATA device as slave only
  - 1 ATAPI device as slave only
  - 1 ATAPI device as master and 1 ATA device as slave

Task 1 - Determine the Number and Location of the IDE Controllers

Determine how many IDE controllers are attached to your system unit and where the IDE controllers are located. An IDE adapter may be in an adapter slot or built into the system planar. Remember that IDE adapters have two IDE controllers (IDE buses). Thus, two IDE controllers are found in an adapter slot or built into the system planar.

You can obtain this information two different ways:

- Using a software configuration command. This method is available only when the operating system has been installed on the system unit.

- Using the *About Your Machine* document shipped with your system unit. This method is valid only for initial setup and installation of a new system unit.

Using a Software Configuration Command

This method applies to a system that already has the operating system installed.

To list the IDE I/O controllers on the system, type the following commands:

```
lscfg -l ide*
```

Examine the list of IDE controllers that are displayed. The following sample display from the **lscfg -l ide** command shows two IDE I/O controllers. Controller `ide0` and `ide1` are located on the system planar. The planar indicator is the second digit in the location value with a value of 1.

```
DEVICE    LOCATION      DESCRIPTION

ide0      01-00-00      ATA/IDE Controller Device
ide1      01-00-01      ATA/IDE Controller Device

           |     |
2nd digit is     6th digit indicates the controller number.
the adapter
slot number
```

Initial Setup

Use the *About Your Machine* document to determine the IDE I/O controllers on the system if the device is being installed during initial setup.

> **Note:** Incorrect results are produced if controllers have been added after the system was shipped from the factory.

Determine whether the system unit has an IDE controller built into the planar board. A built-in IDE I/O controller is standard on some system units. Your system unit has a built-in IDE controller if *About Your Machine* document shows an internal media IDE device with a blank slot number.

Task 2 - Select an IDE Controller and an IDE Address on the Controller

After identifying the IDE controllers attached to the system unit, select the IDE I/O controller to which you want to connect a device. This IDE I/O controller must have at least one IDE setting that is not already assigned to another device.

Determine whether IDE device setting must be jumpered as master or slave. If no device is currently attached to the controller, the IDE device jumper must be set to master (some devices require no device ID setting in this situation). If an IDE device is already attached, the type of device must be determined. Disks are ATA devices. CD-ROM and tape are ATAPI devices. If ATA and ATAPI devices are both attached to the same IDE controller, the ATA device must be set to master ID and the ATAPI device must be set to slave ID.

Determine what IDE devices are attached to a controller by viewing information about the devices already connected to the IDE controllers.

You can use two methods to select an IDE I/O controller and an IDE address on the controller that is not already assigned to another device:

- Using a software configuration command if the operating system is already installed on the system unit.
- Using the *About Your Machine* document for initial setup and installation of a new system unit.

Using a Software Configuration Command

This method applies to a system that already has the operating system installed.

1. Type the following command to list all the currently defined IDE devices:

```
lsdev -C -s ide -H
```

2. Examine the list of devices already assigned to each IDE controller. Each row in this display shows the logical name, status, location, and description of an IDE device. The location for each device begins with the location of the controller that the device is connected. In the sample below, the IDE I/O controller with address 01-00-00 has two IDE devices attached. The IDE I/O controller with location 01-00-01 has one IDE device attached.

```
name     status       location       description
hdisk0   Available    01-00-00-00    720 MB IDE Disk Drive
hdisk1   Available    01-00-00-01    540 MB IDE Disk Drive
cd0      Available    01-00-01-00    IDE CD-ROM Drive
                             |
                         IDE controller address (6th digit)
```

3. Select a controller that does not have two IDE devices already connected.
4. If one device is already attached to the controller, determine the type of the device. Also determine the type of device to be installed. Disk devices are classified as ATA devices. CD-ROM and tape devices are classified as ATAPI devices.
5. Determine the IDE jumper setting for the new device depending upon the combination of devices to be connected to the IDE controller. If the new device is the only device connected to the controller, the device jumper setting must be set to the master position (some devices require no setting in this case). If both devices are the same type, the new device jumper setting can be set to the slave position. If there is a mix of devices (ATA and ATAPI), the ATA device jumper must be set to the master position and the ATAPI device jumper must be set to the slave position. If there is a mix of devices and the new device is an ATA device (disk), the device jumper for the currently existing ATAPI device must be changed to the slave position and the new ATA device jumper must be set to master. If there is a mix of devices and the new device is an ATAPI device (CD-ROM or tape), the device jumper for the new ATAPI device must be set to slave and if the ATA device does not currently have a jumper setting, it must be set to master.

Initial Setup

Use the *About Your Machine* document to determine the devices assigned to the IDE I/O controllers on the system if the device is being installed during initial setup.

> **Note:** Incorrect results are produced if controllers have been added after the system was shipped from the factory.

1. To determine the IDE devices assigned to addresses on the IDE controllers, see ″Internal Media Devices″ in *About Your Machine*.
2. Select a controller that does not have two IDE devices already connected.
3. If one device is already attached to the controller, determine the type of the device. Also determine the type of device to be installed. Disk devices are classified as ATA devices. CD-ROM and tape devices are classified as ATAPI devices.
4. Determine the IDE jumper setting for the new device depending upon the combination of devices to be connected to the IDE controller. If the new device will be the only device connected to the controller, the device jumper setting must be set to the master position (some devices require no setting in this case). If both devices are the same type, the new device jumper setting can be set to the slave position. If there is a mix of devices (ATA and ATAPI), the ATA device jumper must be set to the master position and the ATAPI device jumper must be set to the slave position. If there is a mix of devices and the new device is an ATA device (disk), the device jumper for the currently existing ATAPI device must be changed to the slave position and the new ATA device jumper must be set to master. If there is a mix of devices and the new device is an ATAPI device (CD-ROM or tape), the device jumper for the new ATAPI device must be set to slave and if the ATA device does not currently have a jumper setting, it must be set to master.

Task 3 - Setting Up the Hardware

Prerequisites

- Do not begin this task until you have selected and recorded the following:
  - Position of the IDE I/O controller where the device will be connected (either built-in or identified by an adapter slot number).
  - IDE address for the device.
- Determine the physical position on the system unit to connect the selected IDE controller. For example, locate the position of the built-in IDE controller. Refer to the operator's guide for help.

Procedure

1. Shut down the system unit using the **shutdown** command after stopping all applications that are currently running. Type `shutdown -F` to stop the system immediately without notifying other users.
2. Wait for the message `Halt Completed` or a similar message to be displayed.
3. Turn off the system unit and all attached devices.
4. Unplug the system unit and all attached devices.
5. Make the physical connections following the procedure described in the setup and operator guide.

   Note: Do not power on the system unit; proceed to the next task.

Task 4 - Add the Device to the Customized Configuration Database

This task makes the device known to the system. During system unit startup, the operating system reads the current configuration and detects new devices. A record of each new device is added to the customized configuration database and are given default attributes.

If the device is being installed on a new system unit, the operating system must be installed. Instructions for installing the operating system are included in the installation guide for the operating system.

Follow this procedure to add a device to the customized configuration database:

1. Plug in the system unit and all attached devices.
2. Turn on all the devices, but leave the system unit turned off.
3. Turn on the system unit when all the attached devices have completed power-on self-tests (POSTs).

   Note: The startup process automatically detects and records the device in the customized configuration database.
4. Confirm that the device was added to the customized configuration database using the Web-based System Manager (type **wsm**), or the SMIT fast path, **smit lsdidea**. A list of all defined devices is displayed. Look at the location field for the IDE adapter and IDE address values of the device you just installed.

Task 5 - Customize the Attributes for the Device (Optional)

Default attributes are assigned to a supported device when it is added to the customized configuration database. These attributes are appropriate for typical use of the device. Change the device attributes when the device you are installing is not supported or when you need to customize some part of the device's operation. For example, you might need to change your tape drive to write tapes in a lower-density format.

To customize the attributes for a device use the SMIT fast path, **smit dev**.

Configuring a Read/Write Optical Drive

There are two methods for configuring a read/write optical drive.

Prerequisite

The read/write optical drive must be connected to the system and powered on.

Method 1

Method one is the faster of the two methods. It only configures the read/write optical drive specified. To use this method, you must provide the following information:

Subclass	Defines how the drive is attached.
Type	Specifies the type of read/write optical drive.
Parent Name	Specifies the system attachment the drive is connected to.
Where Connected	Specifies the logical address of the drive.

Enter the following command to configure the read/write optical drive:

```
mkdev -c rwoptical -s Subclass -t Type -p ParentName -w WhereConnected
```

The following is an example of a read/write optical drive that has a SCSI ID of 6, a logical unit number of zero, and is connected to the third (scsi3) SCSI bus:

```
mkdev -c rwoptical -s scsi -t osomd -p scsi3 -w 6,0 -a pv=yes
```

Method 2

Method two uses the Configuration Manager, searching the current configuration, detecting any new devices, and automatically configuring the devices. This method is used when little information is known about the read/write optical drive.

1. Use the configuration manager to configure all newly detected devices on the system (including the read/write optical drive) by typing:
   ```
   cfgmgr
   ```
2. Type the following command to list the names, location codes, and types of all currently configured read/write optical drives:
   ```
   lsdev -C -c rwoptical
   ```
3. Determine the name of the newly configured read/write optical drive using the location code that matches the location of the drive being added.

Managing Hot Plug Connectors

This section includes the following procedures for managing hot plug connectors and slots and for preparing PCI hot plug adapters to be added, removed, or replaced:

- “Displaying PCI Hot-Plug Slot Information” on page 175
- “Unconfiguring Communications Adapters” on page 175
- “Unconfiguring Storage Adapters” on page 180
- “Unconfiguring Async Adapters” on page 181
- “Removing or Replacing a PCI Hot Plug Adapter” on page 182
- “Adding a PCI Hot Plug Adapter” on page 182

For additional information about hot plug management, see PCI Hot Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Displaying PCI Hot-Plug Slot Information

Before you add, remove, or replace a hot-plug adapter, you can display the following information about the PCI hot-plug slots in a machine:

- A list of all the PCI hot-plug slots in the machine
- Whether a slot is available or empty
- Slots that are currently in use
- The characteristics of a specific slot such as slot name, description, connector type, and the attached device name

You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

For additional information, see PCI Hot-Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about hot-plug slots and connected devices:

- The **lsslot** command displays a list of all the PCI hot-plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.

Unconfiguring Communications Adapters

Before you can remove or replace a hot-plug adapter, you must unconfigure that adapter. This section provides the following procedures for unconfiguring communications adapters:

- “Unconfiguring Ethernet, Token-ring, FDDI, and ATM Adapters” on page 176
- “Unconfiguring WAN Adapters” on page 177
- “Unconfiguring Other Adapters” on page 177

Unconfiguring a communications adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing or replacing
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter’s slot location
- Displaying and removing interface information from the network interface list
- Making the adapter unavailable

To perform these tasks, you must log in as **root**.

For additional information about unconfiguring communications adapters, see PCI Hot-Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Unconfiguring Ethernet, Token-ring, FDDI, and ATM Adapters

To unconfigure an Ethernet, Token-ring, FDDI, or ATM Adapter:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type the appropriate SMIT command, shown in the following examples, to list installed adapters and show the current state (see "Chapter 18. Devices" on page 163) of all the devices in the system unit:

`smit lsdenet`	To list Ethernet adapters
`smit lsdtok`	To list token-ring adapters
`smit ls_atm`	To list ATM adapters

   The following naming convention is used for the different type of adapters:

Name	**Adapter Type**
atm0, atm1, ...	ATM adapter
ent0, ent1, ...	Ethernet adapter
tok0, tok1, ...	Token Ring adapter

3. Close all applications that are using the adapter you are unconfiguring.
4. Type `netstat -i` to display a list of all configured interfaces and determine whether your adapter is configured for TCP/IP. Output similar to the following displays:

```
Name  Mtu    Network   Address        Ipkts  Ierrs  Opkts Oerrs Coll
lo0   16896  link#1                     076      0    118     0    0
lo0   16896  127       127.0.0.1        076      0    118     0    0
lo0   16896  ::1                        076      0    118     0    0
tr0    1492  link#2    8.0.5a.b8.b.ec   151      0    405    11    0
tr0    1492  19.13.97  19.13.97.106     151      0    405    11    0
at0    9180  link#3    0.4.ac.ad.e0.ad    0      0      0     0    0
at0    9180  6.6.6     6.6.6.5            0      0      0     0    0
en0    1500  link#5    0.11.0.66.11.1   212      0      1     0    0
en0    1500  8.8.8     8.8.8.106        212      0      1     0    0
```

   Token-ring adapters can have only one interface. Ethernet adapters can have two interfaces. ATM adapters can have multiple interfaces. For additional information, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

5. Type the appropriate ifconfig command, shown in the following examples, to remove the interface from the network interface list.

`ifconfig` *en0* `detach`
`ifconfig` *et0* `detach`
	To remove the standard Ethernet interface
	To remove the IEEE 802.3 Ethernet interface

`ifconfig` *tr0* `detach`	To remove a token-ring interface
`ifconfig` *at0* `detach`	To remove an ATM interface

   For an explanation of the association between these adapters and their interfaces, see Unconfiguring Communications adapters in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

6. Type the appropriate rmdev command, shown in the following examples, to unconfigure the adapter and *keep* its device definition in the Customized Devices Object Class:

`rmdev -l` *ent0*	To unconfigure an Ethernet adapter
`rmdev -l` *tok1*	To unconfigure a token-ring adapter
`rmdev -l` *atm1*	To unconfigure an ATM adapter

Note: To unconfigure the adapter and *remove* the device definition in the Customized Devices object class, you can use the rmdev command with the **-d** flag. *Do not* use the **-d** flag with the **rmdev** command for a hot-plug operation unless your intent is to remove the adapter and not replace it.

Unconfiguring WAN Adapters

To unconfigure a WAN Adapter:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type the appropriate SMIT command, shown in the following examples, to list installed adapters and show the current state of all the devices in the system unit:

`smit 331121b9_ls`	To list 2-Port Multiprotocol WAN adapters
`smit riciophx_ls`	To list ARTIC WAN adapters

The following naming convention is used for the different type of adapters:

Name	**Adapter Type**
dpmpa	2-Port Multiprotocol Adapter
riciop	ARTIC960 Adapter

3. Type `lsdev -C -c port` to list X.25 ports on your host. A message similar to the following displays:

```
sx25a0  Available 00-05-01-00     X.25 Port
x25s0   Available 00-05-01-00-00  V.3 X.25 Emulator
```

4. Close all applications that are using the adapter you are unconfiguring.
5. Remove an X.25 driver and port, following the steps in Configuration Commands in *AIXLink/X.25 1.1 for AIX: Guide and Reference*.
6. Use the commands in the following table to unconfigure and remove the device drivers and emulator ports for these adapters:

2-Port Multiprotocol adapter	
`smit rmhdlcdpmpdd`	To unconfigure the device
`smit rmsdlcscied`	To unconfigure the SDLC COMIO emulator

For additional information, see 2-Port Multiprotocol Adapter HDLC Network Device Driver Overview in the *AIX 5L Version 5.1 System Management Guide: Communications and Networks*.

ARTIC960Hx PCI adapter	
`smit rmtsdd`	To unconfigure the device driver
`smit rmtsdports`	To remove an MPQP COMIO emulation port

For additional information, see ARTIC960HX PCI Adapter Overview in the *AIX 5L Version 5.1 System Management Guide: Communications and Networks*.

Unconfiguring Other Adapters

This section includes procedures for unconfiguring adapters that require special handling.

IBM 4-Port 10/100 Base-TX Ethernet PCI Adapters

The 4-Port 10/100 Base-TX Ethernet PCI adapter has four ethernet ports and each port must be unconfigured before you can remove the adapter.

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.

2. Type `smit lsdenet` to list all the devices in the PCI subclass. A message similiar to the following displays:

```
ent1  Available 1N-00 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 1)
ent2  Available 1N-08 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 2)
ent3  Available 1N-10 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 3)
ent4  Available 1N-18 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 4)
```

3. Close all applications that are using the adapter you are unconfiguring.
4. Type `netstat -i` to display a list of all configured interfaces and determine whether your adapter is configured for TCP/IP. Output similar to the following displays:

```
Name  Mtu    Network   Address        Ipkts  Ierrs  Opkts Oerrs Coll
lo0   16896  link#1                     076      0    118     0    0
lo0   16896  127       127.0.0.1        076      0    118     0    0
lo0   16896  ::1                        076      0    118     0    0
tr0    1492  link#2    8.0.5a.b8.b.ec   151      0    405    11    0
tr0    1492  19.13.97  19.13.97.106     151      0    405    11    0
at0    9180  link#3    0.4.ac.ad.e0.ad    0      0      0     0    0
at0    9180  6.6.6     6.6.6.5            0      0      0     0    0
en0    1500  link#5    0.11.0.66.11.1   212      0      1     0    0
en0    1500  8.8.8     8.8.8.106        212      0      1     0    0
```

   Ethernet adapters can have two interfaces, for example, **et0** and **en0**. For additional information, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

5. Use the ifconfig command to remove each interface from the network interface list. For example, type `iconfig en0 detach` to remove the standard Ethernet interface, and type `iconfig et0` to remove the IEEE 802.3 interface. For an explanation of the association between these adapters and their interfaces, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.
6. Use the rmdev command to unconfigure the adapter amd retain its device definition in the Customized Devices Object Class. For example, `rmdev -l ent0`.

   > **Note:** To unconfigure the adapter and *remove* the device definition in the Customized Devices object class, you can use the rmdev command with the **-d** flag. *Do not* use the **-d** flag with the **rmdev** command for a hot-plug operation unless your intent is to remove the adapter and not replace it.

ATM Adapters

Classic IP and LAN emulation protocols can run over ATM adapters. LAN emulation protocol enables the implementation of emulated LANs over an ATM network. Emulated LANs can be Ethernet/IEEE 802.3, Token-ring/IEEE 802.5, and MPOA (MultiProtocol Over ATM). You must unconfigure each LAN-emulated device before you can remove the adapter.

For instructions for removing a classical interface, see “Unconfiguring Ethernet, Token-ring, FDDI, and ATM Adapters” on page 176. To remove a LAN interface, do the following:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type `smit ls_atm` to list all the ATM adapters. A message similiar to the following displays:

```
.
.
atm0 Available 04-04 IBM PCI 155 Mbps ATM Adapter (14107c00)
atm1 Available 04-06 IBM PCI 155 Mbps ATM Adapter (14104e00)
```

3. Type `smit listall_atmle` to list all the LAN-emulated clients on the adapters. A message similiar to the following displays:

```
ent1 Available  ATM LAN Emulation Client (Ethernet)
ent2 Available  ATM LAN Emulation Client (Ethernet)
ent3 Available  ATM LAN Emulation Client (Ethernet)
tok1 Available  ATM LAN Emulation Client (Token Ring)
tok2 Available  ATM LAN Emulation Client (Token Ring)
```

All ATM adapters can have multiple emulated clients running on them.

4. Type `smit listall_mpoa` to list all the LAN-emulated clients on the adapters. A message similar to the following displays:

   ```
   mpc0 Available     ATM LAN Emulation MPOA Client
   ```

   atm0 and *atm1* are the physical ATM adapters. *mpc0* is an MPOA-emulated client. *ent1, ent2, ent3, tok1,* and *tok2* are LAN-emulated clients.
5. Type entstat to determine on which adapter the client is running. A message similiar to the following displays:

   ```
   -------------------------------------------------------------
   ETHERNET STATISTICS (ent1) :
   Device Type: ATM LAN EmulationATM Hardware Address: 00:04:ac:ad:e0:ad
   .
   .
   .
   ATM LAN Emulation Specific Statistics:
   --------------------------------------
   Emulated LAN Name: ETHelan3
   Local ATM Device Name: atm0
   Local LAN MAC Address:
   .
   .
   ```
6. Close all applications that are using the adapter you are unconfiguring.
7. Use the rmdev -l *device* command to unconfigure the interfaces in the following order:
   - Emulated interface = en1, et1, en2, et2, tr1, tr2 ...
   - Emulated interface = ent1, ent2, tok1, tok2 ...
   - Multiprotocol Over ATM (MPOA) = mpc0
   - ATM adapter = atm0

Resolving Adapter-Removal Problems

If the following type of message displays when the **rmdev** command is to unconfigure an adapter, this indicates that the device is open, possibly because applications are still trying to access the adapter you are trying to remove or replace.

```
#rmdev -l ent0
Method error (/usr/lib/methods/ucfgent):
        0514-062
Cannot perform the requested function because the
specified device is busy.
```

To resolve the problem, you must identify any applications that are still using the adapter and close them. These applications can include the following:

- TCP/IP
- SNA
- OSI
- IPX/SPX
- Novell NetWare
- Streams
- The generic data link control (GDLC)
  - IEEE Ethernet DLC
  - Token-ring DLC
  - FDDI DLC

Systems Network Architecture (SNA) Applications

Some SNA applications that may be using your adapter include:

- DB2
- TXSeries (CICS & Encina)
- DirectTalk
- MQSeries
- HCON
- ADSM

Streams Applications

Some of the streams-based applications that may be using your adapter include:

- IPX/SPX
- Novell NetWare V4 and Novell NetWare Services 4.1
- Connections and NetBios for this operating system

Applications Running on WAN Adapters

Applications that may be using your WAN adapter include:

- SDLC
- Bisync
- X.25
- ISDN
- QLLC for X.25

TCP/IP Applications

All TCP/IP applications using the interface layer can be detached with the ifconfig command. This causes the applications using TCP/IP to time out and warn users that the interface is down. After you add or replace the adapter and run the **ifconfig** command to attach the interface, the applications resume.

Unconfiguring Storage Adapters

This section provides steps for unconfiguring SCSI, SSA, and Fibre Channel storage adapters.

Before you can remove or replace a storage adapter, you must unconfigure that adapter. Unconfiguring a storage adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing, replacing, or moving
- Unmounting file systems
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter's slot location
- Making parent and child devices unavailable
- Making the adapter unavailable

To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Unconfiguring SCSI, SSA, and Fibre Channel Adapters

Storage adapters are generally parent devices to media devices, such as disk or tape drives. Removing the parent requires that all attached child devices either be removed or placed in the define state.

To unconfigure SCSI, SSA, and Fibre Channel Adapters:

1. Close all applications that are using the adapter you are unconfiguring.
2. Type `lsslot-c pci` to list all the hot plug slots in the system unit and display their characteristics.
3. Type `lsdev -C` to list the current state of all the devices in the system unit.
4. Type `umount` to unmount previously mounted file systems, directories, or files using this adapter. For additional information, see “Mounting or Unmounting a File System” on page 65 in the *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*.
5. Type `rmdev -l adapter -R` to make the adapter unavailable.

   Attention: Do *not* use the `-d` flag with the **rmdev** command for hot plug operations because this will cause your configuration to be removed.

Unconfiguring Async Adapters

This section provides steps for unconfiguring async adapters.

Before you can remove or replace an async adapter, you must unconfigure that adapter. Unconfiguring an async adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing, replacing, or moving
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter’s slot location
- Making parent and child devices unavailable
- Making the adapter unavailable

To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Unconfiguring Async Adapters

Before you can replace or remove an async adapter, you must unconfigure the adapter and all the devices controlled by that adapter. To unconfigure the devices, you must terminate all the processes using those devices. Use the following steps:

1. Close all applications that are using the adapter you are unconfiguring.
2. Type `lsslot-c pci` to list all the hot plug slots in the system unit and display their characteristics.
3. Type `lsdev -C -c tty` to list all available tty devices and the current state of all the devices in the system unit. For additional information, see Removing a TTY in the *AIX 5L Version 5.1 Asynchronous Communications Guide*.
4. Type `lsdev -C -c printer` to list all printer and plotter devices connected to the adapter. For additional information, see Printers, Print Jobs, and Queues for System Administrators in the *AIX 5L Version 5.1 Guide to Printers and Printing*.
5. Use the rmdev command to make the adapter unavailable.

   Attention: Do *not* use the `-d` flag with the **rmdev** command for hot plug operations because this will cause your configuration to be removed.

Removing or Replacing a PCI Hot Plug Adapter

This section provides procedures for removing a PCI hot plug adapter. You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

You can remove or replace a PCI hot plug adapter from the system unit without shutting down the operating system or turning off the system power. Removing an adapter makes the resources provided by that adapter unavailable to the operating system and applications.

Replacing an adapter with another adapter of the same type retains the replaced adapter's configuration information and compares the information to the card that replaces it. The existing device driver of the replaced adapter must be able to support the replacement adapter.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

Prerequisites

Before you can remove an adapter, you must unconfigure it. See Unconfiguring Communications Adapters, Unconfiguring Storage Adapters, or Unconfiguring Async Adapters for instructions for unconfiguring adapters.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about hot plug slots and connected devices and to remove a PCI hot plug adapter:

- The **lsslot** command displays a list of all the PCI hot plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.
- The **drslot** command prepares a hot plug slot for removal of a hot plug adapter. For information about using this command, see drslot in the *AIX 5L Version 5.1 Commands Reference, Volume 2*.

For information about the physical handling of a PCI hot plug adapter, refer to your system unit documentation.

Adding a PCI Hot Plug Adapter

This section provides procedures for adding a new PCI hot plug adapter.

Attention: Before you attempt to add PCI hot plug adapters, refer to the *PCI Adapter Placement Reference*, shipped with system units that support hot plug, to determine whether your adapter can be hot plugged. Refer to your system unit documentation for instructions for installing or removing adapters.

You can add a PCI hot plug adapter into an available slot in the system unit and make new resources available to the operating system and applications without having to reboot the operating system. The adapter can be another adapter type that is currently installed or it can be a different adapter type.

Adding a new PCI hot plug adapter involves the following tasks:

- Finding and identifying an available slot in the machine
- Preparing the slot for configuring the adapter
- Installing the device driver, if necessary
- Configuring the new adapter

You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

> **Note:** When you add a hot plug adapter to the system, that adapter and its child devices might not be available for specification as a boot device using the **bootlist** command. You might be required to reboot your system to make all potential boot devices known to the operating system.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about PCI hot plug slots and connected devices and to add a PCI hot plug adapter:

- The **lsslot** command displays a list of all the hot plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.1 Commands Reference, Volume 3*.
- The **drslot** command prepares a hot plug slot for adding or removing a hot plug adapter. For information about using this command, see drslot in the *AIX 5L Version 5.1 Commands Reference, Volume 2*.

For information about installing or removing adapters, refer to your system unit documentation.

Working with Device Problems

Use the following procedures to determine the cause problems with devices on your operating system:

1. “Check the Device Software”
2. “Check the Device Hardware” on page 185

Check the Device Software

Correct a device software problem by:

- “Checking the Error Log” on page 184

- “Listing All Devices”
- “Checking the State of a Device”
- “Checking the Attributes of a Device”
- “Changing the Attributes of a Device”
- “Using a Device with Another Application” on page 185
- “Defining a New Device” on page 185

Checking the Error Log

Check the error log to see whether any errors are recorded for either the device, its adapter, or the application using the device. Go to Error Logging Facility for information about performing this check. Return to this step after completing the procedures.

Did you correct the problem with the device?

If you were not able to correct the correct the problem using the previous method, go to the next step, “Listing All Devices”.

Listing All Devices

Use the **lsdev -C** command to list all defined or available devices. This command shows the characteristics of all the devices in your system.

If the device is in the list of devices, go to the next step, “Checking the State of a Device”.

If the device is not in the list of devices, go to “Defining a New Device” on page 185.

Checking the State of a Device

Find the device in the list generated from the **lsdev -C** command. Check whether the device is in the Available state.

If the device is in the Available state, go to the next step, “Checking the Attributes of a Device”.

If the device is not in the Available state, go to “Defining a New Device” on page 185.

Checking the Attributes of a Device

Use the **lsattr -E -l** *DeviceName* command to list the attributes of your device.

The **lsattr** command shows attribute characteristics and possible values of attributes for devices in the system. Refer to the documentation for the specific device for the correct settings.

If the device attributes are set correctly, go to “Using a Device with Another Application” on page 185.

If the device attributes are not set correctly, go to the next step, “Changing the Attributes of a Device”.

Changing the Attributes of a Device

Use the **chdev -l** *Name* **-a** *Attribute***=***Value* command to change device attributes. Before you run this command, refer to *AIX 5L Version 5.1 Commands Reference*.

The **chdev** command changes the characteristics of the device you specify with the **-l** *Name* flag.

If changing the attributes did not correct the problem with the device, go to the next step, “Using a Device with Another Application” on page 185.

Using a Device with Another Application

Try using the device with another application. If the device works correctly with another application, there might be a problem with the first application.

If the device worked correctly with another application, you might have a problem with the first application. Report the problem to your software service representative.

If the device did not work correctly with another application, go to the next step, “Defining a New Device”.

Defining a New Device

> **Note:** You must either have root user authority or be a member of the security group to use the **mkdev** command.

Use the **mkdev** command to add a device to the system.

The **mkdev** command can either define and make available a new device or make available a device that is already defined. You can uniquely identify the predefined device by using any combination of the **-c**, **-s**, and **-t** flags. Before you run this command, refer to the *AIX 5L Version 5.1 Commands Reference*.

If defining the device did not correct the problem, You can either stop and report the problem to your service representative or use a diagnostics program to test your device.

Check the Device Hardware

Correct a device hardware problem by using the following procedures:

- “Checking the Device Connections”
- “Checking the Ready State of a Device”
- “Running Diagnostics on a Device” on page 186

Checking the Device Connections

Follow these steps to check your device connections:

1. Check that power is available at the electrical outlet.
2. Check that the device power cable is correctly attached to the device and to the electrical outlet.
3. Check that the device signal cable is attached correctly to the device and to the correct connection on the system unit.
4. For SCSI devices, check that the SCSI terminator is correctly attached and the SCSI address setting is correct.
5. For communications devices, check that the device is correctly attached to the communications line.
6. Check that the device is turned on.

Refer to the documentation for the specific device for cabling and configuring procedures and for further troubleshooting information.

If your check of the device connections have not corrected the problem. Go to the next step, “Checking the Ready State of a Device”

Checking the Ready State of a Device

To determine whether the device is in a ready state, do the following:

1. Check that the device’s Ready indicator is on.
2. Check that removable media, such as tape, diskette, and optical devices, are inserted correctly.

3. Check the ribbon, the paper supply, and the toner supply for printers and plotters.
4. Check that the write medium is write-enabled if you are trying to write to the device.

Did your checks correct the problem with the device?

If your check of the device's ready state did not correct the problem, go to the next step, "Running Diagnostics on a Device"

Running Diagnostics on a Device

You might have a defective device. Run your hardware diagnostics.

If running hardware diagnostics fails to find a problem with your device, go to "Check the Device Software" on page 183 If your device passes the diagnostic tests, you might have a problem with the way your device works with your system software. If it is possible that the preceding problem exists, report the problem to your software service organization.

Chapter 19. Tape Drives

This chapter covers system management functions related to tape drives. Many of these functions change or get information from the device configuration database that contains information about the devices on your system. The device configuration database consists of the predefined configuration database that contains information about all possible types of devices supported on the system, and the customized configuration database that contains information about the particular devices currently on the system. For the operating system to make use of a tape drive, or any other device, the device must be defined in the customized configuration database and must have a device type defined in the predefined configuration database.

Basic tasks for Tape Drives are shown in the following table:

Tape Drive Tasks		
Task	*SMIT Fast Path*	*Command or File*
List All Defined Tape Drives	**smit lsdtpe**	**lsdev -C -c tape -H**
List All Supported Tape Drives	**smit lsstpe**	**lsdev -P -c tape -F** ″***type subclass description***″ **-H**
Add New Tape Drives Automatically	**smit cfgmgr**	**cfgmgr**
Add a User-Specified Tape Drive	**smit addtpe**	**mkdev -c tape -t ’8mm’ -s ’scsi’ -p ’scsi0’ -w ’4,0’ -a extfm=yes**
Show Characteristics of a Tape Drive	**smit chgtpe**	**lsdev -C -l rmt0** **lsattr -D -l rmt0***
Change Attributes of a Tape Drive	**smit chgtpe**	**chdev -l rmt0 -a block_size=’512’ -a mode=no***
Remove a Tape Drive	**smit rmvtpe**	**rmdev -l ’rmt0’***
Generate an Error Report for a Tape Drive	**smit errpt**	See Error Logging Tasks in *Messages Guide and Reference*.
Trace a Tape Drive	**smit trace_link**	See Starting the Trace Facility in in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

Note:
* Where `rmt0` is the logical name of a tape drive.

Tape Drive Attributes

The following describes tape drive attributes you can adjust to meet the needs of your system. The attributes can be displayed or changed using the Web-based System Manager Devices application, SMIT, or commands (in particular, the **lsattr** and the **chdev** commands).

Each type of tape drive only uses a subset of all the attributes.

General Information about Each Attribute

Block Size

The block size attribute indicates the block size to use when reading or writing the tape. Data is written to tape in blocks of data, with inter-record gaps between blocks. Larger records are useful when writing to unformatted tape, because the number of inter-record gaps is reduced across the tape, allowing more data to be written. A value of **0** indicates variable length blocks. The allowable values and default values vary depending on the tape drive.

Device Buffers

Setting the Device Buffers attribute (the **mode** attribute for the **chdev** command) to the Yes value indicates an application is notified of write completion after the data has been transferred to the data buffer of the tape drive, but not necessarily after the data is actually written to the tape. If you specify the No value, an application is notified of write completion only after the data is actually written to the tape. Streaming mode cannot be maintained for reading or writing if this attribute is set to the No value. The default value is Yes.

With the No value, the tape drive is slower but has more complete data in the event of a power outage or system failure and allows better handling of end-of-media conditions.

Extended File Marks

Setting the Extended File Marks attribute (the **extfm** attribute for the **chdev** command) to the No value writes a regular file mark to tape whenever a file mark is written. Setting this attribute to the Yes value writes an extended file mark. For tape drives, this attribute can be set on. The default value is No. For example, extended filemarks on 8 mm tape drives use 2.2 MB of tape and can take up to 8.5 seconds to write. Regular file marks use 184 K and take approximately 1.5 seconds to write.

When you use an 8 mm tape in append mode, use extended file marks for better positioning after reverse operations at file marks. This reduces errors.

Retension

Setting the Retension attribute (the **ret** attribute for the **chdev** command) to Yes instructs the tape drive to retension a tape automatically whenever a tape is inserted or the drive is reset. *Retensioning* a tape means to wind to the end of the tape and then rewind to the beginning of the tape to even the tension throughout the tape. Retensioning the tape can reduce errors, but this action can take several minutes. If you specify the No value, the tape drive does not automatically retension the tape. The default value is Yes.

Density Setting #1 and Density Setting #2

Density Setting #1 (the **density_set_1** attribute for the **chdev** command) sets the density value that the tape drive writes when using special files **/dev/rmt***, **/dev/rmt*.1**, **/dev/rmt*.2**, and **/dev/rmt*.3**. Density Setting #2 (for the **density_set_2** attribute of the **chdev** command) sets the density value that the tape drive writes when using special files **/dev/rmt*.4**, **/dev/rmt*.5**, **/dev/rmt*.6**, and **/dev/rmt*.7**. See “Special Files for Tape Drives” on page 197 for more information.

The density settings are represented as decimal numbers in the range 0 to 255. A zero (0) setting selects the default density for the tape drive, which is usually the drive’s high density setting. Specific permitted values and their meanings vary with different types of tape drives. These attributes do not affect the ability of the tape drive to read tapes written in all densities supported by the tape drive. It is customary to set Density Setting #1 to the highest density possible on the tape drive and Density Setting #2 to the second highest density possible on the tape drive.

Reserve Support

For tape drives that use the Reserve attribute (the **res_support** attribute for the **chdev** command), specifying the Yes value causes the tape drive to be reserved on the SCSI bus while it is open. If more than one SCSI adapter shares the tape device, this ensures access by a single adapter while the device is open. Some SCSI tape drives do not support the reserve or release commands. Some SCSI tape drives have a predefined value for this attribute so that the reserve and release commands are always supported.

Variable Length Block Size

The Variable Length Block Size attribute (the **var_block_size** attribute for the **chdev** command) specifies the block size required by the tape drive when writing variable length records. Some SCSI tape drives require that a nonzero block size be specified in their Mode Select data even when writing variable length records. The Block Size attribute is set to 0 to indicate variable length records. Refer to the specific tape drive SCSI specification to determine whether this is required.

Data Compression

Setting the Data Compression attribute (the **compress** attribute for the **chdev** command) to Yes causes the tape drive to be in compress mode, if the drive is capable of compressing data. If so, then the drive writes data to the tape in compressed format so that more data fits on a single tape. Setting this attribute to No forces the tape drive to write in native mode (noncompressed). Read operations are not affected by the setting of this attribute. The default setting is Yes.

Autoloader

Setting the Autoloader attribute (the **autoload** attribute for the **chdev** command) to Yes causes Autoloader to be active, if the drive is so equipped. If so, and another tape is available in the loader, any read or write operation that advances the tape to the end is automatically continued on the next tape. Tape drive commands that are restricted to a single tape cartridge are unaffected. The default setting is Yes.

Retry Delay

The Retry Delay attribute sets the number of seconds that the system waits after a command has failed before reissuing the command. The system may reissue a failed command up to four times. This attribute applies only to type ost tape drives. The default setting is 45.

Read/Write Timeout

The Read/Write Timeout or Maximum Delay for a READ/WRITE attribute sets the maximum number of seconds that the system allows for a read or write command to complete. This attribute applies only to type ost tape drives. The default setting is 144.

Return Error on Tape Change

The Return Error on Tape Change or Reset attribute, when set, causes an error to be returned on open when the tape drive has been reset or the tape has been changed. A previous operation to the tape drive must have taken place that left the tape positioned beyond beginning of tape upon closing. The error returned is a -1 and **errno** global value is set to **EIO**. After being presented to the application, the error condition is cleared. Also, reconfiguring the tape drive itself clears the error condition.

Attributes for 2.0 GB 4 mm Tape Drives (Type 4mm2gb)

Block Size

The default value is 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values

If a tape drive is configured as a 2.0 GB 4 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Density Setting #1, and Density Setting #2 attributes have predefined values that cannot be changed. The density settings are predefined because the tape drive always writes in 2.0 GB mode.

Attributes for 4.0 GB 4 mm Tape Drives (Type 4mm4gb)

Block Size

The default value is 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The user cannot change the density setting of this drive; the device reconfigures itself automatically depending on the Digital Data Storage (DDS) media type installed, as follows:

<table>
<tr><th>Media Type</th><th>Device Configuration</th></tr>
<tr><td>DDS</td><td>Read-only.</td></tr>
<tr><td>DDS ||||</td><td>Read/write in 2.0 GB mode only.</td></tr>
<tr><td>DDS2</td><td>Read in either density; write in 4.0 GB mode only.</td></tr>
<tr><td>non-DDS</td><td>Not supported; cartridge will eject.</td></tr>
</table>

Data Compression

The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values

If a tape drive is configured as a 4.0 GB 4 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Density Setting #1, and Density Setting #2 attributes have predefined values that cannot be changed.

Attributes for 2.3 GB 8 mm Tape Drives (Type 8mm)

Block Size

The default value is 1024. A smaller value reduces the amount of data stored on a tape.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values

If a tape drive is configured as a 2.3 GB 8 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Data Compression, Density Setting #1, and Density Setting #2 attributes have predefined values which cannot be changed. The density settings are predefined because the tape drive always writes in 2.3 GB mode.

Attributes for 5.0 GB 8 mm Tape Drives (Type 8mm5gb)

Block Size

The default value is 1024. If a tape is being written in 2.3 GB mode, a smaller value reduces the amount of data stored on a tape.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
140	5 GB mode (compression capable)
21	5 GB mode noncompressed tape
20	2.3 GB mode
0	Default (5.0 GB mode)

The default values are 140 for Density Setting #1, and 20 for Density Setting #2. A value of 21 for Density Setting #1 or #2 permits the user to read or write a noncompressed tape in 5 GB mode.

Data Compression

The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values

If a tape drive is configured as a 5.0 GB 8 mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 20000 MB 8mm Tape Drives (Self-Configuring)

Block Size

The default value is 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The drive can read and write data cartridges in 20.0 GB format. During a Read command, the drive automatically determines which format is written on tape. During a Write, the Density Setting determines which data format is written to tape.

The following settings apply:

Setting	Meaning
39	20 GB mode (compression capable)
0	Default (20.0 GB mode)

The default value is **39** for Density Setting #1 and Density Setting #2.

Data Compression

The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values

If a tape drive is configured as a 20.0 GB 8 mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 35 GB Tape Drives (Type 35gb)

Block Size

The IBM 7205 Model 311 throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32 K Bytes. Any block size less than 32 K Bytes restricts the data rate (backup and restore time). The following table lists recommended block sizes by command:

Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32 K or 51.2 K (default)	Uses either 32 K or 51.2 K depending on if ″Backup″ is by name or not. No change is required.
TAR	10 K	There is an error in the manual that states a 512 K byte block size. Set the Blocking Parameter to *-N64*.
MKSYSB	See BACKUP	MKSYSB uses the BACKUP Command. No change is required.
DD	n/a	Set the Blocking Parameter to *bs=32K*.
CPIO	n/a	Set the Blocking Parameter to *-C64*.

Note: Be aware of the capacity and throughput when you select a blocksize. Small blocksizes have a significant impact on performance and a minimal impact on capacity. The capacities of the 2.6 GB format (density) and 6.0 GB format (density) are significantly impacted when you use smaller than the recommended blocksizes. As an example: using a blocksize of 1024 bytes to backup 32 GB of data takes approximately 22 hours. Backing up the same 32 GB of data using a blocksize of 32 K Bytes takes approximately 2 hours.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following chart shows the Supported Data Cartridge type and Density Settings (in decimal and hex) for the IBM 7205-311 Tape Drive. When you perform a Restore (Read) Operation, the tape drive automatically sets the density to match the written density. When you perform a Backup Operation (Write), you must set the Density Setting to match the Data Cartridge that you are using.

Supported Data Cartridges	Native Capacity	Compressed Data Capacity	Web-based System Manager or SMIT Density Setting	HEX Density Setting
DLTtape III	2.6 GB	2.6 GB (No Compression)	23	17h
	6.0 GB	6.0 GB (No Compression)	24	18h
	10.0 GB	20.0 GB (Default for drive)	25	19h
DLTtapeIIIxt	15.0 GB	30.6 GB (Default for drive)	25	19h
DLTtapeIV	20.0 GB	40.0 GB	26	1Ah
	35.0 GB	70.0 GB (Default for drive)	27	1Bh

Note: If you request an unsupported Native Capacity for the Data Cartridge, the drive defaults to the highest supported capacity for the Data Cartridge that is loaded into the drive.

Data Compression

The actual compression depends on the type of data being that is being written (see previous table). A Compression Ratio of 2:1 is assumed for this Compressed Data Capacity.

Attributes with Fixed Values

The general information for this attribute applies to this tape drive type.

Attributes for 150 MB 1/4-Inch Tape Drives (Type 150mb)

Block Size

The default block size is 512. The only other valid block size is 0 for variable length blocks.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
16	QIC-150
15	QIC-120
0	Default (QIC-150), or whatever was the last density setting by a using system.

The default values are 16 for Density Setting #1, and 15 for Density Setting #2.

Attributes with Fixed Values

If a tape drive is configured as a 150 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 525 MB 1/4-Inch Tape Drives (Type 525mb)

Block Size

The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you want to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
17	QIC-525*
16	QIC-150
15	QIC-120
0	Default (QIC-525), or whatever was the last density setting by a using system.

* QIC-525 is the only mode that supports the 1024 block size.

The default values are 17 for Density Setting #1, and 16 for Density Setting #2.

Attributes with Fixed Values

If a tape drive is configured as a 525 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 1200 MB 1/4-Inch Tape Drives (Type 1200mb-c)

Block Size

The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
21	QIC-1000*
17	QIC-525*
16	QIC-150
15	QIC-120
0	Default (QIC-1000), or whatever was the last density setting by a using system.

* QIC-525 and QIC-1000 are the only modes that support the 1024 block size.

The default values are 21 for Density Setting #1, and 17 for Density Setting #2.

Attributes with Fixed Values

If a tape drive is configured as a 1200 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 12000 MB 4 mm Tape Drives (Self-Configuring)

Block Size

The IBM 12000 MB 4 mm Tape Drive’s throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32 K Bytes. Any block size less than 32 K Bytes restricts the data rate (backup/restore time). The following table lists recommended block sizes by command:

Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32 K or 51.2 K (default)	Will use either 32 K or 51.2 K depending on if ″Backup″ is by name or not. No change is required.
TAR	10 K	There is an error in the manual that states a 512 K byte block size. Set the Blocking Parameter to **-N64**.
MKSYSB	See BACKUP	MKSYSB uses the BACKUP Command. No change is required.
DD	n/a	Set the Blocking Parameter to **bs=32K**.
CPIO	n/a	Set the Blocking Parameter to **-C64**.

Note: You should be aware of the capacity and throughput when you select a blocksize. Small blocksizes have a significant impact on performance and a minimal impact on capacity.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following chart shows the Supported Data Cartridge type and Density Settings (in decimal and hex) for the IBM 12000 MB 4 mm Tape Drive. When you perform a Restore (Read) Operation, the tape drive automatically sets the density to match the written density. When you perform a Backup Operation (Write), you must set the Density Setting to match the Data Cartridge you are using.

Supported Data Cartridges	Native Capacity	Compressed Data Capacity	Web-based System Manager or SMIT Density Setting	HEX Density Setting
DDS III	2.0 GB	4.0 GB	19	13h
DDS2	4.0 GB	8.0 GB	36	24h
DDS3	12.0 GB	24.0 GB	37	25h

Note: If you request an unsupported Native Capacity for the Data Cartridge, the drive defaults to the highest supported capacity for the Data Cartridge that is loaded into the drive.

Data Compression

The actual compression depends on the type of data being that is being written (see the previous table). A Compression Ratio of 2:1 is assumed for this Compressed Data Capacity.

Attributes with Fixed Values

The general information for this attribute applies to this tape drive type.

Attributes for 13000 MB 1/4-Inch Tape Drives (Self-Configuring)

Block Size

The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
33	QIC-5010-DC*
34	QIC-2GB*
21	QIC-1000*
17	QIC-525*
16	QIC-150

Setting	Meaning
15	QIC-120
0	Default (QIC-5010-DC)*

* QIC-525, QIC-1000, QIC-5010-DC, and QIC-2GB are the only modes that support the 1024 block size.

The default values are 33 for Density Setting #1, and 34 for Density Setting #2.

Attributes with Fixed Values

If a tape drive is configured as a 13000 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 1/2-Inch 9-Track Tape Drives (Type 9trk)

Block Size

The default block size is 1024.

Device Buffers

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The following settings apply:

Setting	Meaning
3	6250 bits per inch (bpi)
2	1600 bpi
0	Whichever writing density was used previously.

The default values are 3 for Density Setting #1, and 2 for Density Setting #2.

Attributes with Fixed Values

If a tape drive is configured as a 1/2-inch 9-track tape drive, the Extended File Marks, Retension, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 3490e 1/2-Inch Cartridge (Type 3490e)

Block Size

The default block size is 1024. This drive features a high data transfer rate, and block size can be critical to efficient operation. Larger block sizes can greatly improve operational speeds, and in general, the largest possible block size should be used.

> **Note:** Increasing the block value can cause incompatibilities with other programs on your system. If this occurs, you receive the following error message while running those programs:

```
A system call received a parameter that is not valid.
```

Device Buffers

The general information for this attribute applies to this tape drive type.

Compression

The general information for this attribute applies to this tape drive type.

Autoloader

This drive features a tape sequencer, an autoloader that sequentially loads and ejects a series of tape cartridges from the cartridge loader. For this function to operate correctly, the front panel switch must be in the AUTO position and the Autoloader attribute must be set to Yes.

Attributes for Other SCSI Tapes (Type ost)

Block Size

The system default is 512, but this should be adjusted to the default block size for your tape drive. Typical values are 512 and 1024. 8 mm and 4 mm tape drives usually use 1024 and waste space on the tape if the block size attribute is left at 51. 0 indicates variable block size on some drives.

Device Buffers

The general information for this attribute applies to this tape drive type.

Extended File Marks

The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2

The default value is 0 for both of these settings. Other values and their meanings vary for different tape drives.

Reserve Support

The default value is No. This may be set to Yes, if the drive supports reserve/release commands. If you are unsure, No is a safer value.

Variable Length Block Size

0 is the default value. Nonzero values are used primarily on quarter inch cartridge (QIC) drives. Refer to the SCSI specification for the particular tape drive for advice.

Retry Delay

This attribute applies exclusively to type ost tape drives

Read/Write Timeout

This attribute applies exclusively to type ost tape drives

Attributes with Fixed Values

If a tape drive is configured as an Other SCSI tape drive, the Extended File Marks, Retension, and Data Compression attributes have predefined values which cannot be changed.

Special Files for Tape Drives

Writing to and reading from files on tapes is done by using **rmt** special files. There are several special files associated with each tape drive known to the operating system. These special files are **/dev/rmt***, **/dev/rmt*.1**, **/dev/rmt*.2**, ... **/dev/rmt*.7**. The **rmt*** is the logical name of a tape drive, such as **rmt0**, **rmt1**, and so on.

By selecting one of the special files associated with a tape drive, you make choices about how the I/O operations related to the tape drive will be performed.

Density
You can select whether to write with the tape drive Density Setting #1 or with the tape drive Density Setting #2. The values for these density settings are part of the attributes of the tape drive. Because it is customary to set Density Setting #1 to the highest possible density for the tape drive and Density Setting #2 to the next highest possible density for the tape drive, special files that use Density Setting #1 are sometimes referred to as high density and special files that use Density Setting #2 sometimes are referred to as low density, but this view is not always correct. When reading from a tape, the density setting is ignored.

Rewind-on-Close
You can select whether the tape is rewound when the special file referring to the tape drive is closed. If rewind-on-close is selected, the tape is positioned at the beginning of the tape when the file is closed.

Retension-on-Open You can select whether the tape is retensioned when the file is opened. Retensioning means winding to the end of the tape and then rewinding to the beginning of the tape to reduce errors. If retension-on-open is selected, the tape is positioned at the beginning of the tape as part of the open process.

The following table shows the names of the **rmt** special files and their characteristics.

Special File	Rewind on Close	Retension on Open	Density Setting
/dev/rmt*	Yes	No	#1
/dev/rmt*.1	No	No	#1
/dev/rmt*.2	Yes	Yes	#1
/dev/rmt*.3	No	Yes	#1
/dev/rmt*.4	Yes	No	#2
/dev/rmt*.5	No	No	#2
/dev/rmt*.6	Yes	Yes	#2
/dev/rmt*.7	No	Yes	#2

Suppose you want to write three files on the tape in tape drive **rmt2**. The first file is to be at the beginning of the tape, the second file after the first file, and the third file after the second file. Further, suppose you want Density Setting #1 for the tape drive. The following list of special files, in the order given, could be used for writing the tape.

Appendix. Notices

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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.

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.
Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.
The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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.

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.

Index

Readers' Comments — We'd Like to Hear from You

AIX 5L Version 5.1
System Management Guide:
Operating System and Devices

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM Corporation
Publications Department
Internal Zip 9561
11400 Burnet Road
Austin, TX
78758-3493

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A