Bull

AIX 4.3 System Management Guide
Operating System and Devices

AIX

ORDER REFERENCE
86 A2 99HX 04

Bull

AIX 4.3 System Management Guide
Operating System and Devices

AIX

Software

May 2000

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 99HX 04

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this book.

AIX® is a registered trademark of International Business Machines Corporation, and is being used under licence.

UNIX is a registered trademark in the United States of America and other countries licensed exclusively through the Open Group.

Year 2000

The product documented in this manual is Year 2000 Ready.

About This Book

This book contains information about the major tasks that you perform in your day–to–day life as a system administrator and the tools that AIX provides for system management.

Note: You can also find the information in this book on the ”Hypertext Library for AIX 4.3” CD-ROM. This online documentation is designed for use with an HTML version 3.2 compatible web browser.

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 4.3 System Management Concepts: Operating System and Devices*, 86 A2 21KX
- *AIX 4.3 System User’s Guide: Operating System and Devices*, 86 A2 97HX
- *AIX 4.3 System User’s Guide: Communications and Networks*, 86 A2 98HX
- *AIX 4.3 Installation Guide*, 86 A2 43GX

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

Note: The troubleshooting sections are helpful when you know the cause of your problem. If you encounter a problem for which you do not know the cause, refer to the *AIX Version 4.3 Problem Solving Guide and Reference*.

For conceptual information about system management tasks, see the *AIX 4.3 System Management Concepts: Operating System and Devices*.

Overview of Contents

This book contains the following chapters and appendixes:

- Chapter 1, ”Starting and Stopping the System,” contains procedural information to guide you through the tasks of starting and stopping the system.
- Chapter 2, ”Security,” introduces the security features, including the Trusted Computing Base (TCB), the **virscan** command that detects viruses, auditing, and access control.
- Chapter 3, ”Administrative Roles,” contains procedural information for setting up and maintaining roles and authorizations.
- Chapter 4, ”Managing Users and Groups,” provides step–by–step information for managing users and groups of users.
- Chapter 5, ”Logical Volumes,” contains procedures for managing logical volume storage.

- Chapter 6, ”File Systems,” contains in–depth procedures for managing files, directories, and file systems.
- Chapter 7, ”Paging Space and Virtual Memory,” covers how to create and maintain paging space for your system.
- Chapter 8, ”Backup and Restore,” introduces the commands used to save your data and restore it from backup.
- Chapter 9, ”System Environment,” provides steps for managing the basic environment components. Included are instructions that explain how to change the message of the day, broadcast messages to users, and work with profiles.
- Chapter 10, ”National Language Support,” introduces tasks for managing a system in various languages and time zones.
- Chapter 11, ”Process Management,” provides information about using system processes.
- Chapter 12, ”Workload Management,” introduces tasks for managing system resources.
- Chapter 13, ”System Resource Controller and Subsystems,”covers ways to use the controller.
- Chapter 14, ”System Accounting,” introduces the wide array of system accounting commands and subroutines.
- Chapter 15, ”Setting Up and Running Web-based System Manager” describes how to set up and run Web-based System Manager in both stand–alone and Client–Server environments.
- Chapter 16, ”System Management Interface Tool,” describes how to use the System Management Interface Tool (SMIT). SMIT is a command–building user interface that assists the system manager in constructing and recreating many system management tasks. The interface can be used in an ASCII or windows environment.
- Chapter 17, ”Managing the CDE Desktop,” provides detailed instructions for starting, stopping, disabling and enabling the CDE Desktop, and customizing display devices for CDE Desktop.
- Chapter 18, ”Documentation Search Service,” provides information for installing and configuring the Documentation Search Service, which allows you to search online HTML documents on your documentation server that have been indexed. Also covered is how to create your own indexes to search user created documents.
- Chapter 19, ”Using Power Management,” includes procedures for utilizing the technique of power management.
- Chapter 20, ”Devices,” provides procedures for managing a wide range of devices.
- Chapter 21, ”Tape Drives,” provides procedures for managing tape drives.

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.

Other Key Sources of System Management Information

Publications Covering Other Aspects of System Management

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.

The following books cover other key topics of interest to you:

- *AIX 4.3 System Management Guide: Communications and Networks*, 86 A2 31JX, covers network administration and maintenance.
- *AIX 4.3 Installation Guide*, 86 A2 43GX
- Problem Solving and Messages:
  - *AIX Version 4.3 Problem Solving Guide and Reference*, 86 A2 32JX
  - *AIX Messages Guide and Reference*, 86 A2 33JX
- *AIX General Programming Concepts: Writing and Debugging Programs*, 86 A2 34JX, introduces you to the programming tools and interfaces available for writing and debugging application programs.
- *AIX Communications Programming Concepts*, 86 A2 35JX, provides conceptual and procedural information about various communications programming tools.
- *AIX Files Reference*, 86 A2 79AP.
- Monitoring and tuning system performance:
  - *AIX Performance Tuning Guide*, 86 A2 72AP, describes the performance monitoring and tuning tools available with the base operating system.
  - *Performance Toolbox 1.2 and 2.1 for AIX: User's Guide*, 86 A2 10AQ, describes the additional monitoring tools available with Performance Toolbox for AIX.
- *AIX 4.3 Network Installation Management Guide and Reference*, 86 A2 17HX, covers configuration and maintenance of diskless workstations.
- *Distributed SMIT 2.2 for AIX: Guide and Reference*, 86 A2 09AQ, covers information about the Distributed System Management Interface Tool (DSMIT).
- *Common Desktop Environment 1.0: Advanced User's and System Administrator's Guide*, 86 A2 85AT, covers advanced tasks in customizing the appearance and behavior of the Common Desktop Environment (CDE).

AIX Support for the X/Open UNIX95 Specification

Beginning with AIX Version 4.2, the operating system is designed to support the X/Open UNIX95 Specification for portability of UNIX–based operating systems. Many new interfaces, and some current ones, have been added or enhanced to meet this specification. Beginning with Version 4.2, AIX is even more open and portable for applications.

At the same time, compatibility with previous AIX releases is preserved. This is accomplished by the creation of a new environment variable, which can be used to set the system environment on a per–system, per–user, or per–process basis.

To determine the proper way to develop a UNIX95–portable application, you may need to refer to the X/Open UNIX95 Specification, which can be obtained on a CD–ROM by ordering the printed copy of *AIX Commands Reference*, order number 86 A2 38JX to 86 A2 43JX, or by ordering *Go Solo: How to Implement and Go Solo with the Single Unix Specification*, a book which includes the X/Open UNIX95 Specification on a CD–ROM.

Reference Information

The following publications contain information on the commands and files used in the operating system.

- *AIX Commands Reference*, 86 A2 38JX to 86 A2 43JX, is a six–volume set that contains supported commands in alphabetical order.
- *AIX Files Reference*, 86 A2 79AP, contains information on the files available with the operating system.

The following books contain other information you may find useful in day–to–day managing:

- *AIX Quick Reference*, 86 A2 55AP, contains brief descriptions of frequently used commands, along with brief summaries of the commands.
- *AIX INed Editor User's Guide* contains information on the INed editor.

Ordering Publications

You can order publications from your sales representative or from your point of sale.

To order additional copies of this book, use order number 86 A2 99HX.

Use *AIX and Related Products Documentation Overview* for information on related publications and how to obtain them.

Note to Users

The term ”network information service (NIS)” is now used to refer to the service formerly known as ”Yellow Pages.” The functionality remains the same; only the name has changed. The name ”Yellow Pages” is a registered trademark in the United Kingdom of British Telecommunications plc, and may not be used without permission.

Legal Notice to Users Issued by Sun Microsystems, Inc.

”Yellow Pages” is a registered trademark in the United Kingdom of British Telecommunications plc, and may also be a trademark of various telephone companies around the world. Sun will be revising future versions of software and documentation to remove references to ”Yellow Pages.”

Table of Contents

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 Installation Guide*.

Rebooting a Running System

There are two methods for shutting down and rebooting your system, depending upon whether multiple users are logged on to the system:

- If multiple users are logged in to the system, use the **shutdown** command.
- If you are the only user logged in to the system, use the **reboot** command.

Rebooting a Running System Tasks		
Web-based System Manager: **wsm system** fast path (System application) –OR–		
Task	*SMIT Fast Path*	*Command or File*
Rebooting a Multiuser System	**smit shutdown**	**shutdown –r**
Rebooting a Single–User System		**reboot**

Booting from Hard Disk for Maintenance

Prerequisites

A bootable removable media (tape or CD–ROM) must not be in the drive.

Procedure

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

1. Set the key to the Service position and reboot the machine. To reboot, either turn the machine off and then power it back on, or press the yellow 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. Refer to the *AIX Version 4.3 Problem Solving Guide and Reference* for information on copying the dump to removable media.

   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, and the user will be asked to 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 will continue booting and enter 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.

Booting a System That Crashed

In some instances, you may 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 properly 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 will reboot 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 refer to the User Guide or documentation that came with the machine for the specific steps for booting 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 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 instead contact their service representative.
2. This procedure is not intended for system managers who have just completed a new installation, since in this case the system will not contain data that needs to be recovered. If you are unable to boot from the hard disk after completing a new installation, you should 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 will then be asked to select which display is the system console at reboot time. If the user selects a graphics adapter (non–TTY device), it will also become the new default display. If the user selects a TTY device instead of an LFT device, no system login will appear. The machine will need to be rebooted again at which time the TTY login screen will come up. 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 will become the default display.

   Note: Since the TTY is the system console, it will remain the system console.
3. If the system console is `/def/lft0`, then after reboot, DPMS will come up disabled in order to show the system console selection text on the screen for an indefinite period of time. To re–enable DPMS, the system will need to be rebooted for the second time.

Diagnosing Boot Problems

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

- Hardware problems
- Defective boot tapes or CD–ROMs
- Damaged file systems
- Errors in scripts such as /**etc**/**rc.boot**

For information on accessing a system that will not boot from the disk drive, see ”Accessing a System That Will Not Boot”, on page 1-6.

For other diagnostic information, refer to the *AIX Version 4.3 Problem Solving Guide and Reference*.

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

1. You must have root user authority to use the **bosboot** command.
2. The /**tmp** file system must have at least 7MB of free space.
3. The physical disk must contain the boot logical volume. To determine which disk device to specify, enter:

   ```
   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 use the following command:

   ```
   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 /**dev**/**hdisk0**, enter:

```
bosboot -a -d /dev/hdisk0
```

Note: Do not reboot the machine if the **bosboot** command fails while creating a boot image. The problem should be resolved and the **bosboot** command run to successful completion. For information about solving boot problems, see the *AIX Version 4.3 Problem Solving Guide and Reference*.

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

Creating a Boot Image Containing an Uncompressed RAM File System Boot Image

To create an uncompressed RAM file system boot image for the fixed disk /**dev**/**hdisk0**, enter:

```
bosboot -a -U -d /dev/hdisk0
```

Creating a Boot Image Containing a Compressed RAM File System for a Network

To create a compressed RAM file system boot image for an Ethernet boot, enter:

```
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 may 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` and press the Enter key. 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 `/usr/lib/acct/fwtmp </var/adm/wtmp |grep run-level` and press the Enter key.

   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. Enter 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. Enter 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:

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

then press Enter. For example, to add a record for tty2, type:

```
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 should run.
`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:

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

then press Enter. 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 should run.
`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:

```
lsitab -a
```

then press Enter.

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

```
lsitab Identifier
```

then press Enter.

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

Removing Records

To remove a record from the /**etc**/**inittab** file, type:

```
rmitab Identifier
```

then press Enter. 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

There are three methods you can use to shut down the system without rebooting: the Web-based System Manager fastpath, the SMIT fastpath, and the shutdown command.

Prerequisites

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

Procedure

To shut down the system using Web-based System Manager

1. Login as **root**.
2. At the command prompt, type:

   ```
   wsm system
   ```

   then press Enter.

To shut down the system using SMIT:

1. Login as **root**.
2. At the command prompt, type:

   ```
   smit shutdown
   ```

   then press Enter.

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

1. Login as **root**.
2. At the command prompt, type:

   ```
   shutdown
   ```

   then press Enter.

Shutting Down the System to Single–User Mode

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

1. Type `cd /` and press the Enter key 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` and press the Enter key. 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` and press the Enter key. The **–F** flag instructs the **shutdown** command to bypass sending messages to other users and shut down the system as quickly as possible.

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

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

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

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 Overview”, on page 2-5 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 will require 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 4.3 System Management Guide: Communications and Networks* for recommendations.
2. Change the root password as soon as you log on to the new system.
3. Activate minimal accounting by using the procedure in ”Setting Up an Accounting System”, on page 14-2. However, you should 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. You should 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. Enter the following command:

    ```
    li -Ra -l -a > listofallfiles
    ```

    If possible, you should print the `listofallfiles` file (it will be 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 will run continuously or be shut down every evening.

    Most multiuser systems should be left running continuously, although display terminals should be shut off when not in use.

    If the system will be shut down in the evenings, you should 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 will be 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 may want to set a **cron** job to do this automatically.

    You should also 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

The following tasks should be performed 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 should always be active. This 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 *AIX Version 4.3 Problem Solving 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, and the files should be reduced in size periodically.

Security Tasks for Adding Users

You should 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 ”Users and Group”, on page 4-1.
2. If the user is being removed permanently, remove all the user information. See ”Users and Groups”, on page 4-1 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 should include 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 properly 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 will be disabled. The command can be properly 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 may 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** option 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, use the following command:

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

Only attributes whose values can or should not be 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 may not know which new files should be 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 should 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, you should also remove the description of this file. For example, if you have deleted the **/etc/cvid** program, the following command will 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 should be 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's 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 should be 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 appears, the initial login screen was an unauthorized program that may have been trying to steal your password. You should 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. You should run as root user only after establishing a trusted communication path. This ensures that no untrusted programs will be run with root user authority.

  – Running the **su**, **passwd**, and **newgrp** commands. You should only run these commands 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 should have 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 4.3 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.

LDAP Exploitation of the Security Subsystem

The Light Directory Access Protocol (LDAP) devines a standard method for accessing and updating information in a directory (a database) either locally or remotely in a client–server model. The LDAP method is exploited by AIX to allow distributed security authentication as well as access to user, group and role information. This functionality is intended to be used in a clustering environment to keep authentication, user, group and role information common across the cluster.

Once LDAP is enabled to serve user, group and role information, most high level APIs, commands and system management tools should work in the same manner as in a normal environment. One restriction is tha tto create a new user, the **mkuser** command must be called on the server machine and the calling process must have the **AUTHSTATE** environment variable set to LDAP. It is also required that all users and groups that are provided by default on a system must remain locally defined on all client LDAP enable machines. This allows the root user at least to be able to log in on a client if there happens to be some server problem.

The client system knows a user is an LDAP user if that user's **SYSTEM** attribute in the /**etc**/**security**/**user** file is set to LDAP. If the **SYSTEM** attribute in the default stanza is set to LDAP, then all users are considered LDAP users. The LDAP keyword may be used with other **SYSTEM** attribute values as described in Identification and Authentication. The client side communicates to the server through the **secldapclntd** daemon. The daemon accepts

requests from applications, queries the LDAP server and returns data to the application. The **secldapclntd** daemon is also responsible for caching.

Setting Up an AIX LDAP–exploited Security Subsystem

To set up a system as an LDAP server to serve authentication and user, group and role information through LDAP, the LDAP server and client packages must be installed and configured. The AIX LDAP server needs to be configured as a client as well as a server. The DB2 database is also required, as the LDAP server needs it. If the Secure Socket Layer (SSL) version is required, then the SSL version of the LDAP server and client should be installed and configured. When using the SSL version of LDAP, the system administrator must create a key using the LDAP Web Interface. The certificate must be carried to the clients.

To set up the server, use the **mksecldap** command.

For non–SSL, type :

```
mksecldap –s –a <adminDN> –p <adminpasswd>
```

followed by:

```
mksecldap –c –h <hostlist> –d <AIXtreeDN> –u <ALL|userlist> –a
<adminDN> –p <adminpasswd>
```

For SSL, type:

```
mksecldap –s –a <adminDN> –p <adminpasswd> –k <ssl key file path>
–w <client certificate passwd>
```

The Client

The LDAP client must have the LDAP client package installed. If the SSL version of the client package needs to be installed, running the **mksecldap** command changes the user's **SYSTEM** line to LDAP, stores all the information the client needs to talk to the server, and starts the client side daemon.

For non–SSL, type :

```
mksecldap –c –h <hostlist> –d <AIXtreeDN> –u <ALL|userlist> –a
<adminDN> –p <adminpasswd>
```

For SSL, type:

```
mksecldap –c –h <hostlist> –d <AIXtreeDN> –u <ALL|userlist> –a
<adminDN> –p <adminpasswd> –k <ssl key file path> –w <client
certificate passwd>
```

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 can only add an event to this file 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 will 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 will 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 may 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. You should 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, you should 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.

Chapter 3. Administrative Roles

AIX Version 4.3 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

AIX provides SMIT fast paths (shown in the following table) 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**

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 Understanding Authorizations in the *AIX 4.3 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 may 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 Manage Backup Restore 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, on page 4-3. See the disk quotas section in the *AIX 4.3 System Management Concepts: Operating System and Devices* for an overview on this topic. For suggestions on how to improve the efficiency of managing users, see CPU–Efficient User ID Administration in Chapter 5 of *AIX Performance Tuning Guide*.

The following table lists tasks that are used for managing users and groups. You must have root authority to perform many of these tasks.

Managing Users and Groups Tasks		
Web-based System Manager: **wsm users** fast path (Users application) –OR–		
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**	

Managing Users and Groups Tasks		
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** facilities 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 will not work at all for NIS clients and it will work 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

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 should 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** would appear 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** would appear 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`, enter:

```
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

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.

Note: You must have root authority to perform most of the tasks in the following table.

Managing Logical Volumes and Storage Tasks		
Web-based System Manager: **wsm lvm** fast path (Volumes application) –OR–		
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**
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**	

Managing Logical Volumes and Storage Tasks		
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**	

Managing Logical Volumes and Storage Tasks		
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**	
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.

Note:

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 5-24.
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.

Managing Logical Volumes and File Systems Tasks		
Web-based System Manager: **wsm fs** fast path (File Systems application) –OR–		
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 may 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”.
  - ”File Systems Overview”.

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 below.

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 will not be 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 will be 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 will be 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 will fail. 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 would come 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, use 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 will include 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 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 AIX 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 doing the following:

```
importvg -y VGName PVName
```

14. You can mount all file systems using the command:

```
mount all
```

Note: You may 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 is to use this disk, it must also be made a physical volume.

Use Method 0 if you are able to shut down and power off the system before attaching the disk. Otherwise, use Method 1 or Method 2. 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

This method is used when it is possible to shut down and power off the system prior to attaching the disk. Upon boot–up, the **cfgmgr** command is run, which will automatically configure 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
```

Once 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 5-11 to allow the disk to be used by the LVM. If the new disk did not appear in the **lspv** output, refer to the problem determination procedures in *AIX Version 4.3 Problem Solving Guide and Reference*.

Method 1

This method may be used when it is not possible to shut down or power off the system prior to attaching the disk.

1. Run **lspv** 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, enter:

   ```
   cfgmgr
   ```

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

   ```
   hdisk1    none                none
   ```

   or:

   ```
   hdisk1   00005264d21adb2e     none
   ```

   Once you have determined the name of the newly configured disk, use the procedure ”Making an Available Disk a Physical Volume”, on page 5-11 to allow the disk to be utilized by the Logical Volume Manager. If the new disk did not appear in the list, refer to the problem determination procedures in *AIX Version 4.3 Problem Solving Guide and Reference*.

Method 2

This method may be used when it is not possible to shut down or power off the system prior to 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 entering:

   ```
   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 670MB 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”, on page 5-2, or ”Add fixed disk without data to new volume group”, on page 5-2, and ”Migrating the Contents of a Physical Volume”, on page 5-12 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 Drive”, on page 5-8.

- 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 should be cleared. Failure to clear this record may 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 articles:

- The **migratepv** command
- ”Logical Volume Storage Overview”

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.

   ```
   lsvg -p VGname
   ```

   The output will look 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 entering the following:

      ```
      lsdev -Cc disk
      ```

      The output should resemble 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 using 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 using the 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 using the following command (*SourceDiskNumber* will be of the form 'hdiskNumber'):

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

      The output will look similar to the following:

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

      In this example, you would 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 using 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 will 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:

   ```
   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 will 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. Do the following:

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

   then:

   ```
   bootlist -m normal DestinationDiskNumber
   ```

   then:

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

5. Now you can migrate your data. Enter 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 will be 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 will 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, enter 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 may help. See ”Synchronizing the Device Configuration Database”, on page 5-31.

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.

Among the reasons you would organize physical volumes into separate volume groups are the following:

- 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 articles before you import or export a volume group:

- **importvg** and **exportvg** commands
- ”Logical Volume Storage Overview”

  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		
Web-based System Manager: **wsm lvm** fast path (Volumes application) –OR–		
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 running the following command:

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

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

Note:

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**, it is highly recommended that you 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 will not be 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, use 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 4.3 System Management Concepts: Operating System and Devices*.
  - ”Developing a Volume Group Strategy” in *AIX 4.3 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 does not appear in the list, follow step 3. Otherwise, follow step 2.

2. To make a standard user–defined volume group a nonquorum volume group, use the following command;

   ```
   chvg -Qn VGName
   ```

3. If the volume group is not active (varied on), use 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), use the following commands to make the change to nonquorum status effective:

   ```
   varyoffvg VGname
   ```

   then:

   ```
   chvg -Qn VGName
   ```

   then:

   ```
   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, use the following command:

   ```
   chvg -Qn rootvg
   ```

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

   ```
   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 4MB. 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. See ”Resource Requirements of Diskless Workstations” in *AIX Performance Tuning Guide* for more details.

Prerequisites

- ”Logical Volume Storage Overview”
- ”Developing a Logical Volume Strategy”

Procedure

You can use the Web-based System Manager fast path **wsm 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 will be the dedicated device for the file system log. The log will be on hdisk1 and the file system will be on hdisk2 (a 256MB 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` will be the new volume group name). Use the SMIT fast path:

   ```
   smit mkvg
   ```

2. Select the volume group name you created using 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 enter 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. Enter the following SMIT fast path:

   ```
   smit mklv
   ```

6. Enter 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 enter 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, use the following command:

   ```
   lsvg –l fsvg1
   ```

   There should be two logical volumes of the following types listed:

   ```
   /dev/fsvg1log   jfslog
   ```

   then:

   ```
   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”
- ”File Systems Overview”

Procedure

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

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

   ```
   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:

   ```
   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 will be prompted to run **chfs** on all file systems that use the renamed log device.

4. Remount the file systems:

   ```
   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 fast path **wsm lvm** instead of **smit rmlv** or **wsm fs** 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”
- ”Developing a Logical Volume Strategy”
- ”File Systems Overview”

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:

   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.

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

2. To select which file system to remove, enter:

   ```
   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. Enter 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 would be named `/adam/usr/local` and the logical volume would be `locallv`. To verify this, use the following fast path:

   ```
   smit lslv2
   ```

3. To select which logical volume to remove, enter:

   ```
   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. Care must be taken 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”.
- ”File Systems Overview”.

Procedure

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

1. Type

   ```
   smit lspv
   ```

   then 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 using the following on the command line:

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

In this example, `-y` indicates that you will name the logical volume instead of using a system name. The number `38` represents the number of 4MB physical partitions. The raw volume capacity in this example is thus 152MB. 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 should 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 5-12. 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”, on page 5-26
- If the disk drive must be reformatted or replaced, you should 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 may be lost. See ”Recovering Using a Reformatted or Replacement Disk Drive”, on page 5-26.

Prerequisites

- Run diagnostics on the failed disk drive. For instructions, refer to ”How to Run Hardware Service Aids” in your system unit operator guide.
- The following scenario will be 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 **myvg** diagram 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, you should 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 will 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. Use the command:

   ```
   unmount /Directory
   ```

4. Remove all single–copy file systems from the failed physical volume by using 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:

   ```
   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 will not allow you to remove these logical volumes because there should be 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:

   ```
   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 will return 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 may fail.
8. Remove any other logical volumes, such as those with only one copy, using the **rmlv** command. For example:

   ```
   rmlv -f lv00
   ```

   The **rmlv** command removes a logical volume from a volume group.

9. Reduce the size of the volume group to omit the failed drive using the **reducevg** command. For example:

   ```
   reducevg -df myvg hdisk3
   ```

   This example reduces the size of the `myvg` volume group to omit 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:

    ```
    shutdown -F
    ```

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

After Reformatting a Drive

Since the disk has been reformatted, the volume group defined in the disk is gone. If you have forgotten to or were unable to **reducevg** 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, which was reformatted, enter:

   ```
   exportvg VGName
   ```

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

   ```
   varyonvg VGName
   ```

3. You will receive a message about a missing or unavailable disk, and the disk you have now reformatted will be 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. Enter:

   ```
   varyonvg -f VGName
   ```

   The missing disk is now displayed with the PVREMOVED label.

   ```
   hdiskX PVID PVREMOVED
   ```

5. Then, enter the command:

   ```
   reducevg -df VGName PVID
   ```

   Attention: The logical volumes defined on this missing disk will be 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:

```
cfgmgr

mkdev -l hdisk3
```

If you want to reboot the system, this will automatically configure 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:

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

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

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

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

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

   ```
   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:

   ```
   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:

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

6. Restore single–copy file system data from backup media. See ”Restoring Individual User Files”, on page 8-9

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.

   ```
   mkvg –y workvg hdisk1
   ```

2. Create two more disks for this volume group.

   ```
   extendvg workvg hdisk2

   extendvg workvg hdisk3
   ```

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

   ```
   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 aren’t counting on the copy on hdisk2 anymore.

   ```
   rmlvcopy testlv 2 hdisk2
   ```

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

   ```
   reducevg workvg hdisk2
   ```

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

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

7. Shut down the system.

   ```
   shutdown -F
   ```

8. Put in a new disk. It may or may 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 will choose 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.

    ```
    extendvg workvg hdisk2
    ```

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

    ```
    mklvcopy testlv 3
    ```

Synchronizing the Device Configuration Database

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

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

OR

```
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:

```
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 *ESCALA D Series Operator Guide* for details on the hot removability feature. For details on physical removal and insertion of disks, refer to *ESCALA D Series Installation and 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”, on page 5-33.)
- Permanently remove a disk from a volume group. (See ”Removing a Disk without Data Using the Hot Removability Feature”, on page 5-34.)
- Add a disk. (See ”Adding a Disk Using the Hot Removability Feature”, on page 5-35)
- Correct a disk failure. (See ”Recovering from Disk Failure Using the Hot Removability Feature”, on page 5-36.)

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 5-2.

Procedure

1. Unmount any file systems on the logical volumes on the disk using the procedure ”Unmounting a File System on a Removeable Disk”, on page 6-5.
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”, on page 5-4.

   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 should automatically open.
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 *ESCALA D Series Installation and 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 ”Unmounting a File System on a Removeable Disk”, on page 6-5.
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”, on page 5-4.

   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”, on page 5-33.

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, refer to *ESCALA D Series Installation and Service Guide*.
2. Perform the procedure ”Power on a removable disk”, on page 5-3.
3. If the disk has no data, add a physical volume to the volume group.

   OR

   If the disk contains data, go to the procedure ”Importing or Exporting a Volume Group”, on page 5-15.

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 5-26. The notes below provide extra information that applies to disks with the hot removability feature.

Note:

1. To unmount file systems on a disk, use the procedure ”Unmounting a File System on a Removeable Disk”, on page 6-5.
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 5-34.
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 5-35. Then follow the procedure ”Configuring a Disk Drive”, on page 5-8 and finally continue with step 4 of procedure ”After Adding a Reformatted or Replacement Disk Drive”, on page 5-28.

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

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: **wsm fs** fast path (File Systems application) –OR–	
Task	*SMIT Fast Path*
Add a journaled file system	**smit crjfs**
Add a file system to an existing logical volume	**smit crjfslv**
Change the attributes of a journaled file system	**smit chjfs**
List Mounted File Systems	**smit fs**
List of File Systems on a Removeable Disk	**smit lsmntdsk**
Remove a journaled file system	**smit rmjfs**

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. This procedure should be used before mounting any file system.

You can use the Web-based System Manager fast path **wsm fs** to check file systems for inconsistencies or you can use one of the following procedures.

Among the many reasons to verify file systems are the following:

- After a malfunction. For example, if a user cannot change directories to a directory that has that user's permissions (uid).
- Prior to backing up file systems to prevent errors and possible restoration problems.
- At installation or system boot to make sure 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**, or the **fsck** command will fail.
- Check the / and /**usr** file systems only from the maintenance shell (see "Check a File System", on page 6-3).
- You must have write permission on files, or **fsck** will 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. 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 will be 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's device is **/dev/hd4** and the **/usr** file system's device is **/dev/hd2**. To check /, enter the following:

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

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

   You may 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 6-3 or running the **fsck** command.

Mounting or Unmounting a File System Tasks	
Web-based System Manager: **wsm fs** fast path (File Systems application) –OR–	
Task	*SMIT Fast Path*
Mount a Journaled File System (JFS)	**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		
Web-based System Manager: **wsm fs** fast path (File Systems application) –OR–		
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 may not contain all data that was written immediately before the snapshot is taken. Modifications that start after the snapshot begins may 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 exampleassumes 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:

  ```
  rmfs /backup
  ```

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

For additional information about mirrored logical volumes, see the Logical Volume Storage Overview, 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		
Web-based System Manager: (File Systems application) –OR–	**wsm fs** fast path	
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*

Note:

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.

Note:

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) –OR–	**wsm fs** fast path	
Task	*SMIT Fast Path*	*Command or File*
Add a journaled file system	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[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[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*

Note:

1. This procedure is required whenever inserting media containing journaled file systems.
2. Removing a journaled file system will destroy 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”, on page 6-10.
- To terminate the process, go to ”Terminating the Process”, on page 6-10.
- To reclaim file space without terminating the process, go to ”Reclaiming File Space without Terminating the Process”, on page 6-10.
- To fix an overflow in the **/usr** directory, go to ”Fixing a /usr Overflow”, on page 6-11.
- To fix an overflow in a user file system, go to ”Fixing a User File System Overflow”, on page 6-12.

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 may be causing the problem, enter:

   ```
   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, enter:

   ```
   ps -u
   ```

Terminating the Process

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

   ```
   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. For example:

   ```
   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 due to 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. For example:

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

2. Remove **uucp** log files. For example:

   ```
   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:

   ```
   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 don't need the files for accounting. Since /**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**:

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

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

      ```
      vi wtmp.new
      ```

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

      ```
      /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 14-2.

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 Individual User Files”, on page 8-9.

   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 or read/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. For help in diagnosing hardware problems, refer to the *AIX Version 4.3 Problem Solving Guide and Reference*.

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, try using 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 6-13.)
4. If the disk drive is the problem, determine whether you can still address the disk drive (if it is available). There are three ways to do this:
   - Use the Web-based System Manager fast path **wsm devices**.
   - 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, try replacing 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 will no longer be able to read the information stored on the platters and will 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 will be lost, you may 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. Repeat steps 2 through 4.

Getting More Space on a Disk Drive

If you run out of space on a disk drive, there are several ways you can try 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:

```
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, refer to ”Fixing Disk Overflows”, on page 6-10.

For information on typical **cron** entries, refer to ”Setting Up an Accounting System”, on page 14-2.

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. For example:

  ```
  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. Refer to ”Setting Up an Accounting System”, on page 14-2 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 three ways to mount space from one disk drive to another:

- Use the Web-based System Manager fast path **wsm fs**.
- 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 6-5.

Chapter 7. Paging Space and Virtual Memory

This chapter includes the following procedures for allocating page space. For performance implications related to paging spaces, see the section on performance considerations of paging spaces in *AIX Performance Tuning Guide*.

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: You should not add paging space to volume groups on portable disks because removing a disk with an active paging space will cause the system to crash.

To improve paging performance, you should 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, you should 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 would 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		
Web-based System Manager: **wsm lvm** fast path (Volumes application) –OR–		
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 should only be attempted by experienced system managers.

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		
Web-based System Manager: **wsm lvm** fast path (Volumes application) –OR–		
Task	*Procedure*	
Changing the characteristics of a paging space	**smit chps**	
Removing a paging space	1. Use **smit chps** and change the value of the RESTARTED field to **no**. 2. Shut down and reboot the system: **shutdown –r** 3. Show your default dump device:[1] **sysdumpdev –l** 4. Remove the paging space: **smit rmps**	

Note:

1. 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 use 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. For a discussion of recommended sizes of paging spaces, see ”Placement and Sizes of Paging Spaces” in *AIX Performance Tuning Guide*.

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, which 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 should significantly improve 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) would likely contain fewer logical partitions belonging to the busiest file systems.

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

```
lspv -l hdiskX
```

Note: The steps in the following procedures are all necessary, even those not directly related to the hd6 paging space. The additional steps are needed because a paging space cannot be deactivated while the system is running.

Prerequisites

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

- Paging Space Overview
- Managing Paging Spaces
- Logical Volume Storage Overview

Making the hd6 Paging Space Smaller

Note:

1. If you decide to reduce hd6, you must leave enough space for the software in rootvg. A rule of thumb for reducing hd6 paging space is to leave enough space to match *physical* memory. To find out the amount of physical memory, use the following command:

   ```
   lsattr -E -l sys0 -a realmem
   ```

2. AIX Version 4.2.1 and later does not support reducing the size of hd6 below 32MB or the system will not boot.

This procedure assumes that hd6 is on rootvg, which is located on hdisk0. Create a temporary paging space for this procedure on rootvg as follows:

```
mkps -a -n -s 20 rootvg
```

This command outputs the name of the paging space (paging00 if no others exist).

1. Use the following command to deactivate the `hd6` paging spaces in preparation for the reboot later in the procedure:

   ```
   chps -a n hd6
   ```

2. Change the paging space entry in the /**sbin**/**rc.boot** file from:

   ```
   swapon /dev/hd6
   ```

   to

   ```
   swapon /dev/paging00
   ```

3. Change the primary dump device designation to be the paging space paging00.

   ```
   sysdumpdev -P -p /dev/paging00
   ```

4. Create a bootable image with the **bosboot** command for a hard disk image:

   ```
   bosboot -d /dev/hdisk0 -a
   ```

5. Put the system key (if present) in the Normal position and use the following command, which will both shut down the operating system and reboot it:

   ```
   shutdown -r
   ```

6. Remove the hd6 paging space:

   ```
   rmps hd6
   ```

7. Create a new logical volume of the size you want for the hd6 paging space:

   ```
   mklv -t paging -y hd6 rootvg 10
   ```

8. Change the primary dump device designation back to be the paging space hd6.

   ```
   sysdumpdev -P -p /dev/hd6
   ```

9. Change the paging space entry in the /**sbin**/**rc.boot** file from:

   ```
   swapon /dev/paging00
   ```

   to

   ```
   swapon /dev/hd6
   ```

10. Create a bootable image with the **bosboot** command for a hard disk image:

    ```
    bosboot -d /dev/hdisk0 -a
    ```

11. Make the hd6 paging space available to the system:

    ```
    swapon /dev/hd6
    ```

12. Change the temporary paging space, paging00, so that it does not automatically activate at reboot time:

    ```
    chps -a n paging00
    ```

13. Put the system key (if present) in the Normal position and use the following command, which will both shut down the operating system and reboot it:

    ```
    shutdown -r
    ```

14. Remove the temporary paging space:

    ```
    rmps paging00
    ```

Moving the hd6 Paging Space within the Same Volume Group

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 will be 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 7-2)

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 as in the other procedure in this article.

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

```
migratepv -l hd6 hdisk0 hdisk2
```

Chapter 8. Backup and Restore

This chapter contains the following procedures for backing up and restoring information:

Compressing Files

Several methods exist for compressing a file system:

- Use the **–p** option 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, enter:

```
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 may 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 may 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

Three procedures can be used to back up files and file systems: the Web-based System Manager fast path **wsm fs**, 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 4.3 System Management Concepts: Operating System and Devices*.

Prerequisites

- If you are backing up file systems by i–node 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 displays. 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		
Web-based System Manager: **wsm backup** fast path (Backups application) –OR–		
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 4.3 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. Enter 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. Refer to Installing Optional Software and Service Updates in the *AIX Installation Guide* for instructions.

  ```
  installp -agqXd device bos.sysmgt.sysbr
  ```

  where *device* is the location of the software; for example, `/dev/rmt0` for 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		
Web-based System Manager: (Backups application) **wsm backup** fast path –OR–		
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 **savevg** command.

Note:

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 properly 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 will be 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, since the *VGName***.data** file will be overwritten.

For more information about installing (or *restoring*) a backup image, see Installing BOS from a System Backup in the *AIX 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 should 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 **cron** runs the script.
- Make sure the device is connected and available, especially when using scripts that run at night. Use the following **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 may be in use, you should unmount them first to prevent file system corruption.
- Check the file system before making the backup. Use the procedure ”Verifying a File System”, on page 6-3 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 **cron** for execution each night (the default editor is **vi**).

   ```
   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 should run 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 Files Reference* for information on the meaning of extension .1 and other extensions (1–7).

3. Enter 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 **cron**.

Restoring from Backup Image Individual User Files

If you need to restore a backup image destroyed by accident, your most difficult problem will be 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 will help 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. Use the **lsdev –C** | **pg** to check availability.

Restoring from Backup Image Tasks		
Web-based System Manager: **wsm backup** fast path (Backups application) –OR–		
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 log in. 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.

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 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**.

For additional information, see Enabling Dynamic Processor Deallocation in the *AIX 4.3 System Management Concepts: Operating System and Devices*.

Web–based System Manager Fastpath Procedure

1. Type `wsm system` at the system prompt, then press Enter, to start the Web-based System Manager Systems Environment application.
2. In the Web-based System Manager Systems Environment window, select AIX **Operating System**.
3. Using the **Device Properties – sys0 window**, complete the task.

To obtain additional information while completing this task, you can select the **More Info** button in the TaskGuide dialogs.

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 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 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 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 change the NLS environment using the Web-based System Manager Users application or the Manage Language Environment SMIT interface to:

- Change the default language environment.
- Change 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 4.3 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, on page 0.

   ```
   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:

   ```
   vi gwm.src change d_fmt "%d%m%y" to d_fmt "%m-%d-%y"
   ```

3. Compile the locale definition source file:

   ```
   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**:

   ```
   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:

   ```
   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/loccp 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:

   ```
   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` locale:

   ```
   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 enter:

   ```
   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:

   ```
   LC_COLLATE=gwm; export LC_COLLATE
   ```

   Any command will now use the collation order specified in the `gwm` locale. In this example, the characters `a-d` are sorted in reverse order by commands such as **li**, **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 4.3 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, commands and subroutines are provided by the Message Facility. 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 proper 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)

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. There are three suggested printer subsystem scenarios:

- 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		
Web-based System Manager: **wsm system** fast path (System application) –OR–		
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 with the Web-based System Manager fast path, **wsm 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 may 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

The Input Method is a set of subroutines that translate key strokes into character strings in the code set specified by a locale. The 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 Methods overview in *AIX 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.

You can also see Process Management in the *AIX 4.3 System Management Concepts: Operating System and Devices* and the *AIX 4.3 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 4.3 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 will list, 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–pro cess 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 this process's parent 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 AIX 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

For a detailed discussion of process–priority alteration, see ”Controlling Contention for the CPU” in *AIX Performance Tuning Guide*. 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 **renice**. 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. To reset process *ProcID*’s nice value to 20, you would have to be root and enter:

```
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 may end or may keep running. The signals you would 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. You would issue:

```
kill -term ProcessID
```

(The **–term** could be omitted.) If the process does not respond to the SIGTERM, enter:

```
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 may 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 will 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		
Web-based System Manager: **wsm processes** fast path (Processes application) –OR–		
Task	*SMIT Fast Path*	*Command or File*
Binding a Process	**smit bindproc**	**bindprocessor –q**
Unbinding a Process	**smit ubindproc**	**bindprocessor –u**

Chapter 12. Workload Management

AIX Workload Management (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 and physical memory 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 the name of the user or group of the process or the pathname of the applications.

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).

Starting WLM

WLM is an optional service of AIX and must be started manually orautomatically 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. This is a major enhancement from the previous version where existing processes remained Unclassified and outside WLM's control. System administrators of existing WLM configuration should check that the resource shares and limits of the various classes can accommodate the extra workload that used to be Unclassified. This is especially critical for the System class, which is now likely to get all the daemons started early in the system initialization phase.

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 CPU and memory 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 Setting Up WLM, 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, 10ms 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 a reporting tool, **wlmstat**, which shows the amount of resource currently being used by each class.

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, or by creating flat ASCII files. The Web-based System Manager and SMIT interfaces 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**. Only the root user can load WLM property files.

The command to submit the WLM property file, **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 AIX are in **/etc/wlm/standard**.

Defining Classes

In order to fully define a class, you must give it a name. You can also specify its tier value, however, this is optional. If a tier value is not specified, the default value is zero. Next, you define the CPU and physical memory resource limits, then the class assignment rules for this class. These rules are used by WLM to automatically assign processes to this class at exec() time.

Class Names

Class names can contain up to 16 upper and lowercase alphanumeric characters and can include the underscore character. The only names that have a special meaning to the system are **Default** and **System**. The maximum total number of classes you can define is 29.

Default is a special class that is always defined. All processes that are not automatically assigned to another class are assigned to the **Default** class. You cannot specify classification rules for this class. Resource limits can be placed on this class as they can for any other class. The default is to have no resource limits applied.

System is another special class that is always defined. This class gets all privileged processes (root processes) that are not automatically assigned to another class. Resource limits can be placed on this class as they can for any other class. The default is for this class to have a memory minimum limit of 1%.

Class File Format

The class files are stored in a subdirectory of /**etc**/**wlm** that you create. For example, you can create a subdirectory named *sample_config*. The file /**etc**/**wlm**/**sample_config**/**classes** contains a character string describing the WLM configuration in subdirectory **sample_config**. This string appears in the WLM Manage Configurations menu in Web-based System Manager.

Example /etc/wlm/sample_config/description File

```
My sample configuration
```

Format the class file /**etc**/**wlm**/**sample_config**/**classes** as a standard AIX attribute stanza file, with the class name as the stanza header followed by a colon and attribute–value pairs on separate lines following the class name. Separate the attribute and values with an equal sign (=).

The only whitespace that is significant in the class file is the carriage return. Begin comment lines with an asterisk.

Example /etc/wlm/sample_config/classes File

```
Default:
        description=”The WLM default class”
        tier = 0
System:
        description=”The WLM system class”
        tier = 0
student:
        description=”The WLM student class”
        tier = 1
```

Limitation of Resources

Resource Types

The following types of resources are supported:

CPU: This resource is the percentage of available CPU time used by a process. This is the sum of the CPU time used by each thread in the process. (Note that for an MP system, the maximum available CPU time is the sum of that for each CPU individually.)

memory: This resource is the percentage of available system physical memory used by a process.

Specifying Resource Limit Values

Resource limit values are specified in the resource limit file by resource type within stanzas for each class. The limits are specified as a minimum to maximum range separated by a hyphen (with whitespace ignored).

WLM Resource Limits File Format

The files are stored in a subdirectory of **/etc/wlm** that you create. For example, you can create a subdirectory named *sample_config*. Format the WLM resource limits file **/etc/wlm/sample_config/limits** as a standard AIX attribute stanza file with the class name as the stanza header followed by a colon and attribute–value pairs on separate lines following the class name. The attribute and values are separated by an equal sign (=).

The only whitespace that is significant in the resource limits file is the carriage return. Comment lines are preceded by an asterisk.

The resources CPU and memory are used as attributes with the percentage specified as an integral value from 0 to 100.

Future resource limits and other attributes can be added and still preserve backward compatibility with old WLM resource limitation files.

Example /etc/wlm/sample_config/limits File

```
Default:
        CPU = 0% - 100%
        memory = 0% - 100%
System:
        CPU = 10% - 100%
        memory = 20% - 100%
student:
        CPU = 10% - 100%
        memory = 20% - 100%
```

Specifying Target Shares

Create a subdirectory in the **/etc/wlm** directory, for example *sample_config*. Specify resource target share values in the **/etc/wlm/sample_config/shares** file by resource type within stanzas for each class. The target shares are specified by a number between 1 and 65535.

Example /etc/wlm/sample_config/shares File

```
Default:
        CPU = 20
        memory = 20
System:
        CPU = 20
        memory = 20
student:
        CPU = 10
        memory = 20
```

Class Assignment

Unclassified Pseudo–class

In the previous version of WLM, all processes already in existence at the time that WLM is initialized were classified in the **Unclassified** pseudo–class. Now that all the existing processes are classified using the newly loaded assignment rules when WLM is started, there will not be any processes in the Unclassified pseudo–class when WLM is on (in active or passive mode).

The Unclassified pseudo–class can however have memory pages charged to it, for pages which cannot be attributed to a specific process at the time WLM is started. Some of these pages will be classified to the correct class when they get accessed (faulted on), so generally the amount of Unclassified memory will decrease, over time, from the time WLM was started. But there will always be a certain amount of memory remaining Unclassified.

Automatically Classifying Processes

Processes are automatically classified by WLM according to several criteria defined in the rules file. Each of these criteria are specified with a list and a set of values for each class. If no list is specified, no process will match that criterion for that class.

When a process is classified, it will be checked against each class assignment rule in the **/etc/wlm/rules** file so that the rules are listed in the file.

A logical NOT can be performed by prefacing a property value with an exclamation point (!). Thus, ”all users except X that are also not in group Y” can be specified by a single rule.

The classification choices are as follows:

user: This lists the user names as specified in the **/etc/passwd** file. The names are translated to numeric user IDs at the time the WLM parameter files are loaded and the numeric user IDs are used for all classifications. The real (not effective) user ID of a process is used to match against this list.

group: This lists the group names as specified in the **/etc/group** file. The names are translated to numeric group IDs at the time the WLM parameter files are loaded and the numeric group IDs are used for all classifications. The real (not effective) group ID of a process is used to match against this list.

application: This is the pathname of the executable processes to be included in the class. The application names are either full pathnames or Korn shell patterns that match pathnames. Basenames are not allowed, therefore application path names **must** start with a ”/”. The matching is done by actual file executed. If the actual executable file is the same as the file that is derived by following the specified pathname (including symbolic links), then the process is included in the class. The application file needs to exist at the time that a class rule is loaded into the workload management system. Any changes to the application file after the class assignment rule is loaded may not result in a match.

Patterns can be specified to match a set of full pathnames using full Korn shell pattern matching syntax.

The total number of automatic classification rules that can be specified is limited to 255.

Class Assignment File Format

The files are stored in a subdirectory of /**etc**/**wlm** that you create. For example, you can create a subdirectory named *sample_config*. Format the class assignment rules file /**etc**/**wlm**/**sample_config**/**rules** as a table, with each line representing one class assignment rule. The first column is the name of the class to which a process matching all of the attributes in subsequent columns are assigned. The columns are separated by any number of spaces or tabs.

An attribute condition consists of a value or list of values separated by commas (and no spaces).

- If the attribute for a process matches one of the values in the list, then the attribute condition is satisfied.
- If the attribute value for a process matches one of the values in the list that is preceded by an exclamation point (!), then the condition fails.
- The special attribute condition, a single hyphen (–), is always satisfied.

The second column in the file is reserved for future extensions. The only legal value for this reserved attribute is a single hyphen (–).

The order of attributes in the file is **class name**, **reserved**, **user**, **group** and **application**.

Comments are lines preceded by an asterisk. The default shipped class assignment file contains comments on the first two lines that contain column headings and dividing lines to indicate which columns correspond to which attributes.

Example /etc/wlm/sample_config/rules File

```
* class   reserved user      group     application
*_______  _________ _____     ______    ____________

System    -                 root      -         -
student   -                 -         student   !/bin/ksh,!/bin/bsh,!/bin/csh
Default   -                 -         -         -
```

Command Line Interfaces

Defining WLM Properties

Load the WLM properties files with the **wlmcntrl** command:

```
wlmcntrl [-a | -p] [-u] [-d WLM_directory]
```

or

```
wlmcntrl -q
```

or

```
wlmcntrl -o
```

If you do not specify the path of the directory where your WLM configuration files reside, the files **classes**, **limits**, **shares** and **rules** are taken from the directory pointed to by /**etc**/**wlm**/**current**. Otherwise, these files are taken from the directory **WLM_directory**, and the symbolic link /**etc**/**wlm**/**current** is updated to point to **WLM_directory**.

The **–a** and **–p** options are used to start WLM in active or passive mode, or dynamically switch from active to passive mode while WLM is running.

The **–u** option is used to dynamically update shares, limits, tier numbers, and/or assignment rules when WLM is running in active or passive mode.

The **–q** option queries the status (on/running active)/running in passive mode) of WLM.

The **–o** option turns off WLM.

Examining Resource Utilization

Use the **wlmstat** command to show the current resource utilizations by class. This command lists the class name and the percentage of each resource that is currently being used by the class. For CPU utilization, the decayed CPU utilization calculated after the last second by the swapper will be output.

The ps Command

Use the **ps** command with the –c *Clist* option to display the current class association for each process. The default output of the **ps** command is not altered. This option takes the class name as the parameter.

The scheduling priority reported through the **ps** command indicates the scheduling priority used to determine which thread to run. If the scheduling priority of a thread is degraded because its class CPU utilization is reduced, that result is made visible through the output of the **ps** command.

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 may 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 should it stop 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 would be 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. Since the **srcmstr** command requires the SRC to be running, removing the **srcmstr** daemon from the /**etc**/**inittab** file would cause these **startsrc** commands to fail.

See **srcmstr** (man page) 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, enter:

   ```
   mkitab -i fbcheck srcmstr:2:respawn:/usr/sbin/srcmstr
   ```

   The **–i fbcheck** flag ensures that the record will be inserted before all subsystems records.

2. Tell the **init** command to reprocess the /**etc**/**inittab** file by entering:

   ```
   telinit q
   ```

   When **init** revisits the /**etc**/**inittab** file, it will process the newly entered record for the **srcmstr** daemon and start 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.

- 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 a SRC resource such as a subsystem, a group of subsystems, or a subserver.

See **srcmstr** 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, enter **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		
Web-based System Manager: (Subsystems application) **wsm subsystems** fast path –OR–		
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.

Displaying the Status of Subsystems Tasks		
Web-based System Manager: **wsm subsystems** fast path (Subsystems application) –OR–		
Task	*SMIT Fast Path*	*Command or File*
Display the status of a subsystem	**smit qssys**	**lssrc –s** *SubsystemName*
Display the status of all subsystems on a particular host	**smit lsssys**	**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.

Prerequisites

- The SRC must be running. See ”Starting the System Resource Controller”, on page 13-2 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.

Prerequisites

- To turn on or off the SRC resource, the SRC must be running. See ”Starting the System Resource Controller”, on page 13-2 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		
Web-based System Manager: **wsm subsystems** fast path (Subsystems application) –OR–		
Task	*SMIT Fast Path*	*Command or File*
Turn on Subsystem	**smit tracessyson**	**traceson –h Host –s Subsystem**
Turn off Subsystem	**smit tracessysoff**	**tracesoff –h Host –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. Enter the **nulladm** command to ensure that each file has the proper access permission: read (r) and write (w) permission for the file owner and group and read (r) permission for others:

   ```
   /usr/sbin/acct/nulladm wtmp pacct
   ```

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 1984, with prime time beginning at 8:00 a.m. and ending at 5:00 p.m., enter:

   ```
   1984  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**, **/var/adm/acct/fiscal**, 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:

   ```
   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, enter:

   ```
   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 **/usr/lib/acct/holidays**. 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 that accounting is enabled for.
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 comand 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 Comand Summary provides information about all commands that executed since the previous monthly report using the **monacct** command. 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 montly 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 14-2 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 14-2 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, enter:

```
/usr/sbin/sa
```

To summarize the accounting information and merge it into the summary file, enter:

```
/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.

Note:

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 may need to use the full path name **/usr/sbin/acct/runacct** rather than the simple command name, **runacct**.

Procedure

To start the **runacct** command, enter 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 **runacct** command can fail for a variety of reasons, most commonly because the system goes down, the /**usr** file system runs out of space, or 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, enter 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, enter 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, enter:

```
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 would look 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, enter:

  `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, enter:

  `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 14-2 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, enter:

```
ps -ef
```

Another useful variation displays a list of all processes associated with terminals:

```
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:

```
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 14-2 for guidelines.

Show CPU Usage for Each Process

To produce a formatted report of CPU usage by process, enter:

```
acctprc1 </var/adm/pacct
```

This information will be useful in some situations, but you will probably 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 entering:

   ```
   acctprc1 </var/adm/pacct >out.file
   ```

   The /**var**/**adm**/**pacct** file is the default output for process accounting records. You may want to specify an archive **pacct** file instead.

2. Produce a binary total accounting record file from the output of the previous step by entering:

   ```
   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 entering:

   ```
   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, enter:

  ```
  /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, enter:

  ```
  /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, enter:

  ```
  /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 14-2.

Procedure

To display disk space utilization information, enter:

```
acctmerg -a1 -2,13 -h </var/adm/acct/nite/dacct
```

This command displays disk accounting records, which include the number of 1KB 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 14-2 for guidelines.
- The printer or plotter for which you want accounting records must have an `acctfile=` clause in the printer’s 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, enter:

  ```
  /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, enter:

  ```
  /usr/sbin/pac -PPrinter User1 User2 ...
  ```

The **pac** command offers a number of other flags for controlling what information gets displayed. See the *AIX Commands Reference* for details.

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:

   ```
   cd /var/adm/acct/sum
   ```

2. Use the **prtacct** command to check the total accounting file, **tacctprev**:

   ```
   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 all right, 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:

   ```
   acctmerg -i < tacct.new > tacct.mmdd
   ```

5. Create the **tacct** file again:

   ```
   acctmerg tacctprev < tacct.mmdd > tacct
   ```

Fixing wtmp Errors

The **/var/adm/wtmp**, or ”who temp” file, may 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 complaining of bad times.

Prerequisites

You must have root user or adm group authority.

Procedure

1. Move to the **/var/adm/acct/nite** directory:

   ```
   cd /var/adm/acct/nite
   ```

2. Convert the binary **wtmp** file to an ASCII file that you can edit:

   ```
   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:

   ```
   vi wtmp.new
   ```

4. Convert the ASCII **wtmp.new** file back to binary format:

   ```
   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 may encounter several different problems when using the accounting system. You may need to resolve file ownership and permissions problems.

This section describes how to fix general accounting problems:

- To fix incorrect file permissions
- To fix ”bad times” errors
- To fix errors encountered when running the **runacct** command
- To update an out–of–date holidays file

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, enter:

```
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 should be 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 using the following command:

   ```
   cd /var/adm/acct
   ```

   b. Change the ownership for the **sum**, **nite**, and **fiscal** directories to **adm** group authority using the following command:

   ```
   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’s group owner to **adm**, and permissions to 710, that is, no permissions for others. (Processes owned by **adm** will be able to execute the **accton** command, but ordinary users will 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 using the following command:

   ```
   chown adm /var/adm/wtmp
   ```

Fixing Errors

Processing the **/var/adm/wtmp** file may 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 will send 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.

   ```
   /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 14-18.

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 will continue 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’s 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.

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
activ e	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

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 would create the file **active0102** containing the error message.

The abbreviation ”SE message” stands for the standard error message such as:

```
********* ACCT ERRORS : see active0102 *********
```

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 will generate 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 **lockstat** command.

Procedure

Show locking activity by entering:

```
lockstat 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's 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 **lockstat** 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. Setting Up and Running Web-based System Manager

This chapter describes how to set up and run Web-based System Manager in both stand–alone and Client–Server environments.

- Stand–Alone Web-based System Manager
  a. Installing Stand–alone Web-based System Manager
  b. Configuring Stand–alone Web-based System Manager
  c. Running Stand–alone Web-based System Manager
- Client–Server Web-based System Manager
  a. Installing Client–Server Web-based System Manager
  b. Configuring Client–Server Web-based System Manager
  c. Running Client–Server Web-based System Manager
  d. Enabling/Disabling the Web-based System Manager Server on an AIX 4.3 Machine
- Web-based System Manager Security
  a. Installing Web-based System Manager Security
  b. Configuring Web-based System Manager Security
  c. Enabling Web-based System Manager Security
  d. Enabling SMGate
  e. Running Web-based System Manager Security
  f. Troubleshooting Web-based System Manager Security

Stand–Alone Web-based System Manager

Web-based System Manager applications can be run on an AIX machine with Web-based System Manager installed just like other AIX applications. When Web-based System Manager applications are run in this method, no data is transferred over the network. Running Web-based System Manager applications in stand–alone mode requires a graphics terminal.

Installing Stand–alone Web-based System Manager

Web-based System Manager should be installed with the base operating system. The **sysmgt.websm.apps** fileset pre–reqs the necessary filesets. If this fileset is installed, then Web-based System Manager will be available.

Prerequisites:

- **bos.rte 4.3.0.0**
  (base operating system)
- **sysmgt.help.msg.*<LANG>*.websm**
  (SMIT contextual helps fileset)

Co–requisites:

- **Java.rte 1.1.2**
  (Java virtual machine with Java 1.1.2 support)
- **bos.net.tcp.client 4.3.0.0**
  (TCP/IP Client Support)

Configuring Stand–alone Web-based System Manager

No configuration is necessary for running stand–alone Web-based System Manager applications.

Running Stand–alone Web-based System Manager

- *From the command line:*

  Web-based System Manager can be started with the command **wsm**. This will bring up a launch application from which all Web-based System Manager applications can be launched. The following fastpaths are also supported:

Application	Fastpath
Backups	wsm backup
Devices	wsm devices
File Systems	wsm fs
NIM	wsm nim
Network	wsm network
PC Services	wsm pc
Printer Queues	wsm printers
Processes	wsm processes
Registered Applications	wsm register
Software	wsm software
Subsystems	wsm subsystems
System	wsm system
Users	wsm users
Volumes	wsm lvm
Workload Management	wsm wlm
Web-based System Manager Launch App	wsm

- *From the Desktop:*

  Open the Desktop Application Manager. Then open the **System Admin** folder. There will be icons for each of the Web-based System Manager applications. The icon for the Web-based System Manager Launch application is called theWeb-based System Manager **Launch Pad**.

Client–Server Web-based System Manager

Web-based System Manager applications can also be run in client–server mode. In this mode, the AIX machine acts as a server to a graphical client located elsewhere on the network. The Web-based System Manager server does not require a graphical terminal.

Installing Client–Server Web-based System Manager

Server Installation

The same filesets that allow Web-based System Manager Applications to run in stand–alone mode also allow Web-based System Manager to run in client–server mode. In addition, the Web-based System Manager server must be configured to be started by **inetd** when a client connects to the Web-based System Manager server. By default, when Web-based System Manager is installed, the Web-based System Manager server will be configured to run in this manner.

Client Installation

Because Web-based System Manager is written in Java, a Web-based System Manager client can be any machine that has a Java 1.1.2 Virtual Machine installed, including a machine with a browser that supports Java 1.1.2 A Web-based System Manager client could be another AIX machine with a graphics terminal, or a PC. There are two possibilities for Web-based System Manager clients: an applet client in a browser, and an AIX client application.

- **Applets**: A Web-based System Manager client can be run as an applet in a browser, or as a stand–alone Java application. To run a Web-based System Manager client in a browser requires no installation. The Java classes will be downloaded by the browser as needed.
- **AIX client applications**: All AIX machines with Web-based System Manager installed can serve as both Web-based System Manager servers and Web-based System Manager clients. No additional installation is necessary.

Configuring Client–Server Web-based System Manager

Configuring the Web-based System Manager Server

The Web-based System Manager server will be started by **inetd** when a Web-based System Manager client connects to the server. By default, the Web-based System Manager server will listen on port **9090** after initialization.

Configuring the Web-based System Manager client

A remote Web-based System Manager application will prompt the user for a hostname on startup. The port to which the client connects is by default the Web-based System Manager Server default port. The port number can be passed to the client application on the command line, or can be stored in the **websm.cfg** file.

Web-based System Manager Config file

The Web-based System Manager config file **websm.cfg** is kept in the /**usr**/**websm** directory on AIX machines for both the Web-based System Manager server and the Web-based System Manager client.

On non–AIX machines, this file will be searched for in the directory from which an application is invoked.

The Web-based System Manager Config file supports the following parameters:

```
port=9090
```

Configure Web-based System Manager for Applet Mode

There are three possible choices for configuring Web-based System Manager for applet mode:

1. If a web server is detected (such as Lotus Domino Go Webserver or Netscape Web Server), then Web-based System Manager will be automatically configured to be enabled in applet mode upon completion of installation when the Configuration Assistant is run. If a web–server is not installed, then you will be prompted for the document directory for your web–server. To bring up the Configuration Assistant at a later time after install, you can run `configassist` at the command line.

   The default URL for the Web-based System Manager launch page will be at the following URL:

   `http://<hostname>/wsm.html`

2. If a web server is not detected or does not ship with media (such as APACHE Web Server), then configuration will be required by the user if Web-based System Manager is to be used in applet mode. Configuration can be done by two methods:

   a. Invoke the Web-based System Manager System application (**wsm system**). Select the Internet Environment icon. Follow the instructions on the Web-based System Manager Applet page of the Web-based System Manager System notebook.

   b. Configure Web-based System Manager from the command line: `/usr/websm/bin/wsmappletcfg -docdir` <path to the document directory of your webserver> (Example: for Lotus Domino Go Webserver this would be `/usr/lpp/internet/server_root/pub`)

   Some web–servers look in sub–directories under the top–level directory for locale–specific html files. The wsmappletcfg program will search under the document directory for directories with the same name as locales installed for Web-based System Manager. If locale directories are found, wsmappletcfg will link the translated version of the html files to the appropriate directory.

   If you want the top–level html files to be set to the language of your choice, specify the option `-lang <lang>` when running wsmappletcfg with the 5 character locale you want (for example; `ja_JP`).

3. A third method to configure Web-based System Manager for applet mode is by using SMIT. At the command line, enter:
   `smit web_based_system_manager`

Running Client–Server Web-based System Manager

Remote applet

A Web-based System Manager server can also be managed from any machine with a web browser. When Web-based System Manager is installed on an AIX machine, if a web server is detected, a link will be setup for the Web Server to the Web-based System Manager HTML launch page.

The default URL for the Web-based System Manager launch page is `http://<machine name>/wsm.html`. The actual URL may vary. See the owner of the machine for the URL if the default URL does not work.

The Web-based System Manager server will be started automatically when an applet or remote application tries to connect to it.

Remote application

- *From the command–line:*

  A Web-based System Manager application on one machine can be used to manage a Web-based System Manager server on another machine. To start Web-based System Manager to manage a remote machine, enter:

  ```
  wsm –host <hostname> [ –port <port num> ]
  ```

  This will bring up a login box for you to enter your account name and password for the remote machine. If the login is successful, you will see the Web-based System Manager launch container for the Web-based System Manager server you specified in the hostname parameter.

- *From the Desktop:*

  a. Click on the Application Manager icon.

  b. Click on the System_Admin icon.

  c. To manage a machine other than your own, click on the Remote Launch Pad icon.

  d. Type the machine name you want to manage.

  e. In the login window, type your name and password for that machine. The Web-based System Manager launch pad displays.

Enabling/Disabling the Web-based System Manager Server on an AIX 4.3 Machine

By default, the Web-based System Manager server is disabled. To enable the Web-based System Manager server, run:

```
/usr/websm/bin/wsmserver –enable.
```

To disable the server, run:

```
/usr/websm/bin/wsmserver –disable.
```

Web-based System Manager Security

Before installing and configuring Web-based System Manager security be sure that Web-based System Manager for client–server operation has been configured. See Client–Server Web-based System Manager.

In Web-based System Manager secure operation, the managed AIX machines are servers, and the managing users are the clients. The communication between the servers and clients is over the SSL protocol which provides server authentication, data encryption, and data integrity. The user manages the AIX machine by Web-based System Manager using an AIX account on that machine, and authenticates to the Web-based System Manager server by sending the user ID and password over the secured SSL protocol.

Each Web-based System Manager server has its private key and a certificate of its public key signed by a Certificate Authority (CA) which is trusted by the Web-based System Manager clients. The private key and the server certificate are stored in the server's private key ring file **/usr/websm/security/SM.privkr**. The Web-based System Manager client has public key ring file which contains the certificates of the CAs it trusts. This file is **SMpubkr.class**. It is a **.class** file so that the same file may be used both for application and applet modes.

In applet mode (working from the browser), the client must be assured that the applet (.class files) arriving at the browser is coming from the intended server. Moreover, in this mode the public key ring file (**SMpubkr.class**) resides on the server and is transferred to the client with the rest of the applet **.class** files (it is done this way because the browser does not allow applets to read local files). For sender authentication and integrity of these files the client must use the SSL capabilities of the browser and contact the server only with the HTTPS protocol (HTTPS://...). For this you can use the SSL capability of the web server on each managed machine or you can use the SMGate daemon installed with Web-based System Manager Security. SMGate serves as an SSL gateway between the client browser and the web server.

In this section, the following procedures and processes related to Security are discussed at length:

- Installing Web-based System Manager Security
- Configuring Web-based System Manager Security
- Enabling Web-based System Manager Security
- Enabling SMGate
- Running Web-based System Manager Security
- Troubleshooting Web-based System Manager Security

Installing Web-based System Manager Security

Web-based System Manager Security's pre–requisite is the Web-based System Manager. The Web-based System Manager Security fileset, **sysmgt.websm.security**, where available, can be found on the AIX Version 4.3 Bonus Pack.

An additional fileset, **sysmgt.websm.security–us**, with stronger encryption capabilities, is available on the AIX Version 4.3 Bonus Pack that ships only in the U.S. and Canada. This fileset requires that you have **sysmgt.websm.security**.

Configuring Web-based System Manager Security

Web-based System Manager Security provides both a graphical interface and a command line interface for performing the configuration tasks. In the graphical user interface, the security administration panels/task–guides come up as 'actions' when either of the two security icons in the System container are clicked: **Certificate Authority (CA)** and **Server Security**. These icons are visible only in local mode. In different scenarios discussed below, they will be referred as the CA icon and Server icon. In these scenarios, the graphical user interface is used. The corresponding command is listed for each step.

The following scenarios or configuration possibilities are outlined:

- Scenario A: 'Ready to Go' key ring files
- Scenario B: Multiple sites
- Scenario C: Avoid transfer of private keys
- Scenario D: Using another CA
- SMGate Configuration
- Viewing Configuration Properties

Scenario A: 'Ready to Go' key ring files

This is probably the fastest way to get into security operational state. In this scenario you use a single machine to define an internal CA (Certificate Authority) and generate 'ready–to–go' key ring files for all of your Web-based System Manager servers and clients. This generates a public key ring file which you must copy to all of the servers and clients, and a unique private key ring file for each server.

1. Defining an Internal Web-based System Manager–CA
2. Generating the Servers Private Key Ring Files
3. Distributing the Public Key Ring File to All Clients and Servers
4. Distributing the private key ring files to all servers

1. **Defining an internal Web-based System Manager Certificate Authority**

   You should use a 'safe' system for the CA. The CA's private key is the most sensitive data in the Web-based System Manager security configuration.

   Once the CA machine is chosen, log on locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

   Open the "System" container and find the security configuration objects, "Certificate Authority" and "Server Security".

   On the object menu for "Certificate Authority" select "Configure this System as Certificate Authority ...". This will start a task guide. Fill in the following information:

   – **Certificate Authority distinguished name**
     Enter a descriptive name that will help you identify the CA machine and the instance of the CA. Blanks are permitted in the name. The machines hostname plus a sequence number would be a good choice. If you ever redefine the CA, use a different sequence number so you will be able to determine which instance of the CA a certificate is signed by. The name should not be exactly the same as the full TCP/IP name as this will not work with the SMGate utility.

   – **Organization name**
     Enter a descriptive name that identifies your company or your organization.

   – **ISO country code**
     Enter your 2 character ISO country code or select it from the list.

– **Expiration date**
After the expiration date you will need to re–configure Web-based System Manager Security, that is, you will need to re–define the CA and generate new private key ring files for all of your servers. You can change this date or accept the default value.

– **Public key ring directory**
This is the directory where the public key ring containing the CA's certificate will be written. You will need to copy this file to the **/usr/websm/codebase** directory on all of the Web-based System Manager servers and clients.

– **Password**
The CA's private key ring file (**/usr/websm/security/SM.caprivkr**) will be encrypted with this password. Remember this password. You will need to enter it each time you perform a task on this CA.

You can perform this task from the command line with the `smdefca` command.

2. **Generating private key ring files for your Web-based System Manager servers.**

In this step you will need to provide the the full TCP/IP names of all of your Web-based System Manager servers. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line.

On the object menu for "Certificate Authority" select "GenerateServers' Private Keys and Certificate Requests ...". The CA password dialog will appear first. Enter the password that you specified when you defined the CA. Then fill in the following information:

– **List of servers**
Add the names of your Web-based System Manager servers to the list. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the "File containing list of servers" entry field and click the "Browse file" button. The "Browse Server List File dialog" will allow you to select some or all of the servers in the list.

– **Organization name**
Enter a descriptive name that identifies your company or your organization.

– **ISO country code**
Enter your 2 character ISO country code or select it from the list.

– **Location for private key ring files**
Enter the directory where you want the server private key ring files written. Later, you will need to distribute them to the servers and install them.

– **Expiration date**
After the expiration date you will need to generate new private key ring files for your servers. You can change this date or accept the default.

– **Length in bits of server keys**
Select a key length (this field only appears if you have the **sysmgt.websm.security–us** fileset installed).

– **Encrypt the server private key ring files**
This dialog creates a private key ring file for each server that you specified. Each private key ring file contains the private key of a server. If someone steals this key he gains the power of pretending to be that server. Thus this file should be always kept protected. You can protect the private key ring files by encrypting them. If you select this option, you will be prompted for a password. Remember this password. You will be asked for it when you install the private key rings on the servers.

When you click OK, a private key ring file (**S.privkr**) is created for each server, (S) that you specified.

You can perform this task from the command line with the `smgenprivkr` command.

3. **Distributing the public key ring file (SMpubkr.class) to all servers and clients.**

   A copy of **SMpubkr.class** from the directory you specified in step I must be placed in the **/usr/websm/codebase** directory of your Web-based System Manager servers and AIX clients.

Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus access to this file on the client machine should be limited. In applet mode, the client can trust the server to send over this file along with the applet itself – provided the HTTPS protocol is used.

4. **Distributing the private key ring files to all servers**

   Each server's private key ring file must be installed on the server.

   You can move the files to their targets in any secure way. We'll describe here two ways – shared directory and diskette TAR:

   – Shared directory

   Place all of the key ring files on a shared directory (e.g. NFS, DFS) accessible to each server.

Note: For this method you should have chosen to encrypt the server private key ring files on the Generate Servers Private Key Ring Files dialog, since the files will be transferred in the clear. It is also recommended to restrict the access rights to the shared directory to the administrator.

   – Diskette TAR

   Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain just the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

   Next you will need to install the server private key rings on each server. Log on to each server as root, start the Web-based System Manager and open the System container. On the object menu for "Server Security" select "Install Private Key Ring...". Select the source for the server private key ring files. If using a diskette TAR, insert the diskette before clicking OK. Now go ahead and click on OK. If the key ring files are encrypted, you will be asked for the password. The servers private key is installed in **/usr/websm/security/SM.privkr**. Repeat this procedure on each server.

   You can perform this task from the command line with the `sminstkey` command.

Scenario B: Multiple sites

Use this scenario if you have multiple sites and you do not want to distribute private key ring files between sites. Suppose you have site A and site B, and you define your internal Web-based System Manager–CA on a machine in site A. See 1 step I of scenario A for directions on configuring a CA. For all clients, and for site A servers, you can follow Scenario A.

For servers in site B follow these steps:

1. Generating private keys and certificate requests for your Web-based System Manager servers
2. Getting the certificates signed by the CA in site A
3. Importing the signed certificates to the server's private key ring files
4. Distributing the private key ring files to all servers
5. Distributing the public key ring file (**SMpubkr.class**) to all servers and clients in site B

1. **Generating private keys and certificate requests for your Web-based System Manager servers.**

   In this step you will need to provide the the full TCP/IP names of all of your Web-based System Manager servers in site B. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line.

   On a server in site B, log on locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

   Open the ”System” container and find the security configuration object ”Server Security”.

   On the object menu for ”Server Security” select ”Generate Servers’ Private Keys and Certificate Requests...”. Fill in the following information:

   – **List of servers**
     Add the names of your Web-based System Manager servers in site B to the list. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the ”File containing list of servers” entry field and click the ”Browse file” button. The ”Browse Server List File dialog” will allow to select some or all of the servers in the list.

   – **Organization name**
     Enter a descriptive name that identifies your company or your organization.

   – **ISO country code**
     Enter your 2 character ISO country code or select it from the list.

   – **Location for private key files and certificate requests**
     Enter the directory where you want the server private key files and certificate requests written. In Step II, you will need to transfer the certificate request files to the CA in site A for signing. In Step III, you will need to transfer the signed certificates from the CA in Site A back to this directory.

   – **Length in bits of server keys**
     Select a key length (this field only appears if you have the **sysmgt.websm.security–us** fileset installed).

   – **Encrypt the server private key files**
     This dialog creates a private key file for each server that you specified. Each private key file contains the private key of the server. If someone steals this key he gains the power of pretending to be that server. Thus this file should be always kept protected. You can protect the private key ring files by encrypting them. If you select this option, you will be prompted for a password. Remember this password. You will be asked for it when you import the signed certificates and when you install the private key rings on the servers.

   When you click OK, a private key ring file (**S.privk**) and a certificate request (**S.certreq**) is created for each server, (S) that you specified.

   You can perform this task from the command line with the `smgenkeycr` command.

2. **Getting the certificates signed by the CA in Site A**

   In this step you need to transfer the certificate request files to the CA in site A. The certificate requests do not contain secret data, however, the integrity and authenticity during transfer must be insured.

   Transfer a copy of the certificate request files from the server in site B to a directory on the CA machine in site A.

   Log on to the CA machine in site A locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

Open the ”System” container and find the security configuration object ”Certificate Authority”.

On the object menu for ”Certificate Authority” select ”SignCertificates...”. Fill in the following information:

– **Directory for certificate requests**
  Enter the directory containing the certificate requests. Then click the ”Update List” button. The certificate request list will appear in the list box.

– **Select certificate requests to sign**
  To select individual certificate requests, click on them in the list box. To select all of the listed certificate requests, click the ”Select All” button.

– **Certificate Expiration Date**
  After the expiration date you will need to repeat this process to generate new private key ring files for your servers. You can change this date or accept the default date.

When you click OK, a certificate file (**S.cert**) is created for each server (S) that you selected. The certificates are written to the directory containing the certificate requests.

You can perform this task from the command line with the `smsigncert` command.

3. **Importing the signed certificates into the servers’ private key ring files**

   In this step you need to transfer the certificates from the CAin site A back to the server in site B. Copy them to the directory containing the certificate requests and server private key files that you created in step I.

   Then on the server in site B, from the object menu for ”Server Security”,select ”Import Signed Certificates...”. Fill in the following information:

   – **Directory for certificates and private keys**
     Enter the directory containing the signed certificates and server private key files. Then click the ”Update List” button. The list of servers for which there is a signed certificate and a private key file will appear in the list box.

   – **Select one or more servers from the list**
     To select individual servers, click on them in the list box. To select all of the listed servers, click the ”Select All” button.

   When you click OK, if the server private key files were encrypted in step I, you will be prompted for the password. Then, for each server (S) that you selected, the certificate (**S.cert**) is imported in to the private key file (**S.privk**) and the private key ring file (**S.privkr**) is created.

   You can perform this task from the command line with the `smimpservercert` command.

4. **Distributing the private key ring files to the servers**

   Each server’s private key ring file must be installed on the server.

   You can move the files to their targets in any secure way. We’ll describe here two ways – shared directory and diskette TAR:

   – **Shared directory**

     Place all of the key ring files on a shared directory (e.g. NFS, DFS) accessible to each server.

   Note: For this method you should have chosen to encrypt the server private key ring files on the Generate Servers Private Key Ring Files dialog, since the files will be transferred in the clear. It is also recommended to restrict the access rights to the shared directory to the administrator.

– **Diskette TAR**

Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain just the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

Next you will need to install the server private key rings on each server. Log on to each server as root, start the Web-based System Manager and open the System container. On the object menu for ”Server Security” select ”Install Private Key Ring...”. Select the source for the server private key ring files. If using a diskette TAR, insert the diskette before clicking OK. Now go ahead and click on OK. If the key ring files are encrypted, you will be asked for the password. The servers private key is installed in **/usr/websm/security/SM.privkr**. Repeat this procedure on each server.

You can perform this task from the command line with the `sminstkey` command.

5. **Distributing the public key ring file (SMpubkr.class) to all servers and clients in site B to the servers**

   A copy of **SMpubkr.class** from the directory you specified in step I must be placed in the **/usr/websm/codebase** directory of your Web-based System Manager servers and AIX clients.

   Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus access to this file on the client machine should be limited. In applet mode, the client can trust the server to send over this file along with the applet itself – provided the HTTPS protocol is used.

Scenario C: Avoid transfer of private keys

Use this scenario if you want a private key to be generated on the server it belongs to, never to be transferred (by network or diskette) to other systems. In this scenario you configure each server separately. The process must be repeated on each server.

Before you follow this scenario you should configure your CA following the steps in 1scenario A, step I.

Scenario C involves the following tasks:

1. Generating servers’ private keys and certificate requests
2. Getting the signed certificates from your CA
3. Importing the certificates to the private key files
4. Installing the private key on the server
5. Distributing the public key ring file (**SMpubkr.class**) to all servers and clients

1. **Generating a private key and certificate request for your Web-based System Manager server.**

   On the server, log on locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

   Open the ”System” container and find the security configuration object, ”Server Security”.

   On the object menu for ”Server Security” select ”GenerateServers’ Private Keys and Certificate Requests...”. Fill in the following information:

   – **List of servers**
   Add the name of this Web-based System Manager server to the list. The server name is shown in the first text–field by default. Click the ”Add to List” button to add it to the list.

– **Organization name**
Enter a descriptive name that identifies your company or your organization.

– **ISO country code**
Enter your 2 character ISO country code or select it from the list.

– **Location for private key files and certificate requests**
Enter the directory where you want the server private key file and certificate request written. In Step II, you will need to transfer the certificate request file to your CA for signing. In Step III, you will need to transfer the signed certificate from the CA back to this directory.

– **Length in bits of server keys**
Select a key length (this field only appears if you have the **sysmgt.websm.security–us** fileset installed).

– **Encrypt the server private key files**
This dialog creates a private key file for the server that you specified. The private key file contains the private key of the server. If someone steals this key he gains the power of pretending to be that server. Thus this file should be always kept protected. You can protect the private key file by encrypting it. If you select this option, you will be prompted for a password. Remember this password. You will be asked for it when you import the signed certificate and when you install the private key ring on this server.

When you click OK, a private key file (**S.privk**) and a certificate request (**S.certreq**) is created for this server (S).

You can perform this task from the command line with the `smgenkeycr` command.

2. **Getting the certificates signed by the CA**

In this step you need to transfer the certificate request file to your CA. The certificate request does not contain secret data, however, the integrity and authenticity during transfer must be insured.

Transfer a copy of the certificate request file from the server to a directory on your the CA machine. To save time you can transfer the certificate requests from all of your servers and have all of them signed by the CA in one step.

Log on to your CA machine locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

Open the ”System” container and find the security configuration object, ”Certificate Authority”.

On the object menu for ”Certificate Authority” select ”SignCertificates...”. Fill in the following information:

– **Directory for certificate requests**
Enter the directory containing the certificate request(s). Then click the ”Update List” button. The certificate request will appear in the list box.

– **Select certificate requests to sign**
Click on your server’s certificate request(s) in the list box.

– **Certificate Expiration Date**
After the expiration date you will need to repeat this process to generate a new private key ring file for your server. You can change this date or accept the default date.

When you click OK, a certificate file (**S.cert**) is created for each server (S) that you selected. The certificate is written to the directory containing the certificate request.

You can perform this task from the command line with the `smsigncert` command.

3. **Importing the certificates to the private key files**

   In this step you need to transfer the certificate from the CA back to the server. Copy it to the directory containing the certificate request and server private key file that you previously created in step I.

   Then, on the server, from the object menu for ”Server Security”,select ”Import Signed Certificates...”. Fill in the following information:

   – **Directory for certificates and private keys**
     Enter the directory containing the signed certificate and server private key file. Then click the ”Update List” button. The server will appear in the list box.

   – **Select one or more servers from the list**
     Click on your server’s name in the list box.

   When you click OK, if the server private key file was encrypted in step I, you will be prompted for the password. Then, your server’s certificate (**S.cert**) is imported in to the private key file (**S.privk**) and the private key ring file (**S.privkr**) is created in the directory containing the certificate request and private key file.

   You can perform this task from the command line with the `smimpservercert` command.

4. **Installing the private key on the server**

   On the object menu for ”Server Security”, select ”Install Private Key Ring...”. Select the ”Directory” button and enter the directory containing the server’s private key ring file. If the key file was encrypted, you will be asked for the password. Then, the server’s private key is installed in /**usr**/**websm**/**security**/**SM.privkr**.

   You can perform this task from the command line with the `sminstkey` command.

5. **Distributing the public key ring file (SMpubkr.class) to all servers and clients**

   A copy of **SMpubkr.class** from the directory you specified in step I must be placed in the /**usr**/**websm**/**codebase** directory of your Web-based System Manager servers and AIX clients.

   Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus access to this file on the client machine should be limited. In applet mode, the client can trust the server to send over this file along with the applet itself – provided the HTTPS protocol is used.

Scenario D: Using another CA

Use this scenario if you do not want to use an internal Web-based System Manager CA, but instead, you want to use another internal CA product which may already be functioning on your system. In this scenario, your certificate requests will be signed by this other CA.

1. Generating private keys and certificate requests for your Web-based System Manager servers
2. Getting the certificates signed by the CA
3. Importing the signed certificates to the server’s private key ring files
4. Distributing the private key ring files to all servers
5. Importing the CA certificate to the public key ring file
6. Distributing the public key ring file to all clients and servers

1. **Generating private keys and certificate requests for your Web-based System Manager servers.**

   In this step you will need to provide the the full TCP/IP names of all of your Web-based System Manager servers. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line.

   On a server, log on locally as root and start the Web-based System Manager. The security configuration applications of the Web-based System Manager are not accessible if you are not logged in as root or if you are running the Web-based System Manager in remote application or applet mode.

   Open the ”System” container and find the security configuration object, ”Server Security”.

   On the object menu for ”Server Security” select ”GenerateServers’ Private Keys and Certificate Requests...”. Fill in the following information:

   – **List of servers**
     Add the names of your Web-based System Manager servers to the list. You can enter them in the dialog one at a time or you can provide a file containing a list of your servers, one per line. To get the server names from the file, enter the file name in the ”File containing list of servers” entry field and click the ”Browse file” button. The ”Browse Server List File dialog” will allow to select some or all of the servers in the list.

   – **Organization name**
     Enter a descriptive name that identifies your company or your organization.

   – **ISO country code**
     Enter your 2 character ISO country code or select it from the list.

   – **Location for private key files and certificate requests**
     Enter the directory where you want the server private key files and certificate requests written. In Step II, you will need to transfer the certificate request files to the CA for signing. In Step III, you will need to transfer the signed certificates from the CA back to this directory.

   – **Length in bits of server keys**
     Select a key length (this field only appears if you have the **sysmgt.websm.security–us** fileset installed).

   – **Encrypt the server private key files**
     This dialog creates a private key file for each server that you specified. Each private key file contains the private key of a server. If someone steals this key he gains the power of pretending to be that server. Thus this file should be always kept protected. You can protect the private key ring files by encrypting them. If you select this option, you will be prompted for a password. Remember this password. You will be asked for it when you import the signed certificates and when you install the private key rings on the servers.

   When you click OK, a private key file (**S.privk**) and a certificate request (**S.certreq**) is created for each server, (S) that you specified.

   You can perform this task from the command line with the `smgenkeycr` command.

2. **Getting the certificates signed by the CA**

   In this step you need to transfer the certificate request files to the CA. The certificate requests do not contain secret data, however, the integrity and authenticity during transfer must be insured.

   Transfer a copy of the certificate request files from the server to a directory on the CA machine.

   Follow the instructions of your CA to generate the signed certificates out of the certificate requests. The next step will be easier if the name of the certificate file of server S is **S.cert**.

3. **Importing the signed certificates into the servers' private key ring files**

   In this step you need to transfer the certificates from the CA back to the server. Copy them to the directory containing the certificate requests and server private key files that you created in step I. This step requires that the certificate file of a server S be named **S.cert**.

   Then, on the server, from the object menu for "Server Security",select "Import Signed Certificates...". Fill in the following information:

   – **Directory for certificates and private keys**
     Enter the directory containing the signed certificates and server private key files. Then click the "Update List" button. The list of servers for which there is a signed certificate and a private key file will appear in the list box.

   – **Select one or more servers from the list**
     To select individual servers, click on them in the list box. To select all of the listed servers, click the "Select All" button.

   When you click OK, if the server private key files were encrypted in step I, you will be prompted for the password. Then, for each server (S) that you selected, the certificate (**S.cert**) is imported in to the private key file (**S.privk**) and the private key ring file (**S.privkr**) is created.

   You can perform this task from the command line with the `smimpservercert` command.

4. **Distributing the private key ring files to the servers**

   Each server's private key ring file must be installed on the server.

   You can move the files to their targets in any secure way. We'll describe here two ways – shared directory and diskette TAR:

   – **Shared directory**

     Place all of the key ring files on a shared directory (e.g. NFS, DFS) accessible to each server.

   Note: For this method you should have chosen to encrypt the server private key ring files on the Generate Servers Private Key Ring Files dialog, since the files will be transferred in the clear. It is also recommended to restrict the access rights to the shared directory to the administrator.

   – **Diskette TAR**

     Generate a diskette TAR containing all of the server private key ring files. The TAR archive should contain just the file names without the paths. To do this, change directories to the directory containing the server private key ring files and run the command `tar -cvf /dev/fd0 *.privkr`.

   Next you will need to install the server private key rings on each server. Log on to each server as root, start the Web-based System Manager and open the System container. On the object menu for "Server Security" select "Install Private Key Ring...". Select the source for the server private key ring files. If using a diskette TAR, insert the diskette before clicking OK. Now go ahead and click on OK. If the key ring files are encrypted, you will be asked for the password. The servers private key is installed in **/usr/websm/security/SM.privkr**. Repeat this procedure on each server.

   You can perform this task from the command line with the `sminstkey` command.

5. **Importing the CA certificate to the public key ring file**

   Receive the CA (self signed) certificate of your CA (see the documentation for your CA). Copy it to a directory on the server you are working on.

Then, on the server, from the object menu for ”Server Security”,select ”Import CA Certificate...”. Fill in the following information:

– **Directory containing public key ring file**
  Enter a directory for the public key ring file, **SMpubkr.class**. This file will need to be distributed to all of your servers and clients.

– **Full path name of CA Certificate file**
  Enter the directory containing the self signed certificate of your CA.

When you click OK, if the public key ring file **SMpubkr.class** will be written to the directory you specified.

You can perform this task from the command line with the `smimpcacert` command.

6. **Distributing the public key ring file to all clients and servers**

   A copy of **SMpubkr.class** must be placed in the **/usr/websm/codebase** directory of allWeb-based System Manager servers and clients.

   Note: The content of this file is not secret. However, placing it on a client machine specifies which CA the client trusts. Thus access to this file on the client machine should be limited. In applet mode, the client can trust the server to send over this file along with the applet itself – provided the HTTPS protocol is used.

Configuring for SMGate

The SMGate daemon installed with Web-based System Manager Security allows you to run the Web-based System Manager in secure applet mode without having to configure your web server for security on each system to be managed. SMGate serves as an SSL gateway between the client browser and the local web server.

To use SMGate, you will need to receive the Certificate Authoritie’s certificate into your client browsers.

1. If you are using the Web-based System Manager internal certificate authority you can get the CA’s certificate using the following procedure.

   Log on to the CA machine in local mode as root. Start the Web-based System Manager and open the System container. On the object menu for ”Certificate Authority” select ”Export Certificate...”. The ”Export Certificate Authority’s Certificate” dialog will be displayed. Enter the full pathname where you want the certificate written, and click OK. Alternatively, from the command line type:

   ```
   /usr/websm/bin/smexpcacert
   ```

   If you are not using the Web-based System Manager internal certificate authority then use your certificate authority’s procedures for obtaining a copy of its certificate.

2. Copy the certificate to a web server directory so you can access it from the client browsers (for Lotus Go you can put it in the **/usr/lpp/internet/server_root/pub directory**). The MIME type sent by the web server must be **”application/x–x509–ca–cert”**. On the Lotus Go web server you can set the MIME types in ”Configuration and Administration Forms – MIME Types” and by default you can get this MIME type by adding the ”**.DER**” suffix to the certificate file name.

3. In each of your client browsers, point the browser to the CA certificate file and follow your browser’s procedure to accept it as a signer certificate.

Your browsers are now set up to connect to your servers through SMGate. For enabling the SMGate daemon, see ”Enabling SMGate”, for running through SMGate see ”Running Web-based System Manager Security: Applet Mode”.

Viewing Configuration Properties

Once the security configuration is done, it is possible to view the properties of the CA, any server, and any client's public key ring.

CA properties

To view CA properties open the system container and find the security configuration object "Certificate Authority". On the object menu for "Certificate Authority", select "Properties". The dialog provides read–only information for the CA.

Detailed information on all operations executed by the CA (e.g., key ring generation, certificate signing) can be found in the CA log file **/usr/websm/security/SMCa.log**.

You can perform this task from the command line with the `smcaprop` command.

Server properties

To view a server's properties open the system container and find the security configuration object "Certificate Authority". On the object menu for "Certificate Authority", select "Properties". The dialog provides read–only information for the server.

You can perform this task from the command line with the `smserverprop` command.

Public Key Ring Content

To view the CA certificate(s) included in the public key ring **SMpubkr.class**, use the `smlistcerts` command.

Enabling Web-based System Manager Security

On each system you want to manage, you can enable the security option you want enforced. By default, security is enabled so that the managed system will only accept secure connections.

You can enable security so that the managed system will accept secure or unsecure connections by running the command: `wsmserver -ssloptional`. In this mode, the user at the client can select an option on the Web-based System Manager log on dialog to specify a secure or unsecure connection.

You can enable security so that the managed system will only accept secure connections by running the command `/usr/websm/bin/wsmserver -sslalways`.

Enabling SMGate

SMGate can only be enabled after the server has been configured for security, as SMGate uses the server's private key ring **/usr/websm/security/SM.privkr**.

To enable SMGate, enter the command: `/usr/websm/bin/wsmserver -enablehttps`. This starts SMGate and adds an entry to the **/etc/inittab** file so that it is automatically activated when the system is restarted. The default port for SMGate is 9092. You can look in the **/etc/services** file to make sure this port is not being used by another service. You can configure SMGate to use a different port with the command: `/usr/websm/bin/wsmserver -enablehttps <port>` where `<port>` is the port number you want it to use.

If you change the server's security configuration you must disable SMGate and re–enable it. The command for disabling SMGate is `/usr/websm/bin/wsmserver -disablehttps`.

To configure the browser for working through SMGate, see section "Configuring for SMGate".

Running Web-based System Manager Security

Application mode

The Web-based System Manager runs in application mode when you use an AIX machine as a client to manage another AIX machine. On the client you issue the command `wsm -host <hostname>` (where <hostname> is the name of the remote machine you want to manage).

If the machine to be managed is configured to allow secure connections only (see Enabling Web-based System Manager Security), then the client must have the **sysmgt.websm.security** fileset installed and must have a copy of the public key ring file, SMpubkr.class in directory /**usr**/**websm**/**codebase**. In this mode the Web-based System Manager log on dialog will have a check box indicating that security is required.

If the machine to be managed is configured to allow secure or unsecure connections (see Enabling Web-based System Manager Security) and the client has a copy of the public key ring file, **SMpubkr.class** in the /**usr**/**websm**/**codebase** directory, then the Web-based System Manager log on dialog will have a check box that allows the client user to specify a secure or unsecure connection. If the client machine does not have the **SMpubkr.class** file, only a unsecure connection can be established.

Security when running in application mode is indicated by a ”secure connection” message on the status line at the bottom of the Web-based System Manager containers.

Applet mode

The Web-based System Manager runs in applet mode when you use a browser to connect to the machine you want to manage. Applet mode adds another security consideration, the secure transfer of the public key ring file (**SMpubkr.class**) and the applet’s **.class** files. For complete security in applet mode, the client must use the SSL capabilities of its browser and contact the server only with the HTTPS protocol. This requires that the web server is configured for security or that SMGate is configured.

- One option is to use the SSL capability of the web server on the managed machine. For this option, the web server must be configured for security. Follow the instructions provided with your web server. Then you can access the Web-based System Manager on the managed machine with the URL **”https://<hostname>/wsm.html”**. (where <hostname> is the name of the remote machine you want to manage). In this option, the Web-based System Manager applet and public key ring **SMpubkr.class** are transferred securely from the web server on the managed machine to the client.
- Another option is to use the SMGate daemon. SMGate runs on the managed AIX machine and serves as an SSL gateway between the client browser and the local web server. SMGate responds to the HTTPS request of the client browser, and creates an SSL connection with it using the private key and certificate of the Web-based System Manager server. Inside the managed machine, SMGate creates an unsecure connection to the local web server. In this option, the Web-based System Manager applet and public key ring **SMpubkr.class** are transferred securely from SMGate on the managed machine to the browser client and communications between the managed machine and client are over SSL. When you are using a SMGate, you can access the Web-based System Manager on the managed machine with the URL **”https://<hostname>:9092/wsm.html”**. (where <hostname> is the name of the remote machine you want to manage). 9092 is the default port number for SMGate. If you enabled SMGate with a different port number, then specify that number.

There are two security indicators to look for when running in applet mode, the browser’s HTTPS indication, and the ”secure connection” message on the status line at the bottom of the Web-based System Manager containers. If either indicator is missing, the connection is not completely secure.

Troubleshooting Web-based System Manager Security

Problem	Action
No security icons in the System container.	Make sure you're logged in as root, and operating Web-based System Manager on the local machine.
When trying to use the CA for generating key rings or signing certificate requests, a message **CA access is locked (SMCa.lock)** is issued.	If you are sure that no other administrator is currently using the CA, remove the CA lock file **/usr/websm/security/SMCa.lock**.
In SMGate configuration, the browser doesn't recognize the CA certificate file as a CA certificate.	Check in the web server documentation that the MIME type being sent by the web server for the certificate file you placed is indeed **application/x–x509–ca–cert**.
In running through SMGate, the browser issues an error message about invalid signature	It could be that the server is certified by a new CA with the same name as an old CA and that the browser has the CA certificate of the old CA. Delete the old CA certificate in the browser and follow the SMGate configuration section to receive the new certificate.
Secure remote activation of Web-based System Manager fails.	First, verify that non–secure remote activation works (you might need to change the server's setting for that, if it doesn't permit non–secure connections. **Certificate matching and expiration:** • log on as **root** to the server machine and use the *Server Properties* dialog of the Server icon (or the **smserverprop** command line) to verify the server's certificate expiration date, and record the CA name (the CA that signed the server's certificate). • If the problem occurred in application mode use the **smlistcerts** command on the client machine (`smlistcerts /usr/websm/codebase`) and verify that it includes a certificate of the CA that signed the server's certificate (above), and that this certificate hasn't expired. If the problem is in applet mode, issue the **smlistcerts** command on the server's machine,since the public key ring resides on the server and is transferred to the client.

Chapter 16. System Management Interface Tool

This chapter provides information about and procedures for using the System Management Interface Tool (SMIT) fastpaths.

Using Fast Paths in SMIT

You can access different SMIT task through the main menu, or you can use a *fast path* parameter, which can save you time by allowing you to go directly to the menu or dialog for your task, bypassing the upper–level menus.

All commands run by SMIT can be used in a fast path construction. Command names entered as a *FastPath* parameter will take you to a submenu or dialog for that command. For example, to change the characteristics of a user, at the command line enter:

```
smit chuser
```

The **smit** command plus the command **chuser** takes you directly to the menu, Change User Attributes, which guides you through the steps to change a user's characteristics.

At any menu in SMIT, you can show the fast path to that menu by pressing the F8 key or by choosing Fast Path from the Show menu.

Summary of Fast Paths

The following lists provide a quick reference to many SMIT fast paths. In the list, a SMIT menu name is followed by its associated fast path in parentheses. Simply enter the word **smit** and the fast path shown to go directly to its associated menu.

Fast Paths for Installing and Managing the System

- Managing Graphic Input Devices (**input**)
  - Keyboard (**keyboard**)
  - Change/Show Characteristics of the Keyboard(**chgkbd**)
  - Work with LFT Software Keyboard (**keymap**)
  - List Current Software Keyboard Map for LFT ()
  - Change the Keyboard Map for the Next System Restart (**chkbd**)
  - Generate an Error Report (**errpt**)
  - Trace the Keyboard (**trace_link**)
  - Start Trace (**trcstart**)
  - Stop Trace (**trcstop**)
  - Generate a Trace Report (**trcrpt**)
  - Mouse (**mouse**)
  - Generate an Error Report (**errpt**)
  - Trace the Mouse (**trace_link**)
  - Start Trace (**trcstart**)
  - Stop Trace (**trcstop**)
  - Generate a Trace Report (**trcrpt**)
  - Dials/LPF Keys (**dials**)
  - List all Defined Dials/LPF Keys (**lsdials**)
  - Add a Dials/LPF Keys (**makdials**)
  - Change/Show Characteristics of a Dials/LPF Keys (**chdials**)
  - Remove a Dials/LPF Keys(**rmdials**)
  - Configure a Defined Dials/LPF Keys (**cfgdials**)

  - Generate an Error Report (**errpt**)
  - Trace a Dials/LPF Keys(**trace_link**)
  - Start Trace (**trcstart**)
  - Stop Trace (**trcstop**)
  - Generate a Trace Report (**trcrpt**)
  - Tablet (**tablet**)
  - Generate an Error Report (**errpt**)
  - Trace a Dials/LPF Keys(**trace_link**)
  - Start Trace (**trcstart**)
  - Stop Trace (**trcstop**)
  - Generate a Trace Report (**trcrpt**)
  - Spaceball(TM) (**spaceball**)
  - Add a Spaceball (**mksball**)
  - Remove a Spaceball (**rmsball**)
  - Wacom (TM) Serial Tablet (**wacom_tablet**)
  - Add a Wacom (**mkwacom**)
  - Remove a Wacom (**rmwacom**)
  - 6093 Serial Tablet (**6093_tablet**)
  - Add a 6093 (**mk6093**)
  - Remove a 6093 (**rm6093**)
- Managing the Low Function Terminal (LFT) (**lft**)
  - Software Keyboard (**keymap**)
  - List Current Software Keyboard Map for LFT (**lskbd**)
  - Change the Keyboard Map for the Next System Restart (**chkbd**)
  - Displays (**display**)
  - List All Displays Available to the LFT (**lsdisp**)
  - Move the LFT to Another Display (**chdisp**)
  - Display Power Management (**display_pm_select**)
  - Generate an Error Report (**errpt**)
  - Start Trace (**trcstart**)
  - Stop Trace (**trcstop**)
  - Generate a Trace Report (**trcrpt**)
  - Trace a Display (**trace_link**)
  - Fonts (**font**)
  - List All Fonts in the System (**lsfont**)
  - Select the Active Font for Next System Restart (**chfont**)
  - Add a Font to the System (**mkfont**)

- Managing the System Environment (**system**)
  - Stop the System (**shutdown**)
  - Assign the Console (**chcons**)
  - Change/Show Date, Time, and Time Zone (**chtz**)
  - Manage Language Environment (**mlang**)
  - Change/Show Characteristics of Operating System (**chgsys**)
  - Change/Show Number of Licensed Users (**chlicense**)
  - Broadcast Message to All Users (**wall**)
  - Manage System Logs (**logs**)
  - System Dump (**dump_link**)
  - Change System User Interface (**dtconfig**)
- Managing the System Performance (**performance**)
  - Resource Status and Monitors (**monitors**)
  - Analysis Tools (**analysis**)
  - Resource Controls (**controls**)
  - Schedule Jobs (**at**)
  - Power Management (**pm**)
- Managing the System Problems (**problem**)
  - Error Log (**error**)
  - Trace (**trace**)
  - System Dump (**dump**)
  - Alog (**alog**)
  - Hardware Diagnostics (**diag**)
  - Verify Software Requisites and Installations (**lppchk**)
- Managing Storage and File Systems (**storage**)
  - Logical Volume Manager (**lvm**)
  - File Systems (**fs**)
  - Files and Directories (**filemgr**)
  - Removable Disk Management (**rds**)
  - System Backup Manager (**backsys**)
- Managing Printers (**printer**)
  - List All Defined Printers/Plotters (**lsdprt**)
  - List All Supported Printers/Plotters (**lssprt**)
  - Add a Printer/Plotter (**makprt**)
  - Move a Printer/Plotter to Another Port (**movprt**)
  - Change/Show Characteristics of a Printer/Plotter (**chgprt**)
  - Remove a Printer/Plotter (**rmvprt**)
  - Configure a Defined Printer/Plotter (**cfgprt**)
  - Install Additional Printer/Plotter Software (**printerinst**)

  - Generate an Error Report (**errpt**)
  - Trace a Printer/Plotter (**trace_link**)
- Managing Print Jobs and Queues (**print**)
  - Start a Print Job (**qprt**)
  - Manage Print Jobs (**jobs**)
  - List All Print Queues (**spooler**)
  - Manage Print Queues (**pqmanage**)
  - Add a Print Queue (**mkpq**)
  - Add an Additional Printer to an Existing Print Queue (**ps_mkpq_attachName**)
  - Change/Show Print Queue Characteristics (**chpq**)
  - Change/Show Printer Connection Characteristics (**chprtcom**)
  - Remove a Print Queue (**rmpq**)
  - Manage Print Server (**server**)
  - Programming Tools (**pqtools**)

Fast Paths for Managing Networks

Fast Paths for NFS

- Network File System (**_nfs**)
  - Configure NFS on This System (**nfsconfigure**)
  - Add a Directory to Exports List (**mknfsexp**)
  - Change/Show Attributes of an Exported Directory (**chnfsexp**)
  - Remove a Directory from Exports List (**rmnfsexp**)
  - Add a File System for Mounting (**mknfsmnt**)
  - Change/Show Attributes of an NFS File System (**chnfsmnt**)
  - Remove an NFS File System (**rmnfsmnt**)
- Network Information Service (NIS) (**yp**)
  - Change NIS Domain Name of this Host (**chypdom**)
  - Configure/Modify NIS (**ypconfigure**)
  - Start/Stop Configured NIS Daemons (**ypstartstop**)
  - Manage NIS Maps (**ypmaps**)
- Configure Secure NFS & NIS (**rpc**)
  - Start Keyserv Daemon (**mkkeyserv**)
  - Stop Keyserv Daemon (**rmkeyserv**)
  - Add/Change Keys for Users (**newkey**)

Fast Paths for DCE

- DCE (Distributed Computing Environment) (**dce**)
  - Configure TCP/IP (If Not Already Configured) (**dce_to_tcpip**)
  - Configure DCE/DFS (**mkdce**)
  - DCE Security & Users Administration (**dcesecadmin**)
  - CDS (Cell Directory Service) Administration (**dcecdsadmin**)

- DTS (Distributed Time Service) Administration (**dtsadmin**)
- RPC (Remote Procedure Call) Administration (**rpc_maint**)
- DFS (Distributed File Service) Administration (**dfsadmin**)
- Stop DCE/DFS Daemons (**stopdce**)
- Restart DCE/DFS Daemons (**restartdce**)
- Register Cell Globally (**mkdceregister**)
- Unregister Cell Globally (**rmdceregister**)
- Unconfigure DCE/DFS (**rmdce**)

Fast Paths for TCP/IP

- Host name (**hostname**)
  - Set the Hostname (**mkhostname**)
  - Show a Hostname (**lshostname**)
- Select BSD–Style rc Configuration (**setbootup_option**)
- Static Routes (**route**)
  - List All Routes (**lsroute**)
  - Add a Static Route (**mkroute**)
  - Remove a Static Route (**rmroute**)
  - Flush Routing Table (**fshrttbl**)
- Network Interfaces (**netinterface**)
  - Network Interface Selection (**inet**)
  - List All Network Interfaces (**lsinet**)
  - Add a Network Interface (**mkinet**)
  - Add a Standard Ethernet Network Interface (**mkineten**)
  - Add an IEEE 802.3 Network Interface (**mkinetet**)
  - Add a Token–Ring Network Interface (**mkinettr**)
  - Add a Serial Line INTERNET Network Interface (**mkinetsl**)
  - Add a Serial Optical Network Interface (**mkinetso**)
  - Add an IBM 370 Channel Attach Network Interface (**mkinetca**)
  - Add a FDDI Network Interface (**mkinetfi**)
  - Change/Show Characteristics of a Network Interface (**chinet**, **shinet**)
  - Remove a Network Interface (**rminet**)
  - Network Interface Drivers (**chif**)
- Name Resolution (**namerslv**)
  - Domain Nameserver (**resolvconf**, **resolv.conf**)
  - Start Using the Nameserver (**stnamerslv**)
  - Restore a Copy of /**etc**/**resolv.conf** File (**stnamerslv1**)
  - Create a New /**etc**/**resolv.conf** File (**stnamerslv2**)
  - List all Nameservers (**lsnamerslv**)
  - Add a Nameserver (**mknamerslv**)

  - Remove a Nameserver (**rmnamerslv**)
  - Stop Using a Nameserver (**spnamerslv**)
  - Set/Show the Domain (**mkdomain**)
  - Remove the Domain (**rmdomain**)
  - Hosts Table (**hosts**, **hostent**)
  - List All Hosts (**lshostent**)
  - Add a Host (**mkhostent**)
  - Change/Show Characteristics of a Host (**chhostent**)
  - Remove a Host (**rmhostent**)
- Client Network Services (**clientnet**)
  - Services
  - List All Services (**lsservices**)
  - Add a Service (**mkservices**)
  - Change/Show Characteristics of a Service (**chservices**, **shservices**)
  - Remove a Service (**rmservices**)
  - Syslog (information only)
  - Protocols (information only)
- Server Network Services (**servernet**, **ruser**)
  - Remote Access (**rmtaccess**)
  - Host access (**hostsequiv**, **hosts.equiv**)
  - List All Remote Hosts (**lshostsequiv**)
  - Add a Remote Host (**mkhostsequiv**)
  - Remove a Remote Host (**rmhostsequiv**)
  - Restrict File Transfer Program Users (**ftpusers**)
  - Show All Restricted Users (**lsftpusers**)
  - Add a Restricted User (**mkftpusers**)
  - Remove a Restricted User (**rmftpusers**)
  - Other Available Services (**otherserv**)
  - Super Daemon (**inetd**)
  - **inetd** Subsystem (**inetdsubsys**)
  - Start Using the **inetd** Subsystem (**mkinetd**)
  - NOW (**mkinetd_now**)
  - Next System RESTART (**mkinetd_boot**)
  - BOTH Now and at System Restart (**mkinetd_both**)
  - Change/Show Restart Characteristics of **inetd** Subsystem (**chinetd**, **lsinetd**)
  - Stop Using the **inetd** Subsystem (**rminetd**)
  - NOW (**rminetd_now**)
  - Next System RESTART (**rminetd_boot**)
  - BOTH (**rminetd_both**)

- **inetd** Subservers (**inetdconf, inetd.conf**)
- List All **inetd** Subservers (**lsinetdconf**)
- Add an **inetd** Subserver (**mkinetdconf**)
- Change / Show Characteristics of an **inetd** Subserver (**chinetdconf**, **shinetdconf**)
- Remove an **inetd** subserver (**rminetdconf**)
- **syslogd** Subsystem (**syslogd**)
- Start Using the **syslogd** Subsystem (**stsyslogd**)
- NOW (**stsyslogd_now**)
- Next System RESTART (**stsyslogd_boot**)
- BOTH (**stsyslogd_both**)
- Change/Show Restart Characteristics of **syslogd** Subsystem (**chsyslogd**, **lssyslogd**)
- Stop Using the **syslogd** Subsystem (**spsyslogd**)
- NOW (**spsyslogd_now**)
- Next system RESTART (**spsyslogd_boot**)
- BOTH (**spsyslogd_both**)
- **routed** Subsystem (**routed**)
- Start Using the **routed** Subsystem (**strouted**)
- NOW (**strouted_now**)
- Next System RESTART (**strouted_boot**)
- BOTH (**strouted_both**)
- Change/Show Restart Characteristics of **routed** Subsystem (**chrouted**, **lsrouted**)
- Stop Using the **routed** Subsystem (**sprouted**)
- NOW (**sprouted_now**)
- Next system RESTART (**sprouted_boot**)
- BOTH (**sprouted_both**)
- **gated** Subsystem (**gated**)
- Start Using the **gated** Subsystem (**stgated**)
- NOW (**stgated_now**)
- Next System RESTART (**stgated_boot**)
- BOTH (**stgated_both**)
- Change/Show Characteristics of **gated** Subsystem (**chgated**, **lsgated**)
- Stop Using the **gated** Subsystem (**spgated**)
- NOW (**spgated_now**)
- Next system RESTART (**spgated_boot**)
- BOTH (**spgated_both**)
- **named** Subsystem (**named**)
- Start Using the **named** Subsystem (**stnamed**)
- NOW (**stnamed_now**)
- Next System RESTART (**stnamed_boot**)

- BOTH (**stnamed_both**)
- Change/Show Restart Characteristics of **named** Subsystem (**chnamed**, **lsnamed**)
- Stop Using the **named** Subsystem (**spnamed**)
- NOW (**spnamed_now**)
- Next system RESTART (**spnamed_boot**)
- BOTH (**spnamed_both**)
- **rwhod** Subsystem (**rwhod**)
- Start Using the **rwhod** Subsystem (**strwhod**)
- NOW (**strwhod_now**)
- Next System RESTART (**strwhod_boot**)
- BOTH (**strwhod_both**)
- Stop Using the **rwhod** Subsystem (**sprwhod**)
- NOW (**sprwhod_now**)
- Next system RESTART (**sprwhod_boot**)
- BOTH (**sprwhod_both**)
- **timed** Subsystem (**timed**)
- Start Using the **timed** Subsystem (**sttimed**)
- NOW (**sttimed_now**)
- Next System RESTART (**sttimed_boot**)
- BOTH (**sttimed_both**)
- Change/Show Restart Characteristics of **timed** Subsystem (**chtimed**, **lstimed**)
- Stop Using the **timed** Subsystem (**sptimed**)
- NOW (**sptimed_now**)
- Next system RESTART (**sptimed_boot**)
- BOTH (**sptimed_both**)
- **portmap** Subsystem (information only)
- PTYs (**pty**)
- Change/Show Characteristics of the pty (**chgpty**)
- Remove the pty; Keep Definition (**rmvpty**)
- Configure the Defined pty (**cfgpty**)
- Generate Error Report (**errpt**)
- Trace the pty (**tpty**)
- Start Trace (**trcstart**)
- Stop Trace (**trcstop**)
- Generate a Trace Report (**trcrpt**)
- Routing (information only) **(ruser)**
- Nameserver (information only) **(ruser)**
- Arp Tables (information only) **(ruser)**

- Manage Print Server (**rprint**)
  - List all Remote Clients with Print Access (**lshostslpd**)
  - Add Print Access for a Remote Client (**mkhostslpd**)
  - Remove Print Access for a Remote Client (**rmhostslpd**)
  - Start the Print Server Subsystem (**mkitab_lpd**)
  - Stop the Print Server Subsystem (**rmitab_lpd**)
  - Show Status of the Print Server Subsystem (**statlpd**)

Chapter 17. Managing the CDE Desktop

With the CDE Desktop, 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 will 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 AIX Common Desktop Environment (CDE) 1.0. Help volumes, web–based documentation, and hardcopy manuals may refer to the desktop as CDE Desktop, the AIXwindows desktop, the CDE desktop, AIX CDE 1.0, or simply, the desktop.

Topics covered in this chapter are:

Starting and Stopping the CDE Desktop

You can set up the system so that CDE Desktop comes up automatically when you start the system, or you can start CDE Desktop manually. You must log in as root to perform each of these tasks.

Enabling and Disabling Desktop Autostart

You may find it more convenient to set up your system to start CDE Desktop automatically when the system is turned on. You can do this through the Web-based System Manager fast path, **wsm 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 CDE Desktop Automatically Tasks		
Web-based System Manager: **wsm system** fast path (System application) –OR–		
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**

Note: [1] Restart the machine after completing this task.

Starting CDE Desktop Manually

You can start CDE Desktop manually.

Start the Desktop Login Manager Manually

1. Log in to your system as root.
2. At the command line, enter:

   ```
   /usr/dt/bin/dtlogin –daemon
   ```

A **Desktop Login** screen will display. When you log in, you will start a desktop session.

Stopping CDE Desktop Manually

You can stop CDE Desktop 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 entering the following:

   ```
   cat /var/dt/Xpid
   ```

3. Stop the Login Manager by entering:

   ```
   kill –term process_id
   ```

Modifying Desktop Profiles

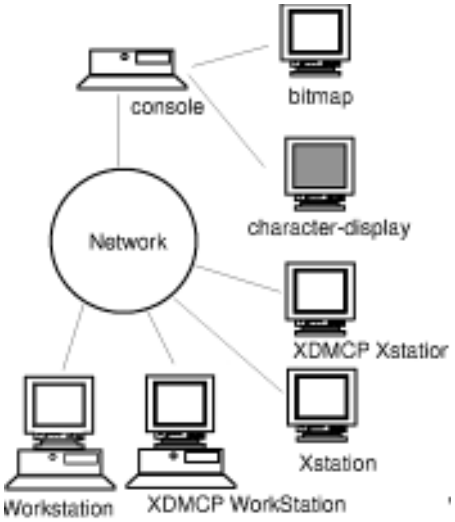
When a user logs in to the desktop, the shell environment file (**.profile** or **.login**) is not automatically read. The desktop runs the X server before the user logs in, so the function provided by the **.profile** file or the **.login** file must be provided by the desktop's login manager.

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 *Common Desktop Environment 1.0: Advanced User's and System Administrator's Guide*.

Adding and Removing Displays and Terminals for CDE Desktop

The login manager may be started from a system with a single local bitmap or graphics console. Many other situations are also possible, however (see figure). You may want to start CDE Desktop from:



- Local consoles.
- Remote consoles.
- Bitmap and character–display.
- X Display Manager Control Protocol (XDMCP) Xstations.
- Non–XDMCP Xstations.
- 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 X server. Clients, including CDE Desktop, are run on one or more host systems on the networks. Output from the clients is directed to the Xterminal display.

Wherever possible, you should use terminals that support XDMCP (X Display Manager Control Protocol).

The following Login Manager configuration tasks support many possible configurations.

- Adding an Xstation Terminal that supports XDMCP
- Adding a Non–XDMCP Xstation Terminal
- Removing a Local Display
- Adding an ASCII or Character–Display Terminal

Adding an Xstation Terminal that supports XDMCP

1. Make sure Login Manager is running on the host system.
2. Enable XDMCP on the Xterminal and direct it to contact Login Manager on the host system.

XDMCP provides a mechanism by which Xterminals can request login services from a network host. It ensures that the Xterminal is communicating with a valid login manager, and provides the protocol for exchanging authentication information between the Xterminal and the host login manager. Documentation for your Xterminal covers the procedure for enabling XDMCP.

Limiting Access by Xterminals to a Host

1. If the **/etc/dt/config/Xaccess** file does not exist, copy the **/usr/dt/config/Xaccess** file to the **/etc/dt/config** directory.
2. If you have to copy Xaccess to **/etc/dt/config**, you must change the **Dtlogin.servers:** line in **/etc/dt/config/Xconfig** to:

   ```
   Dtlogin.accessFile:
   /etc/dt/config/Xaccess
   ```

3. Edit **/etc/dt/config/Xaccess** on the host. List only those X–terminals permitted to access Login Manager.

If Xaccess is empty, any host can connect.

Using a Workstation as an Xterminal

From a command line, enter:

```
/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.

Adding a Non–XDMCP Xstation Terminal

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 include an entry for each terminal. The display type of each terminal must be foreign.
4. Reread the Login Manager configuration files.

When Login Manager receives a SIGHUP, it rereads Xconfig and the Xservers file (or the file specified by the Dtlogin.servers resource). If it finds a new entry, dtlogin starts managing that display. If an entry has been removed, the process associated with that entry is immediately terminated.

Example

The following lines in Xservers directs dtlogin to manage sessions on two non–XDMCP terminals.

```
ext1:0 NPD200X foreign
ext2:0 QCP-19 foreign
```

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 CDE Desktop

You can configure CDE Desktop 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 may be necessary or desirable to use different dtlogin resources for each display.

It may also be necessary or desirable to use different system wide 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 CDE Desktop. 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 Xservers 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 Xservers 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 will be the equivalent to **/etc/opt/dt/Xresources**):

   ```
   Dtlogin.DisplayName.resources: path/file
   ```

3. Create each of the resource files specified in Xconfig.
4. In each file, place the dtlogin resources for that display.

Example

The following lines in Xconfig 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 CDE Desktop session is started.

The script **/etc/dt/config/Xreset** can be used to reverse the setting made in **Xstartup.** Xreset runs when the user logs out.

Example

The following lines in **Xconfig** 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 Xconfig.

Example

The following lines in Xconfig 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 18. Documentation Library Service

The AIX online documentation is delivered on one of two CD-ROMs:
– 86 A2 72JX: Hypertext Library. Basic Subset for AIX 4.3
– 86 X2 73JX: Hypertext Library. Full Set for AIX 4.3

Instructions for installing the *Hypertext Library* are contained in the CD-ROM booklet and must be scrupulously followed.

The *Hypertext Library* comes with a set of tools called *Hypertext Library Utilities.* This set of tools contains a **Search** function allowing to search for information through the entire Library and a **Multi-Print** capability allowing to print several documents with a single click in the Search Results window.

The *Hypertext Library* and the *Hypertext Library Utilities* have both a graphical and character interface.

The contents of the *Hypertext Library* and the *Hypertext Library Utilities* are described in the *Hypertext Library* home page.

More information can be found in the leaflet: *"About the Documentation CD-ROM"*.

The following information in this chapter **does not** concern the *Hypertext Library*. In particular, **do not use** the *Search Service* or the *Library Service* described herafter with the *Hypertext Library*.

The Documentation Library Service allows you to read and search 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.

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 your own company's HTML documents 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.

With the exception of the library's 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.

It is highly recommended that the library service be fully configured since 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 since it is expected that other applications may use it as the library function for their own online documentation.

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 article provides information about changing the configuration of the Documentation Library Service after it has been initially installed and configured.

Note: In AIX Versions 4.3.0 to 4.3.2 the service was called the Documentation Search Service. In AIX Version 4.3.3, it was renamed to the Documentation Library Service to reflect its broader functionality.

The following main topics are covered in this chapter:

- Viewing the Current Configuration
- Changing a Client Computer's Default Remote Documentation Server
- Selecting the Documentation Server for a Single user
- Converting a Client System to a Documentation Server System
- Disabling or Uninstalling the Documentation Library Service
- Converting a Standalone Documentation Server into a Public Documentation Server
- Changing the Default Browser
- Changing the Web Server Software on a Documentation Server
- Changing the Documentation Language

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 will not be affected by the default settings.

You can view the configuration of the documentation library service by using either of the AIX system management tools:

Using Web-based System Manager:

1. Change to the root user.
2. At the command line, type:

   ```
   wsm system
   ```

   then press Enter.
3. In the System Environments window, double–click on **Internet Environments**.
4. When the notebook appears, click on the **Default Browser** tab if it isn't already the front page. This shows the current command that is used to launch the default browser that displays the library application.

   The **Documentation Server** configuration page shows 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
   ```

   then press Enter.
3. From the web configuration menu, select **Show Documentation and Search Server** to display the current configuration information.

Changing a Client Computer's Default Remote Documentation Library Service

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 AIX system management tools:

Using Web-based System Manager:

1. Change to the root user.
2. At the command line, type:

   ```
   wsm system
   ```

   then press Enter. This opens the **System Environments** container.
3. In the System Environments window, double–click on the **Internet Environments** icon to open it, then click on the **Documentation Server** tab.
4. Click on the **Remote server** radio button, then type the name of the documentation server computer in **Computer name**. This is the server computer that contains the documents that you want this client computer to be able to access and search.
5. In **Server port**, at the bottom, 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
   ```

   then press Enter.
3. From the web configuration screen, select **Change Documentation and Search Server**. From the **List**, 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. When the output pane shows the message `Documentation server configuration completed`, the reconfiguration is finished.

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 will be 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 will not affect these users. If these users want to resume using the system–wide default server, they can remove the above two lines from their profile, log out, then log back in.

Manually Going to a Documentation Server:

When users don't 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).

For 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 this 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 appears 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.

Disabling or Uninstall the Documentation Library Service

You can disable a server temporarily, or uninstall it permanently.

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.

Note: 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 process named "httpdlite". To prevent the web server software from being automatically restarted each time the computer reboots, edit the file /etc/inittab and remove or comment out this 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 above 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"):

```
/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_form2, ds_rslt*, and *ds_rslt2* (the last two files only exist in 4.3.0 to 4.3.2). Turn off these files' execution permissions. This turns off access to all the documentation library service functions. An error message will display whenever users try to access the library service on this documentation server.
- To disable just the searching of a specific index without removing the documents or index it from the documentation server, unregister the index.

If you think you might ever want to re–register the index, you must record the index's 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/cli/imndomap /var/docsearch/indexes -l
   <index_name>
   ```

   where `<index_name>` is replaced with the name of the index.
3. Write down the index name, document path, and title.
4. Type the following command to delete the index:

   ```
   /usr/IMNSearch/cli/imndomap /var/docsearch/indexes -d
   <index_name>
   ```
5. Type the following command to complete the deletion:

   ```
   cp /var/docsearch/indexes/imnmap.dat
   /usr/docsearch/indexes/imnmap.dat
   ```

If you ever want to re–register this same index:

1. Login as the root user or library administrator.
2. Type the following command at a command line:

   ```
   /usr/IMNSearch/cli/imndomap /var/docsearch/indexes -c
   <index_name> <document path> "<title>"
   ```

   where you insert the index name, document path, and title values you recorded above in step 2.

Permanently Uninstalling:

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 do uninstalls using SMIT instead of just deleting software. Deletes will not clean up the system properly.

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 read me 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 type:

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, you should go into SMIT and change the name of the default documentation server to another computer. See Changing a Client Computer's Default Remote Documentation Library Server.

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 the section Change the Web Server Software on A Documentation Server.

Changing the Default Browser

This procedure changes the default browser that is used by applications that use the default browser 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 AIX system management tools, Web–based System Manager or SMIT.

Using Web–based System Manager:

1. Change to the root user on the client computer.
2. On a command line, type:

   ```
   wsm system
   ```

   to open the **System Environments** container.
3. In the System Environments window, double–click on the **Internet Environments** icon to open it.
4. In the notebook dialog, click on the **Default Browser** tab if it isn't already the front page.
5. In the 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.bull.com` at a command line to open your wonderbrowser with the www.bull.com page open inside, you would type `wonderbrowser –u` into 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 compute

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 would enter on a command line `wonderbrowser–u http://www.bull.com` to open your wonderbrowser with the www.bull.compage open inside, you would type `wonderbrowser –u` into 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 this 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.
3. Configure and start your new web server software. Consult the documentation that came with your web server software and configure and start your webserver software. Write down the full pathnames of the webserver 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 BULL HTTP Webserver,and you installed them in their default location, you can skip this step). Also, some webservers may 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 will be using this computer as their documentation search server.
Note: If you are using the Lite Net Question web server software you do not need to do this step since the lite server can only be used for standalone documents serves. 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 AIX system management tools, Web–based System Manager or SMIT.

Using Web–based System Manager:

1. Change to the root user.
2. On the command line, type:

   ```
   wsm system
   ```

   to open the System Environments container.
3. In the System Environments window, double–click on the **Internet Environments** icon to open it.
4. In the notebook dialog, click on the **Documentation Server** tab. On this page, the **Local server** radio button should already be selected.
5. Under the heading **Location of documents and CGI programs on local server**, 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 two directories into the fields below Other. If you selected one of the default webserver packages, skip to the next step.
7. In the **Server port** field at the bottom, 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 will now be reconfigured to use the new webserver software. Any users who were logged in when configuration was done 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. then press Enter.
4. From the web configuration screen, select **Change Documentation and Search Server**.
5. 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.
6. 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 will now configure 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 CDE desktop, or the AIX 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 their computer's current default locale. The documentation language can be changed for all users on a computer, or it can be changed for a single user.

Note: 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.

Note: Before a computer can serve documents in a language, the AIX locale (language environment) for that language, and the library service messages for the language must be installed on the documentation server.

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 or SMIT.

Using Web–based System Manager:

1. Change to the root user.
2. On the command line, type:

   ```
   wsm system
   ```

   to open the System Environments container.
3. In the System Environments window, double–click on the **Internet Environments** icon to open it.
4. In the notebook dialog, click on the **Documentation Server** tab.
5. Scroll down until you see the **Default Documentation Language** field, then select your new language.
6. Click **OK**. The documentation service on this computer will now be 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
   ```

   then press Enter.
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 this computer will now be 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 may assign a single user a documentation language that is different than the default language of the user's computer. This is done by running (as **root**) the following command:

```
/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 AIX Language Support Table.

Running the command as described above will add 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), you can 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 CDE Desktop, 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 (as **root**) the following command:

```
/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
- Updating Documents
- Moving Documents
- Security

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; and,
2. The document and its index must be registered with the library service.

You can register documents two ways:

- If an application ships pre–built indexes for its documents, you can register the indexes automatically when you install them on your system; or,
- You can manually create indexes for documents that are already on the server and then manually register the indexes.

This section gives 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 Documentation Library Service in *AIX 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 Documentation Library Service in *AIX General Programming Concepts: Writing and Debugging Programs* and 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 will display 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 may want a library application that only shows accounting documents. For instructions, read the section on creating your own custom library applications in *AIX 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 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 the operating system's normal software uninstall tools to remove the document. If you simply delete a registered document or its index, it will still be registered with the library service. This will generate error messages during searches since the search service will still try to search the missing index.

Note: If you uninstall a package and it does not correctly remove all its indexes, use the procedure below 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 General Programming Concepts: Writing and Debugging Programs*.

Updating Documents

If a document's contents 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 should automatically update the old indexes with the new ones. If you are updating a document that a user created, you will have to manually update the index for the document.

1. Unregister and delete the old index. You **cannot** just delete an index. This will leave the search service corrupted. Follow the procedure in Removing Indexes in Your Documentation in *AIX General Programming Concepts: Writing and Debugging Programs*.
2. Rebuild the index. See Building the Index in *AIX General Programming Concepts: Writing and Debugging Programs* for more information.

Moving Documents

You should **not** move application documents that were automatically installed with an application. For example, you should not move operating system base documentation after it is installed. If you move automatically registered documents, the search service will be unable to find the documents and errors will 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's path has changed so that the service can find the document.

The first part of a document's 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's path depending on which part of the path you are changing.

To determine which method you need to use, type, as root (or a member of the **imnadm** group, the following command:

1. `/usr/IMNSearch/cli/imndomap /var/docsearch/indexes -l <index_name>`

   where <index_name> is replaced with the name of the index that contains the documents you want to move.

   The command will output something like this:

   ```
   Index <index_name> - <index_title>, documents in:
   <path> NetQ function completed.
   ```

   The <path> in the output shows you the part of your document's 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 described below. 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 instead update the index. This is because the lower part of the path is stored inside the index. To update the index, go back to the Updating Documents section and complete all the instructions in that section. You should 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's path in the index registration table, type the following two command parts. These two parts must all be typed on **one** command line with a single space between each part.

   Note: There must be a final slash (/) after the <path> as shown below.

3. If your document is written in a **single–byte language**, type the following two commands, pressing Enter after each:

   ```
   /usr/IMNSearch/cli/imndomap

   /var/docsearch/indexes –u <index_name>  /<path>/  <index_title>
   ```

4. If **double–byte language**, type (all on one line):

   ```
   /usr/IMNSearch/cli/imqdomap

   /var/docsearch/indexes –u <index_name> /<path>/ <index_title>
   ```

   In the above commands you replace the "/<path>/" part of the command with the new path where you moved your document. You replace <index_name> and <index_title> with the values you wrote down from the output of the command in the first step.

   For example, your documents are in the **acctn3en English(single–byte)** index and the index title is "Accounting Documents". You moved these document's tree from the /**doclink**/**en_US**/**engineering** directory into the /**doclink**/**en_US**/**accounting** directory. You would type (all on one line):

   ```
   /usr/IMNSearch/cli/imndomap

   /var/docsearch/indexes –u acctn3en

   /doc_link/en_US/accounting/  Accounting Documents
   ```

   Note: If you need to, you can change the index title by typing a new title in the above command. You **cannot** change the **index_name**.

5. Next, copy the index registration table with the changed entry over the backup copy of the registration. Type:

   ```
   cp /var/docsearch/indexes/imnmap.dat /usr/docsearch/indexes
   ```

   then press Enter. You **must** do this because the Documentation Library Service sometimes requires two copies of the table to process.

   Changing of the document's library service location is now complete. If you haven't 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 should correctly display 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 webserver software.

Indexes should be 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 should be 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 webserver users can both search and read all index files.

- **Search, but not read.**

  All webserver 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 level two above (to prevent reading of index files). In addition, a user's permission to use the search service webserver is disabled (this prevents searches). The user will be unable to search indexes because the webserver will not let them open the search form. This security level is set up using the administration functions in your webserver software to turn off a user's permission to use the webserver. See the documentation that came with your webserver to determine how to configure your webserver 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 AIX administration tools.

Note: If you add users to the **imnadm** group, they will be able to read the contents of all indexes on the system. See Security for more information, on page 18-15

Creating Custom Library Applications

When you open the global library application, all documents that are registered with the global view set are displayed. You may 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 Documentation Library Service in *AIX 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
- Error Message Listings

Note: If you receive an error message when using the AIX documentation search service, and your web browser is using a cache, that error message page will be stored in your web browser's cache. This means that even if you fix the problem that caused the error, the error message will continue to reappear 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's cache before you retest the search after you have done a fix. Usually, there is a **clear cache** function in a browser's Options screens.

Problems That Don't Generate Error Messages

- **In the global docsearch search form, the names of the volumes that are in a different languages have scrambled characters.**

  The volumes are written using different international character sets. The browser cannot display different character sets simultaneously.

- **When the search form appears it isn't in the correct default language of the search server computer.**

  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 should provide the search form in Spanish. Look at the Search link and see if it is specifying a language.

  OR

  The web server software may 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**

  ```
  The specific set of indexes requested to be shown in the search
  form are not registered with the search program. If you want to
  continue now, you can use the generic search page, which will
  allow you to search all volumes.

  Use generic page
  ```

  Invalid Index List

  This error occurs when the search form is passed a list of indexes names and none of them are names of indexes registered with the search engine.

  To get a list of the indexes registered with the search engine, run the following command:

  ```
  /usr/IMNSearch/cli/imnixlst
  ```

  To determine which indexes were passed to the search form, examine the HTML source for the link that was clicked on to get to the search form. The link may contain a list of indexes, or it may refer to a config file that contains a list of indexes.

  If the indexes to be searched do not appear on the list of indexes registered with the search engine, the indexes will need to be installed. If the indexes have already been installed and still don't show up in the list of indexes registered with the search engine, then their install process may not include automatic registration. In this case, see the System Administration guide, Creating Documents and Indexes.

- **ds_form: Error**

  ```
  The configuration file 'XXX' that specified the design of the
  search page does not exist or is read-protected.

  Make sure the file exists and that imnadm has permission to read
  the file. If you want to continue now, you can use the generic
  search page, which will allow you to search all volumes.

  Use generic page
  ```

  Invalid Configuration File

  This error occurs when the search form is passed a configuration file name and that file does not exist or is not readable by the user **imnadm**.

  In this message XXX will indicate the path and name of the configuration file as requested. If the file does exist and is readable to the user imnadm, make sure the full path is specified. If the path XXX given in the message does not match the path of the configuration file, then either move the file to the path specified by the error message, or edit the HTML link being used to call the search form and change the path given for the configuration file to match its location.

- **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.
  ```

  Search Engine Server stopped

  This error occurs if the NetQuestion search engine is not running.

  To start the NetQuestion search engine, you must be root or a member of the group imnadm. Start the NetQuestion search engine with the following command:

  ```
  imnss -start imnhelp
  ```

- **ds_form: Error**

  ```
  The search page is not available in the requested language
  'xx_XX'.
  ```

  Unavailable Language

  This error occurs if the search form is passed a language for which no message catalog is available, or no language is specified and there is no message catalog for the locale of the system.

  In this message xx_XX is the language for which there was no message catalog. If it is available, the message catalog for the language can be installed. Otherwise, specify a language for which there is a message catalog by using the lang parameter. For how to do this, see the developers guide.

- **ds_rslt: Error**

  ```
  No volumes were selected or no selected volumes were searchable.
  You must select at least one searchable volume.

  ds_rslt: Error EhwOpenIndex 1

  Error 77 in index INDEXNAME

  An error occurred when attempting to open or read an index file.
  Contact the system administrator of the search server computer.
  ```

  Index file permissions improperly set

This error occurs if the file permissions for the index specified by INDEXNAME are improperly set on files or directories that are part of that index.

Where INDEXNAME is the name of the 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 follow the following rules:

- All index files and directories should be readable by the user **imnadm**.
- All directories should be executable by the user imnadm.
- The work directory and all files in it should be writable by the user imnadm.
- The in the data directory the imnadmtb.dat and imniq.dat files should be writable.
- All index files and directories should 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 improperly 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
  ```

  Make sure all index file permissions follow the following rules:

  - All index files and directories should be readable by the user **imnadm**.
  - All directories should be executable by the user imnadm.
  - The work directory and all files in it should be writable by the user **imnadm**.
  - The in the data directory the imnadmtb.dat and imniq.dat files should be writable.
  - All index files and directories should 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 AIXASSEM

  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 imnixrst command:

  ```
  /usr/IMNSearch/cli/imnixrst <index name>
  ```

- **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 imnixrst command:

```
/usr/IMNSearch/cli/imnixrst <index name>
```

- **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 may say something like:

  ```
  ds_form is not an executeable.
  ```

  OR

  ```
  Cannot locate ds_form
  ```

  Documentation Library Service is not configured properly.

  The web server software cannot find the search service ds_form CGI program because the server has not been configured properly. Read the Installation and configuration section of this chapter and make sure the Documentation Library Service is installed and configured properly on the server computer.

Chapter 19. Using Power Management

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 4.3 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 20. 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:

See Devices in the *AIX 4.3 System User's Guide: 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 will 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 device's location code and SCSI address. Refer to "Installing a SCSI Device" for more information about installing SCSI devices, on page 20-3.

Procedure

This section documents installation tasks that are common to all devices. Due to the wide variety of devices that you can install on your system, only a general procedure is provided. Refer to 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 the Web-based System Manager fast path, **wsm devices**, or the SMIT fast path, **smit dev**, if you need to customize the device's attributes or if the device is one that the Configuration Manager cannot configure automatically (see the device documentation 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) will only support 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 may 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 may 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, enter 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 since the system was shipped from the factory.

1. Determine the SCSI I/O controllers installed in adapter slots by scanning the listing under "Built in items," in groups labeled "Adapters" or "Adapter Cards" for anything called "SCSI Controller" or "SCSI I/O Controller." The following is a sample entry from the *About Your Machine* document 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 400MB 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. Enter 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 sample below, 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 since 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. Use **shutdown –F** to stop the system immediately without notifying other users.
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 the Web-based System Manager fast path, **wsm 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 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 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 should be 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 using the 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 using the **shutdown –F** command and wait for a `Halt Completed` message.
3. 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 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. You would 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 Web-based System Manager fast path, **wsm 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 three 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, enter 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 the adapter slot number

6th digit indicates the controller 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 since 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. Enter 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 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.

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 since 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. Use **shutdown –F** to stop the system immediately without notifying other users.
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 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 fast path, **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. You would 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 Web-based System Manager fast path, **wsm devices**, or 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 Where
Connected
```

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):

   ```
   cfgmgr
   ```

2. Enter 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

Before you add, remove, or replace a hot plug adapter, you can display the following information about the 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**.

For additional information, see PCI Hot Plug Management in the *AIX 4.3 System Management Concepts: Operating System and Devices***.**

Web-based System Manager Fastpath Procedure

1. Type `wsm` devices at the system prompt, then press Enter, to start the Web-based System Manager Devices application.
2. In the Devices window, select **PCI hot plug Management** from the Device menu.
3. Use the PCI Hot Plug Management TaskGuide to complete the task.

To obtain additional information while completing the task, you can select the **More Info** button in the TaskGuide dialogs.

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 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 Commands Reference, Volume 3*

Unconfiguring Communications Adapters

This section provides the following procedures for unconfiguring communications adapters:

- Unconfiguring Ethernet, Token–ring, FDDI, and ATM Adapters
- Unconfiguring WAN Adapters
- Unconfiguring Other Adapters

Before you can remove or replace a hot plug adapter, you must unconfigure that adapter. 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 4.3 System Management Concepts: Operating System and Devices*.

Unconfiguring Ethernet, Token–ring, FDDI, and ATM Adapters

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 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. See Unconfiguring Communications Adapters in the *AIX 4.3 System Management Concepts: Operating System and Devices* for additional information.

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 IEEE 802.3 Ethernet interface To remove the standard Ethernet interface
`ifconfig` **`tr0`** `detach`	To remove a token–ring interface
`ifconfig` **`at0`** `detach`	To remove an ATM interface

See Unconfiguring Communications Adapters in the *AIX 4.3 System Management Concepts: Operating System and Devices* for an explanation of the association between these adapters and their interfaces.

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
r`mdev -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 option. *Do not* use this 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

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  AIX 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 *X.25 Version 1.1 for AIX: Option 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

See 2–Port Multiprotocol Adapter HDLC Network Device Driver Overview in the *AIX 4.3 System Management Guide: Communications and Networks* for additional information.

ARTIC960Hx PCI adapter	
`smit rmtsdd`	To unconfigure the device driver
`smit rmtsdports`	To remove an MPQP COMIO emulation port

See ARTIC960HX PCI Adapter Overview in the *AIX 4.3 System Management Guide: Communications and Networks* for additional information.

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**. See Unconfiguring Communications Adapters in the *AIX 4.3 System Management Concepts: Operating System and Devices* for additional information.

5. Use the ifconfig command to remove each interface from the network interface list. For example, `ifconfig en0 detach` to remove the standard Ethernet interface and `ifconfig et0` to remove the IEEE 802.3 interface. See Unconfiguring Communications Adapters in the *AIX 4.3 System Management Concepts: Operating*

System and Devices for an explanation of the association between these adapters and their interfaces.

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 option. *Do not* use this flag with the **rmdev** command for a hot plug operation unless your intent is to remove the adapter and not replace it.

ATM Adapters

There can be Classical IP and LAN emulation protocols running 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 (Multi Protocol Over ATM). Each LAN–emulated device must be unconfigured before you can remove the adapter.

See Unconfiguring Ethernet, Token–ring, FDDI, and ATM Adapters for instructions for removing a classical interface. To remove a LAN interface:

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 Problems that Occur While Removing an Adapter

If the following type of message displays when the rmdev command is used during the unconfiguration process, 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
- Tokenring DLC
- FDDI DLC

TCP/IP Applications

All TCP/IP applications using the interface layer can be detached with the ifconfig command. This causes the aplications 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.

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
- AIX Connections and NetBios

Applications Running on WAN Adapters

Applications that may be using your WAN adapter include:

- SDLC
- Bisync
- X.25
- ISDN
- QLLC for X.25

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 filesystems
- 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**.

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.

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. See Mounting or Unmounting a File System in the *AIX 4.3 System Management Guide: Operating System and Devices*.
5. Type rmdev –l adapter –R to make the adapter unavailable.

   Warning: 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**.

For additional information, see PCI Hot Plug Management in the *AIX 4.3 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.

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 Asynchronous Communication Guide*.
4. Type lsdev –C –c printer command 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 Guide to Printers and Printing*.
5. Use the rmdev command to make the adapter unavailable.

Warning: 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**.

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 4.3 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.

Web-based System Manager Fastpath Procedure

1. Type `wsm devices` at the system prompt, then press Enter, to start the Web-based System Manager Devices application.
2. In the Devices window, select **PCI hot plug Management** from the Device menu.
3. Use the PCI Hot Plug Management TaskGuide to complete the task.

To obtain additional information while completing the task, you can select the **More Info** button in the TaskGuide dialogs.

SMIT Fastpath Procedure

1. ype `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 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 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 *AIX 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**.

For additional information, see PCI Hot Plug Management in the *AIX 4.3 System Management Concepts: Operating System and Devices***.**

Note: When you add a hot plug adapter to the system, it 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.

Web-based System Manager Fastpath Procedure

1. Type `wsm devices` at the system prompt, then press Enter, to start the Web-based System Manager Devices application.
2. In the Devices window, select **PCI hot plug Management** from the Device menu.
3. Use the PCI Hot Plug Management TaskGuide to complete the task.

To obtain additional information for completing the task, you can get help in the following ways:

- In the Devices window, select **Contents** from the Help menu.
- In the TaskGuide dialogs, select the **More Info** button.

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 PCI hot plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 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 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 *AIX Commands Reference, Volume 2*.

For information about the physical handling of a PCI hot plug adapter, refer to your system unit documentation.

Chapter 21. 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, which contains information about the devices on your system. The device configuration database consists of the predefined configuration database, which contains information about all possible types of devices supported on the system, and the customized configuration database, which 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		
Web-based System Manager: **wsm devices** fast path (Devices application) –OR–		
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 *AIX Version 4.3 Problem Solving Guide and Reference*
Trace a Tape Drive	**smit trace_link**	See Starting the Trace Facility in *AIX Version 4.3 Problem Solving Guide and Reference*

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 (for **chdev**, the **mode** attribute) 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 (for **chdev**, the **extfm** attribute) 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 8mm tape drives use 2.2MB of tape and can take up to 8.5 seconds to write. Regular file marks use 184K and take approximately 1.5 seconds to write.

When you use an 8mm 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 (for **chdev**, the **ret** attribute) 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 (for **chdev**, the **density_set_1** attribute) 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 **chdev**, the **density_set_2** attribute) 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 21-14 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 tape drive's ability 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 (for **chdev**, the **res_support** attribute), 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 reserve/release commands. Some SCSI tape drives have a predefined value for this attribute so that reserve/release commands are always supported.

Variable Length Block Size

The Variable Length Block Size attribute (for **chdev**, the **var_block_size** attribute) 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 (for **chdev**, the **compress** attribute) 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 (for **chdev**, the **autoload** attribute) 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, will cause 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** is set to **EIO**. Once presented to the application, the error condition is cleared. Also, reconfiguring the tape drive itself will clear the error condition.

Attributes for 2.0GB 4mm 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 2.0GB 4mm 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 2.0GB mode.

Attributes for 4.0GB 4mm 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:

Media Type	Device Configuration
DDS	Read–only.
DDS ||||	Read/write in 2.0GB mode only.
DDS2	Read in either density; write in 4.0GB mode only.
non–DDS	Not supported; cartridge will eject.

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 4.0GB 4mm 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 2.3GB 8mm 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 2.3GB 8mm 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 2.3GB mode.

Attributes for 5.0GB 8mm Tape Drives (Type 8mm5gb)

Block Size

The default value is **1024**. If a tape is being written in 2.3GB 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	5GB mode (compression capable)
21	5GB mode noncompressed tape
20	2.3GB mode
0	Default (5.0GB 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 5GB 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 5.0GB 8mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 20000MB 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 20.0GB 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	20GB mode (compression capable)
0	Default (20.0GB 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 20.0GB 8mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 35GB Tape Drives (Type 35gb)

Block Size

The IBM 7205 Model 311 throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32K Bytes. Any block size less than 32K Bytes restricts the data rate (backup/restore time). The following table lists recommended block sizes by AIX command:

AIX Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32K or 51.2K (default)	Uses either 32K or 51.2 K depending on if ”Backup” is by name or not. No change is required.
TAR	10K	There is an error in the manual that states a 512K 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. The capacities of the 2.6GB format (density) and 6.0GB format (density) are significantly impacted when you use smaller than the recommended blocksizes. As an example: using a blocksize of 1024 bytes to backup 32GB of data takes approximately 22 hours. Backing up the same 32GB of data using a blocksize of 32K 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	2.6GB	2.6GB (No Compression)	23	17h
	6.0GB	6.0GB (No Compression)	24	18h
	10.0GB	20.0GB (Default for drive)	25	19h
DLTtapeIIIxt	15.0GB	30.6GB (Default for drive)	25	19h
DLTtapeIV	20.0GB	40.0GB	26	1Ah
	35.0GB	70.0GB (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 above 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 150MB 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 150MB 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 525MB 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 525MB 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 1200MB 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 1200MB 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 12000MB 4mm Tape Drives (Self Configuring)

Block Size

The IBM 12000MB 4mm Tape Drive's throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32K Bytes. Any block size less than 32K Bytes restricts the data rate (backup/restore time). The following table lists recommended block sizes by AIX command:

AIX Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32K or 51.2K (default)	Will use either 32K or 51.2 K depending on if "Backup" is by name or not. No change is required.
TAR	10K	There is an error in the manual that states a 512K 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 12000MB 4mm 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	2.0GB	4.0GB	19	13h
DDS2	4.0GB	8.0GB	36	24h
DDS3	12.0GB	24.0GB	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 above 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 13000MB 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
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 13000MB 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 properly, the front panel switch should 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**. 8mm and 4mm tape drives usually use **1024** and waste space on the tape if the block size attribute is left at **512**. **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's Density Setting #1 or with the tape drive's 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.

1. `/dev/rmt2.3`
2. `/dev/rmt2.1`
3. `/dev/rmt2`

These particular special files are chosen because:

- `/dev/rmt2.3` is chosen as the first file because this file has Retension–on–Open, which ensures that the first file is at the beginning of the tape. Rewind–on–Close is not chosen because the next I/O operation is to begin where this file ends. If the tape is already at the beginning when the first file is opened, using the `/dev/rmt2.1` file as the first file would be faster since time for retensioning the tape is eliminated.
- `/dev/rmt2.1` is chosen for the second file because this file has neither Retension–on–Open nor Rewind–on–Close chosen. There is no reason to go to the beginning of the tape either when the file is opened or when it is closed.
- `/dev/rmt2` is chosen for the third and final file because Retension–on–Open is not wanted since the third file is to follow the second file. Rewind–on–Close is selected because there are no plans to do any more writing after the third file on the tape. The next use of the tape will begin at the beginning of the tape.

Besides controlling tape operations by choosing a particular **rmt** special file, you can use the **tctl** command to control tape operations.

Index

Symbols

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull AIX 4.3 System Management Guide Operating System and Devices

Nº Reférence / Reference Nº : 86 A2 99HX 04

Daté / Dated : May 2000

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form
Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL ELECTRONICS ANGERS
CEDOC
ATTN / MME DUMOULIN
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

Managers / Gestionnaires :
Mrs. / Mme : **C. DUMOULIN** +33 (0) 2 41 73 76 65
Mr. / M : **L. CHERUBIN** +33 (0) 2 41 73 63 96

FAX : +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web site at: / Ou visitez notre site web à:
`http://www-frec.bull.com` (PUBLICATIONS, Technical Literature, Ordering Form)

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
[__] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

PHONE / TELEPHONE : _____ FAX : _____

E–MAIL : _____

For Bull Subsidiaries / Pour les Filiales Bull :
Identification: _____

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :
Customer Code / Code Client : _____

For Bull Internal Customers / Pour les Clients Internes Bull :
Budgetary Section / Section Budgétaire : _____

For Others / Pour les Autres :
Please ask your Bull representative. / Merci de demander à votre contact Bull.

PLACE BAR CODE IN LOWER LEFT CORNER

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 99HX 04

Bull

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

AIX

AIX 4.3 System Management Guide Operating System and Devices

86 A2 99HX 04

AIX

AIX 4.3 System Management Guide Operating System and Devices

86 A2 99HX 04

AIX

AIX 4.3 System Management Guide Operating System and Devices

86 A2 99HX 04