AIX 5L Version 5.2

System Management Guide: Operating System and Devices

SC23-4126-07

AIX 5L Version 5.2

System Management Guide: Operating System and Devices

SC23-4126-07

Note
Before using this information and the product it supports, read the information in “Notices,” on page 167.

Eighth Edition (August 2004)

This edition applies to AIX 5L Version 5.2 and to all subsequent releases of this product until otherwise indicated in new editions.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Information Development, Department H6DS-905-6C006, 11501 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial Internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

Contents

About This Book

This book contains information for understanding the tasks that you perform as a system administrator, as well as the tools provided for system management. Use this book along with *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Beginning with the AIX 5.2 documentation library, any information that this book contained regarding AIX system security, or any security-related topic, has moved. For all security-related information, see the *AIX 5L Version 5.2 Security Guide*.

This edition supports the release of AIX 5L Version 5.2 with the 5200-04 Recommended Maintenance package. Any specific references to this maintenance package are indicated as *AIX 5.2 with 5200-04*.

Who Should Use This Book

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

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

- *AIX 5L Version 5.2 System User's Guide: Operating System and Devices*
- *AIX 5L Version 5.2 System User's Guide: Communications and Networks*
- *AIX 5L Version 5.2 Installation Guide and Reference*

How to Use This Book

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

- Configuration tasks
- Maintenance tasks
- Troubleshooting

For conceptual information about system management tasks, see the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
Italics	Identifies parameters whose actual names or values are to be supplied by the user.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Case-Sensitivity in AIX

Everything in the AIX operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the

system responds that the command is ″not found.″ Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

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

Related Publications

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

- *AIX 5L Version 5.2 System Management Guide: Communications and Networks*
- *AIX 5L Version 5.2 Security Guide*
- *AIX 5L Version 5.2 Installation Guide and Reference*
- *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*
- *AIX 5L Version 5.2 Communications Programming Concepts*
- *AIX 5L Version 5.2 Kernel Extensions and Device Support Programming Concepts*
- *AIX 5L Version 5.2 Files Reference*
- *Performance Toolbox Version 2 and 3 for AIX: Guide and Reference*
- *Common Desktop Environment 1.0: Advanced User's and System Administrator's Guide*

Chapter 1. How-To's for System Management Tasks

This chapter provides instructions for performing the following system management tasks:

Add a Removable Media Drive

The following procedure uses SMIT to add a CD-ROM drive to your system. Other types of removable media drives are added using different fast paths but all follow the same general procedure. You can also add a removable media drive using Web-based System Manager, the Configuration Manager, or the **mkdev** command.

1. To add a CD-ROM drive to your system, install the hardware according to the documentation that came with your system.
2. With root authority, type the following SMIT fast path:

   ```
   smit makcdr
   ```
3. In the next screen, select the drive type from the available list of supported drives.
4. In the next screen, select the parent adapter from the available list.
5. In the next screen, at minimum, select the connection address from the available list. You can also use this screen to select other options. When you are finished, press Enter, and then SMIT adds the new CD-ROM drive.

At this point, the new CD-ROM drive is recognized by your system. To add a read/write optical drive, use the **smit makomd** fast path. To add a tape drive, use the **smit maktpe** fast path.

Compare File Systems on Different Machines

When file systems that exist on different machines should be identical but you suspect one is damaged, you can compare the file systems. The following procedure describes how to compare the attributes of a file system that resides on your current host (in this scenario, called *orig_host*) to the same file system on a remote host.

1. Log in to the remote host as the root user. For example:

   ```
   tn juniper.mycompany.com
   ```

```
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2002.
login: root
root's Password:
```

2. Using your favorite editor, edit the remote host's **.rhosts** file to add a stanza that allows the root user to execute secure remote commands. Use the following format for the new stanza:

   ```
   orig_host root
   ```

   The resulting **.rhosts** file might look similar to the following:

   ```
   NIM.mycompany.com root
   nim.mycompany.com root
   host.othernetwork.com root
   orig_host.mycompany.com root
   ```

3. Save your changes and exit the remote connection.
4. With root authority on *orig_host*, create another file using your favorite editor. For this scenario, the new file is named **compareFS**. For example:

   ```
   vi compareFS
   ```

5. Insert the following text in this file, where *FSname* is the name of the file system that you want to compare, and *remote_host* is the name of the host on which the comparison file system resides:

   ```
   FSname -> remote_host
   install -v ;
   ```

   Note: In the **install** command line of this file, there must be a space between the **-v** parameter and the semicolon (;).

   For example:

   ```
   /home/jane/* -> juniper.mycompany.com
   install -v ;
   ```

6. Save the file and exit the editor. The **compareFS** file is used as the *distfile* for the **rdist** command in the following step.
7. Type the following at the command prompt:

   ```
   /usr/bin/rdist -f compareFS
   ```

   Or, if you expect a significant amount of output from the comparison, send the output to a file name. For example:

   ```
   /usr/bin/rdist -f compareFS > compareFS_output
   ```

The output lists any differences between the file systems.

Configure Workload Manager (WLM) to Consolidate Workloads

Workload Manager (WLM) gives you control over the resources used by jobs on your system. A default WLM configuration template exists on every installed AIX operating system. The following procedure updates the WLM configuration template to implement a resource-management policy on a shared server. The resulting configuration can be used as a starting point for testing. Exactly how you configure WLM will depend on the workload and policy requirements for your environment.

Notes:

1. Efficient use of WLM requires extensive knowledge of existing system processes and performance. Repeated testing and tuning will probably be needed before you can develop a configuration that works well for your workload. If you configure WLM with extreme or inaccurate values, you can significantly degrade system performance.
2. The process of configuring WLM is simpler when you already know one or more of the classification attributes of a process (for example, user, group, or application name). If you are unfamiliar with the

current use of resources, use a tool such as **topas** to identify the processes that are the primary resource users and use the resulting information as the starting point for defining classes and rules.

3. The following scenario assumes you are familiar with the basic Workload Manager concepts as described in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

The WLM configuration files exist in the **/etc/wlm/***ConfigurationName* directory. Each subclass for each superclass is defined in a configuration file named **/etc/wlm/***ConfigurationName/SuperClassName*. For more information about these files, see the *AIX 5L Version 5.2 Files Reference*.

In the following procedure, you consolidate the workloads from two separate department servers onto one larger server. This example edits the configuration files, but you can also create a configuration using SMIT (use the **smit wlmconfig_create** fast path) or Web-based System Manager (select the **Workload Manager** container, select the **Configuration/Classes** container, then from the **Workload** menu, select **New Configuration**). Briefly, in this procedure, you will do the following:

1. Identify the resource requirements of the applications you want to consolidate. This will help you determine how many applications you can move to the larger server.
2. Define tiers, as well as resource shares and limits, to begin testing with the consolidated workload.
3. Fine-tune the configuration until you achieve your desired results.

Step 1. Identify Application Requirements

In this scenario, the workload is typical of what you might see on a database server. Assume the jobs fall into the following general categories:

Listeners
: These are processes that sleep most of the time and wake up periodically in response to a request. Although these processes do not consume a lot of resources, response time can be critical.

Workers
: These are processes that do the work on behalf of a request, whether the request is local or remote. These processes probably use a lot of CPU time and memory.

Reporters
: These are processes that do automated tasks. They might require a lot of CPU time or memory, but they can tolerate a slower response time.

Monitors
: These are processes that typically run periodically to verify the state of the system or applications. These processes might use a significant amount of resource, but only for a short time.

Commands
: These are commands or other applications that system users might run at any time. Their resource requirements are unpredictable.

In addition to this work, scheduled jobs fall into one of the following categories:

SysTools
: These are processes that perform automated tasks. These jobs are not critical to system operation but need to run periodically and within certain time constraints.

SysBatch
: These are processes that run infrequently, are not critical to system operation, and need not finish in a timely manner.

The first step of creating a configuration is to define classes and rules. In the following steps, you will use the general job categories listed above to define your classes. Use the following procedure:

1. Make a new configuration within the **/etc/wlm** directory called **MyConfig** using the following command:
   ```
   mkdir /etc/wlm/MyConfig
   ```

2. Copy the template files into the **/etc/wlm/MyConfig** directory using the following command:

   ```
   cp -pr /etc/wlm/template/* /etc/wlm/MyConfig
   ```

3. To create the superclasses, use your favorite editor to modify the **/etc/wlm/MyConfig/classes** file to contain the following:

   ```
   System:

   Default:

   DeptA:

   DeptB:

   SysTools:

   SysBatch:
   ```

   As a starting point, you define one superclass for each department (because two departments will be sharing the server). The SysTool and SysBatch superclasses will handle the scheduled jobs outlined in the general categories above. The System and Default superclasses are always defined.

4. Within the **MyConfig** directory, create a directory for each the DeptA and DeptB superclasses. (When creating a configuration, you must create a directory for every superclass that has subclasses.) In the following step, you define five subclasses (one for each category of work) for each department's superclass.

5. To create subclasses for each general category of jobs, edit the **/etc/wlm/MyConfig/DeptA/classes** and **/etc/wlm/MyConfig/DeptB/classes** files to contain the following:

   ```
   Listen:

   Work:

   Monitor:

   Report:

   Command:
   ```

   Note: The contents of the **classes** file can be different for each superclass.

   After the classes are identified, in the following step, you create the classification rules that are used to classify processes at the superclass and subclass levels. For the sake of simplicity, assume that all applications run from known locations, that all processes from one department run under the deptA UNIX group, and that processes from the other department run under the deptB UNIX group.

6. To create the superclass assignment rules, modify the **/etc/wlm/MyConfig/rules** file to contain the following:

   ```
   DeptA - - deptA - -
   DeptB - - deptB - -
   SysTools - root,bin - /usr/sbin/tools/* -
   SysBatch - root,bin - /usr/sbin/batch/* -
   System - root - - -
   Default - - - - -
   ```

   Note: If more than one instance of the same application can be running and all classification attributes (other than the tag) are the same, use the **wlmassign** command or **wlm_set_tag** subroutine to differentiate between them by assigning them to different classes.

7. To create more specific subclass rules, create the **/etc/wlm/MyConfig/DeptA/rules** and **/etc/wlm/MyConfig/DeptB/rules** files with the following content:

```
Listen - - - /opt/myapp/bin/listen* -
Work - - - /opt/myapp/bin/work* -
Monitor - - - /opt/bin/myapp/bin/monitor -
Report - - - /opt/bin/myapp/report* -
Command - - - /opt/commands/* -
```

8. To determine the resource-consumption behavior of each class, start WLM in passive mode using the following command:

   ```
   wlmcntrl -p -d MyConfig
   ```

   After starting WLM in passive mode, you can run each application separately at first to gain a finer perspective of its resource requirements. You can then run all applications simultaneously to better determine the interaction among all classes.

An alternative method of identifying the application resource requirements might be to first run WLM in passive mode on the separate servers from which you are consolidating applications. The disadvantages to this approach are that you would have to re-create the configurations on the larger system, and the required percentage of resources will likely be different on the larger system.

Step 2. Define Tiers, Shares, and Limits

A WLM configuration is an implementation of a resource-management policy. Running WLM in passive mode provides information that helps you determine whether your resource-management policy is reasonable for the given workload. You can now define tiers, shares, and limits to regulate your workload based on your resource-management policy.

For this scenario, assume you have the following requirements:

- The System class must have the highest priority and be guaranteed access to a percentage of system resources at all times.
- The SysTools class must have access to a certain percentage of resources at all times, but not so much that it will significantly impact the applications that are running in DeptA and DeptB.
- The SysBatch class cannot interfere with any of the other work on the system.
- DeptA will receive 60% of the available resources (meaning resources that are available to the classes with shares) and DeptB will receive 40%. Within DeptA and DeptB:
  - Processes in the Listen class must respond to requests with a low latency, but must not consume a lot of resources.
  - The Work class must be allowed to consume the most resources. The Monitor and Command classes must consume some resource, but less than the Work class.
  - The Report class cannot interfere with any of the other work.

In the following procedure, you define tiers, shares, and limits:

1. To create the superclass tiers, use your favorite editor to modify the **/etc/wlm/MyConfig/classes** file to contain the following:

   ```
   System:

   Default:

   DeptA:
           localshm = yes
           adminuser = adminA
           authuser = adminA
           inheritance = yes

   DeptB:
           localshm = yes
           adminuser = adminB
           authuser = adminB
           inheritance = yes
   ```

```
SysTools:
        localshm = yes

SysBatch:
        tier = 1
        localshm = yes
```

The SysBatch superclass is put in tier 1 because this class contains very low-priority jobs that you do not want to interfere with the rest of the work on the system. (When a tier is not specified, the class defaults to tier 0.) Administration of each department's superclass is defined by the adminuser and authuser attributes. The inheritance attribute is enabled for DeptA and DeptB. All new processes started in a class with inheritance will remain classified in that class.

2. To create subclass tiers for each group of jobs, modify the **/etc/wlm/MyConfig/DeptA/classes** and **/etc/wlm/MyConfig/DeptB/classes** files to contain the following:

```
Listen:

Work:

Monitor:

Report:
        tier = 1
Command:
```

3. To assign the initial shares for the superclasses, edit the **/etc/wlm/MyConfig/shares** file to contain the following:

```
DeptA:
        CPU = 3
        memory = 3

DeptB:
        CPU = 2
        memory = 2
```

Because you assigned a CPU total of 5 shares, DeptA processes will have access to three out of five shares (or 60%) of the total CPU resources and DeptB processes will have access to two out of five (or 40%). Because you did not assign shares to the SysTools, System, and Default classes, their consumption targets will remain independent from the number of active shares, which gives them higher-priority access to resources than the DeptA and DeptB (until their limit is reached). You did not assign the SysBatch class any shares because it is the only superclass in tier 1, and therefore any share assignment is irrelevant. Jobs in the SysBatch class can only consume resources that are unused by all classes in tier 0.

4. To assign the initial shares for the subclasses, edit the **/etc/wlm/MyConfig/DeptA/shares** and **/etc/wlm/MyConfig/DeptB/shares** files to contain the following:

```
Work:
        CPU = 5
        memory = 5

Monitor:
        CPU = 4
        memory = 1

Command:
        CPU = 1
        memory = 1
```

Because you did not assign shares to the Listen class, it will have the highest-priority access (in the superclass) to resources when it requires them. You assigned the largest number of shares to the Work class because it has the greatest resource requirements. Accordingly, you assigned shares to the Monitor and Command classes based on their observed behavior and relative importance. You did not

assign shares to the Report class because it is the only subclass in tier 1, and therefore any share assignment is irrelevant. Jobs in the Report class can only consume resources that are unused by subclasses in tier 0.

In the following step of this example, you assign limits to classes that were not assigned shares. (You can also assign limits to classes with shares. See Managing Resources with WLM in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices* for more information.)

5. To assign limits to the superclasses, edit the **/etc/wlm/MyConfig/limits** file to contain the following:

```
Default:
        CPU = 0%-10%;100%
        memory = 0%-10%;100%

SysTools:
        CPU = 0%-10%;100%
        memory = 0%-5%;100%

System:
        CPU = 5%-50%;100%
        memory = 5%-50%;100%
```

   You assigned soft maximum limits to the System, SysTools, and Default classes to prevent them from significantly interfering with other work on the system. You assigned minimum limits to the System class for CPU and memory because this class contains processes that are essential to system operation, and it must be able to consume a guaranteed amount of resource.

6. To assign limits to the subclasses, edit the **/etc/wlm/MyConfig/DeptA/limits** and **/etc/wlm/MyConfig/DeptB/limits** files to contain the following:

```
Listen:
        CPU = 10%-30%;100%
        memory = 10%-20%;100%

Monitor:
        CPU = 0%-30%;100%
        memory = 0%-30%;100%
```

   Note: The limits can be different for each subclass file.

   You assigned soft maximum limits to the Listen and Monitor classes to prevent them from significantly interfering with the other subclasses in the same superclass. In particular, you do not want the system to continue accepting requests for jobs within the Work class, if the Work class does not have access to the resources to process them. You also assigned minimum limits to the Listen class to ensure fast response time. The minimum limit for memory ensures that pages used by this class will not be stolen by page replacement, resulting in faster execution time. The minimum limit for CPU ensures that when these processes can be run, they will have the highest-priority access (in the superclass) to the CPU resources.

Step 3. Fine-Tune the Configuration

Now that you have fully defined a configuration, you will run WLM in active mode to begin regulating the workload and analyzing how well your resource-management policy is being enforced. Based on your analysis, you might need to fine-tune your configuration to achieve your desired results. For maintenance, you might need to refine your configuration if your workload changes over time.

1. To start WLM in active mode, use the following command:

```
wlmcntrl -a
```

2. Analyze the resource consumption using a command such as **wlmstat**.
3. If your desired consumption or performance goals for a particular class or application are not being met, you might need to adjust your WLM configuration to correct the problem. For guidelines, see WLM Troubleshooting Guidelines in the *AIX 5L Version 5.2 System Management Guide: Operating System and Devices*.

4. If you changed the configuration, update the active configuration for WLM using the following command:

   ```
   wlmcntrl -u
   ```

5. Analyze the resource consumption (step 2 on page 7) and, if necessary, fine-tune the configuration again.

Copy a JFS to Another Physical Volume

The following scenario describes copying JFS file system to a different physical volume while retaining file system integrity.

Table 1. Things to Consider

For the following scenario to be successful in a concurrent volume group environment, AIX 4.3.2 or later must be installed on all concurrent nodes.

To copy a JFS to another physical volume while maintaining file system integrity, do the following:

1. Stop activity for the file system that you want to copy. Unless the application that is using the file system is quiescent or the file system is in a state that is known to you, you cannot know what is in the data of the backup.
2. Mirror the logical volume, by typing the following SMIT fast path on the command line:

   ```
   smit mklvcopy
   ```

3. Copy the file system, using the the following command:

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

   The **splitcopy** parameter for the **-a** flag causes the command to split off a mirrored copy of the file system and mount it read-only at the new mount point. This action provides a copy of the file system with consistent journaled meta data that can be used for backup purposes.
4. If you want to move the mirrored copy to a different mount point, use the following SMIT fast path:

   ```
   smit cplv
   ```

At this point, the file system copy is usable.

Define a Raw Logical Volume for an Application

A *raw logical volume* is an area of physical and logical disk space that is under the direct control of an application, such as a database or a partition, rather than under the direct control of the operating system or a file system. Bypassing the file system can yield better performance from the controlling application, especially from database applications. The amount of improvement, however, depends on factors such as the size of a database or the application's driver.

Note: You will need to provide the application with the character or block special device file for the new raw logical volume, as appropriate. The application will link to this device file when it attempts 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. In a raw logical volume, the LVCB is not protected. If an application overwrites the LVCB, commands that normally update the LVCB will fail and generate a message. Although the logical volume might continue to operate correctly and the overwrite can be an allowable event, overwriting the LVCB is not recommended.

The following instructions use SMIT and the command line interface to define a raw logical volume. You can also use the **Create a new logical volume** wizard in Web-based System Manager (select **Volumes** →

Overview and Tasks → **Create a new logical volume**). To define a raw logical volume within the wizard, accept the default use, **applications and data**, from its first selection screen. Online help is available if you need it.

1. With root authority, find the free physical partitions on which you can create the raw logical volume by typing the following SMIT fast path:

   ```
   smit lspv
   ```

2. Select a disk.
3. Accept the default in the second dialog (status) and click OK.
4. Multiply the value in the FREE PPs field by the value in the PP SIZE field to get the total number of megabytes available for a raw logical volume on the selected disk. If the amount of free space is not adequate, select a different disk until you find one that has enough available free space.
5. Exit SMIT.
6. Use the **mklv** command to create the raw logical volume. The following command creates a raw logical volume named `lvdb2003` in the `db2vg` volume group using `38` 4-MB physical partitions:

   ```
   mklv -y lvdb2003 db2vg 38
   ```

   Use the **-y** flag to provide a name for the logical volume instead of using a system-generated name.

At this point, the raw logical volume is created. If you list the contents of your volume group, a raw logical volume is shown with the default type, which is jfs. This type entry for a logical volume is simply a label. It does not indicate a file system is mounted for your raw logical volume.

Consult your application's instructions on how to open **/dev/***rawLVname* and how to use this raw space.

Fix a Corrupted Magic Number in the File System Superblock

If the superblock of a file system is damaged, the file system cannot be accessed. Most damage to the superblock cannot be repaired. The following procedure describes how to repair a superblock in a JFS file system when the problem is caused by a corrupted magic number. If the primary superblock is corrupted in a JFS2 file system, use the **fsck** command to automatically copy the secondary superblock and repair the primary superblock.

In the following scenario, assume **/home/myfs** is a JFS file system on the physical volume **/dev/lv02**.

1. Unmount the **/home/myfs** file system, which you suspect might be damaged, using the following command:

   ```
   umount /home/myfs
   ```

2. To confirm damage to the file system, run the **fsck** command against the file system. For example:

   ```
   fsck -p /dev/lv02
   ```

   If the problem is damage to the superblock, the **fsck** command returns one of the following messages:

   ```
   fsck: Not an AIXV5 file system
   ```

   OR

   ```
   Not a recognized filesystem type
   ```

3. With root authority, use the **od** command to display the superblock for the file system, as shown in the following example:

   ```
   od -x -N 64 /dev/lv02 +0x1000
   ```

   Where the **-x** flag displays output in hexadecimal format and the **-N** flag instructs the system to format no more than 64 input bytes from the offset parameter (+), which specifies the point in the file where the file output begins. The following is an example output:

```
0001000  1234 0234 0000 0000 0000 4000 0000 000a
0001010  0001 8000 1000 0000 2f6c 7633 0000 6c76
0001020  3300 0000 000a 0003 0100 0000 2f28 0383
0001030  0000 0001 0000 0200 0000 2000 0000 0000
0001040
```

In the preceding output, note the corrupted magic value at 0x1000 (`1234 0234`). If all defaults were taken when the file system was created, the magic number should be 0x43218765. If any defaults were overridden, the magic number should be 0x65872143.

4. Use the **od** command to check the secondary superblock for a correct magic number. An example command and its output follows:

```
$ od -x -N 64 /dev/lv02 +0x1f000
001f000  6587 2143 0000 0000 0000 4000 0000 000a
001f010  0001 8000 1000 0000 2f6c 7633 0000 6c76
001f020  3300 0000 000a 0003 0100 0000 2f28 0383
001f030  0000 0001 0000 0200 0000 2000 0000 0000
001f040
```

Note the correct magic value at 0x1f000.

5. Copy the secondary superblock to the primary superblock. An example command and output follows:

```
$ dd count=1 bs=4k skip=31 seek=1 if=/dev/lv02 of=/dev/lv02
dd: 1+0 records in.
dd: 1+0 records out.
```

6. Use the **fsck** command to clean up inconsistent files caused by using the secondary superblock. For example:

```
fsck /dev/lv02 2>&1 | tee /tmp/fsck.errs
```

Make an Online Backup of a Mounted JFS or JFS2

Making an online backup of a mounted journaled file system (JFS) or enhanced journaled file system (JFS2) creates a static image of the logical volume that contains the file system. The following procedures describe how to make an online backup. Which procedure you choose depends on whether the file system is a JFS or JFS2.

Make an Online Backup of a JFS

To make an online backup of a mounted JFS, the logical volume that the file system resides on and the logical volume that its log resides on must be mirrored.

Note: Because the file writes are asynchronous, the split off copy might not contain all data that was written immediately before the split. Any modifications that begin after the split begins might not be present in the backup copy. Therefore, it is recommended that file system activity be minimal while the split is taking place.

To split off a mirrored copy of the **/home/xyz** file system to a new mount point named **/jfsstaticcopy**, type the following:

```
chfs -a splitcopy=/jfsstaticcopy /home/xyz
```

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

```
chfs -a splitcopy=/jfsstaticcopy -a copy=1 /home/xyz
```

At this point, a read-only copy of the file system is available in **/jfsstaticcopy**. Any changes made to the original file system after the copy is split off are not reflected in the backup copy.

To reintegrate the JFS split image as a mirrored copy at the **/testcopy** mount point, use the following command:

```
rmfs /testcopy
```

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

Make and Back Up a Snapshot of a JFS2

Beginning with AIX 5.2, you can make a snapshot of a mounted JFS2 that establishes a consistent block-level image of the file system at a point in time. The snapshot image remains stable even as the file system that was used to create the snapshot, called the *snappedFS*, continues to change. The snapshot retains the same security permissions as the snappedFS had when the snapshot was made.

In the following scenario, you create a snapshot and back up the snapshot to removable media without unmounting or quiescing the file system, all with one command: **backsnap**. You can also use the snapshot for other purposes, such as accessing the files or directories as they existed when the snapshot was taken. You can do the various snapshot procedures using Web-based System Manager, SMIT, or the **backsnap** and **snapshot** commands.

To create a snapshot of the **/home/abc/test** file system and back it up (by name) to the tape device **/dev/rmt0**, use the following command:

```
backsnap -m /tmp/snapshot -s size=16M -i f/dev/rmt0 /home/abc/test
```

This command creates a logical volume of 16 megabytes for the snapshot of the JFS2 file system (**/home/abc/test**). The snapshot is mounted on **/tmp/snapshot** and then a backup by name of the snapshot is made to the tape device. After the backup completes, the snapshot remains mounted. Use the **-R** flag with the **backsnap** command if you want the snapshot removed when the backup completes.

Notify Administrator when Physical Volume Is Missing

Although AIX logs an error when a physical volume becomes inaccessible, there are circumstances in which an error can go undetected. For example, when the physical volume is part of a mirrored volume group, users do not notice a problem because a good copy of the data remains accessible. In such cases, automatic notification can alert the administrator to the problem before the users notice any disruption to their work.

The following procedure describes how to set up automatic notification when a physical volume is declared missing. By modifying the following procedure, you can track other errors that are significant to you.

1. With root authority, make a backup copy of the **/etc/objrepos/errnotify** ODM file. You can name the backup copy anything you choose. In the following example, the backup copy appends the **errnotify** file name with the current date:

   ```
   cd /etc/objrepos
   cp errnotify errnotify_current_date_
   ```

2. Use your favorite editor to create a file named **/tmp/pvmiss.add** that contains the following stanza:

   ```
   errnotify:
    en_pid = 0
    en_name = "LVM_SA_PVMISS"
    en_persistenceflg = 1
    en_label = "LVM_SA_PVMISS"
    en_crcid = 0
    en_type = "UNKN"
    en_alertflg = ""
    en_resource = "LVDD"
    en_rtype = "NONE"
    en_rclass = "NONE"
    en_method = "/usr/lib/ras/pvmiss.notify $1 $2 $3 $4 $5 $6 $7 $8 $9"
   ```

After you complete all the steps in this article, the error notification daemon will automatically expand the $1 through $9 in this script with detailed information from the error log entry within the notification message.

3. Use your favorite editor to create a file named **/usr/lib/ras/pvmiss.notify** with the following contents:

```
#!/bin/ksh
exec 3>/dev/console
print -u3 "?"
print -u3 - "--------------------------------------------"
print -u3 "ALERT!  ALERT!  ALERT!  ALERT!  ALERT!  ALERT!"
print -u3 ""
print -u3 "Desc: PHYSICAL VOLUME IS MISSING. SEE ERRPT."
print -u3 ""
print -u3 "Error label: $9"
print -u3 "Sequence number: $1"
print -u3 "Error ID: $2"
print -u3 "Error class: $3"
print -u3 "Error type: $4"
print -u3 "Resource name: $6"
print -u3 "Resource type: $7"
print -u3 "Resource class: $8"
print -u3 - "--------------------------------------------"
print -u3 "?"
mail - "PHSYICAL VOLUME DECLARED MISSING" root <<-EOF
--------------------------------------------
ALERT!  ALERT!  ALERT!  ALERT!  ALERT!  ALERT!
Desc: PHYSICAL VOLUME IS MISSING. SEE ERRPT.
Error label: $9
Sequence number: $1
Error ID: $2
Error class: $3
Error type: $4
Resource name: $6
Resource type: $7
Resource class: $8
--------------------------------------------
EOF
```

4. Save your file and exit the editor.
5. Set the appropriate permissions on the file you just created. For example:

```
chmod 755 /usr/lib/ras/pvmiss.notify
```

6. Type the following command to add the LVM_SA_PVMISS definition that you created in step 2 on page 11 to the ODM:

```
odmadd /tmp/pvmiss.add
```

At this point, the system runs the **/usr/lib/ras/pvmiss.notify** script whenever an LVM_SA_PVMISS error occurs. This scripts sends a message to the console and also sends mail to the root user.

Re-create a Corrupted Boot Image

The following procedure describes how to identify a corrupted boot image and re-create it. If your machine is currently running and you know the boot image has been corrupted or deleted, re-create the boot image by running the **bosboot** command with root authority.

Attention: Never reboot the system when you suspect the boot image is corrupted.

The following procedure assumes your system is not rebooting correctly because of a corrupted boot image. If possible, protect your system from a possible loss of data or functionality by scheduling your downtime when it least impacts your workload.

1. Insert the product media into the appropriate drive.
2. Power on the machine following the instructions provided with your system.

3. From the System Management Services menu, select **Multiboot**.
4. From the next screen, select **Install From**.
5. Select the device that holds the product media and then select **Install**.
6. Select the AIX version icon.
7. Follow the online instructions until you can select which mode you use for installation. At that point, select **Start Maintenance Mode for System Recovery**.
8. Select **Access a Root Volume Group**.
9. Follow the online instructions until you can select **Access this Volume Group and start a shell**.
10. Use the **bosboot** command to re-create the boot image. For example:

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

    If the command fails and you receive the following message:

    ```
    0301-165 bosboot: WARNING! bosboot failed - do not attempt to boot device.
    ```

    Try to resolve the problem using one of the following options, and then run the **bosboot** command again until you have successfully created a boot image:

    - Delete the default boot logical volume (hd5) and then create a new hd5.

    Or

    - Run diagnostics on the hard disk. Repair or replace, as necessary.

    If the **bosboot** command continues to fail, contact your customer support representative.

    Attention: If the **bosboot** command fails while creating a boot image, do not reboot your machine.
11. When the **bosboot** command is successful, use the **reboot** command to reboot your system.

Reduce the Size of a File System in Your Root Volume Group

The simplest way to reduce *all* file systems to their minimum size is to set the SHRINK option to **yes** when restoring the base operating system from backup. The SHRINK option and the following scenario cannot be used in tandem. If you set the SHRINK option to **yes** after doing the following procedure, the installation overrides your changes to the **/image.data** file.

This scenario leads you through a manual process to reduce the size of a selected rootvg file system. You will identify a file system that is not using all of its allocated disk space and then reallocate based on the amount of space the file system actually uses, thus freeing more space for the root volume group's use. As part of this procedure, you will back up your volume groups and reinstall the operating system, using the revised allocations.

Attention: This procedure requires shutting down and reinstalling the base operating system. Whenever you reinstall any operating system, schedule your downtime when it least impacts your workload to protect yourself from a possible loss of data or functionality. Before reinstalling the operating system, ensure you have reliable backups of your data and any customized applications or volume groups.

1. Create a separate backup of all file systems that are *not* contained in the rootvg. The separate backup helps ensure the integrity of all your file systems.
2. With root authority, check which file systems in your root volume group are not using their allocated disk space by typing the following command:

   ```
   df -k
   ```

   The **-k** flag displays the file-system sizes in kilobytes. Your result will look similar to the following:

   ```
   Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
   /dev/hd4           196608      4976   98%     1944     2% /
   /dev/hd2          1769472    623988   65%    36984     9% /usr
   /dev/hd9var        163840     65116   61%      676     2% /var
   /dev/hd3            65536     63024    4%      115     1% /tmp
   ```

```
/dev/hd1            49152      8536   83%      832     7% /home
/proc                 -          -     -        -      -  /proc
/dev/hd10opt        32768     26340   20%      293     4% /opt
```

Looking at these results, you notice a large number of free blocks and a fairly low percentage of use associated with the file system that is mounted on **/usr**. You decide you can release a significant number of blocks by reducing the number of partitions allocated to the **/usr** file system.

3. Check the contents of the **/etc/filesystems** file to ensure that all file systems in the rootvg are mounted. If not, they will not be included in the reinstalled system.
4. Create an **/image.data** file, which lists all the active file systems in the rootvg that are included in the installation procedure, by typing the following command:

   ```
   mkszfile
   ```

5. Open the **/image.data** file in your favorite editor.
6. Search for the `usr` text string to locate the lv_data stanza that pertains to the **/usr** file system. Use numbers from this stanza as a base to determine how much you can reduce the **/usr** file system's number of logical partitions. The default size of each additional logical partition is defined in the `PP_SIZE` entry of the **/image.data** file. Your **/image.data** file would look similar to the following:

   ```
   lv_data:
    VOLUME_GROUP= rootvg
    LV_SOURCE_DISK_LIST= hdisk0
    LV_IDENTIFIER= 00042345d300bf15.5
    LOGICAL_VOLUME= hd2
    VG_STAT= active/complete
    TYPE= jfs
    MAX_LPS= 32512
    COPIES= 1
    LPs= 108
    STALE_PPs= 0
    INTER_POLICY= minimum
    INTRA_POLICY= center
    MOUNT_POINT= /usr
    MIRROR_WRITE_CONSISTENCY= on/ACTIVE
    LV_SEPARATE_PV= yes
    PERMISSION= read/write
    LV_STATE= opened/syncd
    WRITE_VERIFY= off
    PP_SIZE= 16
    SCHED_POLICY= parallel
    PP= 108
    BB_POLICY= relocatable
    RELOCATABLE= yes
    UPPER_BOUND= 32
    LABEL= /usr
    MAPFILE=
    LV_MIN_LPS= 70
    STRIPE_WIDTH=
    STRIPE_SIZE=
   ```

   The number of logical partitions devoted to this logical volume is 108 (`LPs=108`).
7. Determine the number of logical partitions needed by the existing data in the **/usr** file system by using your result from step 2. You can display the existing file sizes specifically for the **/usr** file system by using the following command:

   ```
   df -k /usr
   ```

   The result repeats the numbers (in kilobytes) you received for the **/usr** file system in step 2. For example:

   ```
   Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
   /dev/hd2          1769472    623988   65%    36984     9% /usr
   ```

   a. Subtract the amount of free space from the total number of 1024-blocks allocated:

      ```
      1769472 - 623988 = 1145484
      ```

b. Add an estimate of the space you might need to accommodate any future growth expected in this file system. For this example, add 200000 to the result.

```
1145484 + 200000 = 1345484
```

c. Divide the result by the logical-partition size in bytes (16*1024) to determine the minimum number of logical partitions you need.

```
1345484 / 16384 = 82.121826171875
```

Use this result, rounded upward, to redefine the number of logical partitions needed (LPs=83).

8. In your **image.data** file, change the LPs field from 108 to 83.
9. Find the fs_data stanza that pertains to the **/usr** file system. Your fs_data stanza will look similar to the following:

```
fs_data:
 FS_NAME= /usr
 FS_SIZE= 3538944
 FS_MIN_SIZE= 2290968
 FS_LV= /dev/hd2
 FS_FS= 4096
 FS_NBPI= 4096
 FS_COMPRESS= no
 FS_BF= false
 FS_AGSIZE= 8
```

10. Calculate the file-system size (FS_SIZE) by multiplying the physical partition size (PP_SIZE) by 2 (the number of 512-byte blocks used by the physical partitions) by the number of logical partitions (LPs). Given the values used in this example, the calculation is:

```
PP_SIZE * 512 blocks * LPs = FS_SIZE
16384 * 2 * 83 = 2719744
```

11. In your **image.data** file, change the FS_SIZE field from 3538944 to 2719744.
12. Calculate the minimum file-system size (FS_MIN_SIZE) based on the actual size of the current data used by the **/usr** file system, as follows:
    a. Calculate the minimum number of partitions needed. Given the values used in this example, the calculation is:

```
size_in_use (see step 7a) / PP_SIZE = partitions
1145484 / 16384 = 69.914794921875
```

    b. Calculate the minimum size required by that number of partitions. Rounding the previous calculation results upward to 70, the calculation is:

```
PP_SIZE * 512 blocks * partitions = FS_MIN_SIZE
16384 * 2 * 70 = 2293760
```

13. In your **image.data** file, change the FS_MIN_SIZE field from 2290968 to 2293760.
14. Save your edits and exit the editor.
15. Unmount all file systems that are not in the rootvg volume group.
16. If you have any user-defined volume groups, type the following commands to vary off and export them:

```
varyoffvg VGName
exportvg VGName
```

17. With a tape in the tape drive, type the following command to initiate a complete system backup:

```
mksysb /dev/rmt0
```

This type of backup includes the file-system size information you specified in the **/image.data** file, which will be used later to reinstall your system with the new file-system sizes.

Note: To initiate this backup, you must run the **mksysb** command from the command line. If you use a system management tool, such as SMIT, the backup creates a new **image.data** file, overwriting the changes you have made.

18. Use this backup to reinstall the operating system using the **Install With Current System Settings** option. During the installation, check that the following options are set appropriately:
    - **Use Maps** must be set to **no**
    - **Shrink the File Systems** must be set to **no**

    If you need more information about the installation procedure, see the *AIX 5L Version 5.2 Installation Guide*.
19. After the operating system is installed, reboot the system in Normal mode. At this point, the **/usr** file system is resized, but your user-defined file systems are not available.
20. Mount all file systems by typing the following command:

    ```
    mount all
    ```

    If you receive `Device Busy` messages about file systems that are already mounted, you can ignore these messages.

At this point, your **/usr** file system is resized, your root volume group has more free space, and your file systems are usable.

Replace a Failed Physical Volume in a Mirrored Volume Group

The following scenario replaces a failed or failing disk associated with a physical volume within a mirrored volume group. In the instructions, you use the Configuration Manager to configure the new disk (named `hdisk10`), and then use the **replacepv** command to replace a physical volume in a mirrored volume group that resides, at least in part, on a failed disk drive (named `hdisk02`) without losing the physical volume's contents. You do not need to reboot or schedule down time to complete the following procedure.

1. Select a new disk drive that has a capacity at least as large as the failed disk.
2. With root authority, run the **Configuration Manager** to configure the new disk. Type the following on the command line:

    ```
    cfgmgr -l hdisk10
    ```

    Use the **-l** flag to configure only the specified device and any ″child″ devices. Without this flag, the **cfgmgr** command runs Configuration Manager against the entire system.
3. Replace the physical volume so it can begin using the new disk, using the following command:

    Note: If the mirror for the logical volume is stale, the **replacepv** command does not work correctly.

    ```
    replacepv hdisk02 hdisk10
    ```
4. When the associated mirrored volume group is the rootvg, you must also run the following commands to clear the failed disk from and add the new disk to the boot image:

    ```
    chpv -c hdisk02
    bootlist hdisk10
    bosboot -a
    ```

    The **chpv -c** command clears hdisk02 from the boot image. The **bootlist** command adds hdisk10 to the list of possible boot devices from which the system can be booted. The **bosboot -a** command creates a complete boot image on the default boot logical volume.

At this point, the physical volume `hdisk02` now maps to the newly configured `hdisk10`.

Reset an Unknown Root Password

The following procedure describes how to recover access to root privileges when the system's root password is unavailable or unknown. The following procedure requires some system downtime. If possible, schedule your downtime when it least impacts your workload to protect yourself from a possible loss of data or functionality.

1. Insert the product media for the same version and level as the current installation into the appropriate drive.
2. Power on the machine.
3. When the screen of icons appears, or when you hear a double beep, press the F1 key repeatedly until the **System Management Services** menu appears.
4. Select **Multiboot**.
5. Select **Install From**.
6. Select the device that holds the product media and then select **Install**.
7. Select the AIX version icon.
8. Define your current system as the system console by pressing the F1 key and then press Enter.
9. Select the number of your preferred language and press Enter.
10. Choose **Start Maintenance Mode for System Recovery** by typing **3** and press Enter.
11. Select **Access a Root Volume Group**. A message displays explaining that you will not be able to return to the Installation menus without rebooting if you change the root volume group at this point.
12. Type **0** and press Enter.
13. Type the number of the appropriate volume group from the list and press Enter.
14. Select **Access this Volume Group and start a shell** by typing **1** and press Enter.
15. At the # (number sign) prompt, type the **passwd** command at the command line prompt to reset the root password. For example:

    ```
    # passwd
    Changing password for "root"
    root's New password:
    Enter the new password again:
    ```

16. To write everything from the buffer to the hard disk and reboot the system, type the following:

    ```
    sync;sync;sync;reboot
    ```

When the login screen appears, the password you set in step 15 should now permit access to root privileges.

Restore Access to an Unlinked or Deleted System Library

When the existing **libc.a** library is not available, most operating system commands are not recognized. The most likely causes for this type of problem are the following:

- The link in **/usr/lib** no longer exists.
- The file in **/usr/ccs/lib** has been deleted.

The following procedure describes how to restore access to the **libc.a** library. This procedure requires system downtime. If possible, schedule your downtime when it least impacts your workload to protect yourself from a possible loss of data or functionality.

Restore a Deleted Symbolic Link

Use the following procedure to restore a symbolic link from the **/usr/lib/libc.a** library to the **/usr/ccs/lib/libc.a** path:

1. With root authority, set the LIBPATH environment variable to point to the **/usr/ccs/lib** directory by typing the following commands:

   ```
   # LIBPATH=/usr/ccs/lib:/usr/lib
   # export LIBPATH
   ```

   At this point, you should be able to execute system commands.
2. To restore the links from the **/usr/lib/libc.a** library and the **/lib** directory to the **/usr/lib** directory, type the following commands:

```
ln -s /usr/ccs/lib/libc.a /usr/lib/libc.a
ln -s /usr/lib /lib
```

At this point, commands should run as before. If you still do not have access to a shell, skip the rest of this procedure and continue with the next section, “Restore a Deleted System Library File.”

3. Type the following command to unset the LIBPATH environment variable.

```
unset LIBPATH
```

Restore a Deleted System Library File

The following procedure to restore a deleted system library file requires system downtime. The system is booted and then the library is restored from a recent **mksysb** tape.

1. Before your reboot, ensure the PROMPT field in the **bosinst.data** file is set to **yes**.
2. Insert a recent **mksysb** tape into the tape drive. The **mksysb** *must* contain the same OS and maintenance level as the installed system. If you restore a **libc.a** library from a **mksysb** that conflicts with the level on the installed system, you will not be able to issue commands.
3. Reboot the machine.
4. When the screen of icons appears, or when you hear a double beep, press the F1 key repeatedly until the **System Management Services** menu appears.
5. Select **Multiboot**.
6. Select **Install From**.
7. Select the tape device that holds the **mksysb** and then select **Install**. It can take several minutes before the next prompt appears.
8. Define your current system as the system console by pressing the F1 key and press Enter.
9. Select the number of your preferred language and press Enter.
10. Choose **Start Maintenance Mode for System Recovery** by typing **3** and press Enter.
11. Select **Access a Root Volume Group**. A message displays explaining that you will not be able to return to the Installation menus without rebooting if you change the root volume group at this point.
12. Type **0** and press Enter.
13. Type the number of the appropriate volume group from the list and press Enter.
14. Select **Access this Volume Group** by typing **2** and press Enter.
15. Mount the **/** (root) and **/usr** file systems by typing the following commands:

```
mount /dev/hd4 /mnt
mount /dev/hd2 /mnt/usr
cd /mnt
```

16. To restore the symbolic link for the **libc.a** library, if needed, type the following command:

```
ln -s /usr/ccs/lib/libc.a /mnt/usr/lib/libc.a
```

After the command runs, do one of the following:

- If the command is successful, skip to step 20 on page 19.
- If a message displays that the link already exists, continue with step 17.

17. Set the block size of the tape drive by issuing the following commands, where *X* is the number of the appropriate tape drive.

```
tctl -f /dev/rmtX rewind
tctl -f /dev/rmtX.1 fsf 1
restbyname -xvqf /dev/rmtX.1 ./tapeblksz
cat tapeblksz
```

If the value from the **cat tapeblksz** command is *not equal* to 512, type the following commands, replacing *Y* with the value from the **cat tapeblksz** command:

```
ln -sf /mnt/usr/lib/methods /etc/methods
/etc/methods/chgdevn -l rmtX -a block_size=Y
```

You should receive a message that rmt*X* has been changed.

18. Ensure the tape is at the correct location for restoring the library by typing the following commands (where *X* is the number of the appropriate tape drive):

    ```
    tctl -f /dev/rmtX rewind
    tctl -f /dev/rmtX.1 fsf 3
    ```

19. Restore the missing library using one of the following commands (where *X* is the number of the appropriate tape drive):
    - To restore the **libc.a** library only, type the following command:

      ```
      restbyname -xvqf /dev/rmtX.1 ./usr/ccs/lib/libc.a
      ```

    - To restore the **/usr/ccs/lib** directory, type the following command:

      ```
      restbyname -xvqf /dev/rmtX.1 ./usr/ccs/lib
      ```

    - To restore the **/usr/ccs/bin** directory, type the following command:

      ```
      restbyname -xvqf /dev/rmtX.1 ./usr/ccs/bin
      ```

20. Flush the data to disk by typing the following commands:

    ```
    cd /mnt/usr/sbin
    ./sync;./sync;./sync
    ```

21. Unmount the **/usr** and **/** (root) file systems by typing the following commands:

    ```
    cd /
    umount /dev/hd2
    umount /dev/hd4
    ```

    If either **umount** command fails, cycle power on this machine and begin this procedure again.

22. Reboot the system by typing the following command:

    ```
    reboot
    ```

After the system is rebooted, operating system commands should be available.

Split a Mirrored Disk from a Volume Group

Beginning with AIX 5.2, *snapshot* support helps you protect the consistency of your mirrored volume groups from potential disk failure. Using the snapshot feature, you can split off a mirrored disk or disks to use as a reliable (from the standpoint of the LVM metadata) point-in-time backup of a volume group, and, when needed, reliably reintegrate the split disks into the volume group. In the following procedure, you first split off a mirrored disk from a volume group and then you merge the split-off disk into the original volume group. To further ensure the reliability of your snapshot, file systems must be unmounted and applications that use raw logical volumes must be in a known state (a state from which the application can recover if you need to use the backup).

A volume group cannot be split if any one of the following is true:

- A disk is already missing.
- The last non-stale partition would be on the split-off volume group.
- Any stale partitions exist in the volume group, unless you use the force flag (**-f**) with the **splitvg** command.

Furthermore, the snapshot feature (specifically, the **splitvg** command) cannot be used in enhanced or classic concurrent mode. The split-off volume group cannot be made concurrent or enhanced concurrent and there are limitations to the changes allowed for both the split-off and the original volume group. For details, read the **chvg** command description in *AIX 5L Version 5.2 Commands Reference*.

1. Ensure that the volume group is fully mirrored and that the mirror exists on a disk or set of disks that contains only this set of mirrors.
2. To enable snapshot support, split off the original volume group (`origVG`) to another disk or set of disks, using the following command:

```
splitvg origVG
```

At this point, you now have a reliable point-in-time backup of the original volume group. Be aware, however, that you cannot change the allocation on the split-off volume group.

3. Reactivate the split-off disk and merge it into the original volume group using the following command:

```
joinvg origVG
```

At this point, the split-off volume group is now reintegrated with the original volume group.

Chapter 2. General Operating System Management Tasks

This chapter provides procedures for several routine maintenance tasks, including:

Starting and Stopping the System

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

The following topics are included in this chapter:

Booting an Uninstalled System

The procedure for booting a new or uninstalled system is part of the installation process. For information on how to boot an uninstalled system, see Start the System in the *AIX 5L Version 5.2 Installation Guide and Reference*.

Rebooting a Running System

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

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

Remotely Rebooting an Unresponsive System

The remote reboot facility allows the system to be rebooted through a native (integrated) serial port. The system is rebooted when the “reboot_string” is received at the port. This facility is useful when the system does not otherwise respond but is capable of servicing serial port interrupts. Remote reboot can be enabled on only one native serial port at a time. Users are expected to provide their own external security for the port. This facility runs at the highest device interrupt class and a failure of the UART (Universal Asynchronous Receive/Transmit) to clear the transmit buffer quickly may have the effect of causing other devices to lose data if their buffers overflow during this time. It is suggested that this facility only be used to reboot a machine that is otherwise hung and cannot be remotely logged into. File systems will *not* be synchronized, and a potential for some loss of data which has not been flushed exists. It is strongly suggested that when remote reboot is enabled that the port not be used for any other purpose, especially file transfer, to prevent an inadvertent reboot.

Two native serial port attributes control the operation of remote reboot.

reboot_enable

Indicates whether this port is enabled to reboot the machine on receipt of the remote **reboot_string**, and if so, whether to take a system dump prior to rebooting.

```
no        - Indicates remote reboot is disabled
reboot    - Indicates remote reboot is enabled
dump      - Indicates remote reboot is enabled, and prior to rebooting a system dump
            will be taken on the primary dump device
```

reboot_string

Specifies the remote **reboot_string** that the serial port will scan for when the remote reboot feature is enabled. When the remote reboot feature is enabled and the **reboot_string** is received on the port, a **’>’** character is transmitted and the system is ready to reboot. If a **’1’** character is received, the system is rebooted; any character other than **’1’** aborts the reboot process. The **reboot_string** has a maximum length of 16 characters and must not contain a space, colon, equal sign, null, new line, or Ctrl-\ character.

Remote reboot can be enabled through SMIT or the command line. For SMIT the path **System Environments -> Manage Remote Reboot Facility** may be used for a configured TTY. Alternatively, when configuring a new TTY, remote reboot may be enabled from the **Add a TTY** or **Change/Show Characteristics of a TTY** menus. These menus are accessed through the path **Devices -> TTY**.

From the command line, the **mkdev** or **chdev** commands are used to enable remote reboot. For example, the following command enables remote reboot (with the dump option) and sets the reboot string to **ReBoOtMe** on **tty1**.

```
chdev -l tty1 -a remreboot=dump -a reboot_string=ReBoOtMe
```

This example enables remote reboot on **tty0** with the current **reboot_string** in the database only (will take effect on the next reboot).

```
chdev -P -l tty0 -a remreboot=reboot
```

If the tty is being used as a normal port, then you will have to use the **pdisable** command before enabling remote reboot. You may use **penable** to reenable the port afterwards.

Booting from Hard Disk for Maintenance

Prerequisites

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

Procedure

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

1. To reboot, either turn the machine off and then power it back on, or press the reset button.
2. Press the key sequence for rebooting in maintenance mode that is specified in your hardware documentation.
3. The machine will boot to a point where it has a console device configured.

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

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

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

Booting a System That Crashed

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

Prerequisites

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

Procedure

1. Ensure that all hardware and peripheral devices are correctly connected.
2. Turn on all of the peripheral devices.
3. Watch the screen for information about automatic hardware diagnostics.
   - If any hardware diagnostics tests are unsuccessful, refer to the hardware documentation.
   - If all hardware diagnostics tests are successful, turn the system unit on.

Accessing a System That Will Not Boot

If you have a system that will not boot from the hard disk, see the procedure on how to access a system that will not boot in Troubleshooting in the *AIX 5L Version 5.2 Installation Guide and Reference*.

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

Notes:

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

Rebooting a System With Planar Graphics

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

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

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

Diagnosing Boot Problems

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

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

For information on accessing a system that will not boot from the disk drive, see “Accessing a System That Will Not Boot” on page 23.

Creating Boot Images

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

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

Prerequisites

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

  ```
  lsvg -l rootvg
  ```

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

  ```
  lsvg -M rootvg
  ```

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

Creating a Boot Image on a Boot Logical Volume

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

The **bosboot** command does the following:

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

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

```
bosboot -a
```

OR:

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

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

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

Creating a Boot Image for a Network Device

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

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

For a Token-Ring boot:

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

Identifying System Run Levels

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

Identifying the Current Run Level

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

Displaying a History of Previous Run Levels

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

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

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

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

   The system displays information similar to the following:

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

Changing System Run Levels

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

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

The following are the currently defined run levels:

0-9	When the **init** command changes to run levels 0-9, it kills all processes at the current run levels then restarts any processes associated with the new run levels.
0-1	Reserved for the future use of the operating system.
2	Default run level.
3-9	Can be defined according to the user's preferences.
a, b, c	When the **init** command requests a change to run levels **a**, **b**, or **c**, it does not kill processes at the current run levels; it simply starts any processes assigned with the new run levels.
Q, q	Tells the **init** command to reexamine the **/etc/inittab** file.

Changing Run Levels on Multiuser Systems

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

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

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

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

Changing Run Levels on Single-User Systems

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

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

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

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

Executing Run Level Scripts

Run level scripts allow users to start and stop selected applications while changing the run level.

Put run level scripts in the subdirectory of **/etc/rc.d** that is specific to the run level:

- **/etc/rc.d/rc2.d**
- **/etc/rc.d/rc3.d**
- **/etc/rc.d/rc4.d**
- **/etc/rc.d/rc5.d**
- **/etc/rc.d/rc6.d**
- **/etc/rc.d/rc7.d**
- **/etc/rc.d/rc8.d**
- **/etc/rc.d/rc9.d**

The **/etc/rc.d/rc** will run the start script it finds in the specified directory, and execute it when the run level changes. The script will first stop application scripts, then start application scripts.

Note:
Scripts beginning with **K** are stop scripts, while scripts beginning with **S** are start scripts.

Changing the /etc/inittab File

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

Adding Records - mkitab Command

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

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

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

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

In the above example:

`tty002`	Identifies the object whose run level you are defining.
`2`	Specifies the run level at which this process runs.
`respawn`	Specifies the action that the **init** command should take for this process.

`/usr/sbin/getty /dev/tty2`	Specifies the shell command to be executed.

Changing Records - chitab Command

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

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

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

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

In the above example:

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

Listing Records - lsitab Command

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

```
lsitab -a
```

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

```
lsitab Identifier
```

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

Removing Records

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

```
rmitab Identifier
```

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

Stopping the System

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

- "Shutting Down the System without Rebooting"
- "Shutting Down the System to Single-User Mode" on page 29
- "Shutting Down the System in an Emergency" on page 29

Shutting Down the System without Rebooting

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

Prerequisites

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

Procedure

To shut down the system using SMIT:

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

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

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

Shutting Down the System to Single-User Mode

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

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

Shutting Down the System in an Emergency

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

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

Reactivating an Inactive System

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

Use the following procedures to reactivate an inactive system:

- “Checking the Hardware”
- “Checking the Processes” on page 30
- “Restarting the System” on page 32

Checking the Hardware

Check your hardware by:

- “Checking the Power”
- “Checking the Operator Panel Display” on page 30 if available
- “Activating Your Display or Terminal” on page 30

Checking the Power: If the Power-On light on your system is active, go to “Checking the Operator Panel Display” on page 30

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

Checking the Operator Panel Display: If your system has an operator panel display, check it for any messages.

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

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

Activating Your Display or Terminal: Check several parts of your display or terminal, as follows:

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

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

If your system became inactive while you were trying to restart the system, go to “Restarting the System” on page 32.

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

Checking the Processes

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

- “Restarting Line Scrolling”
- “Using the Ctrl-D Key Sequence”
- “Using the Ctrl-C Key Sequence”
- “Logging In from a Remote Terminal or Host” on page 31
- “Ending Stalled Processes Remotely” on page 31

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

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

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

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

Using the Ctrl-D Key Sequence: End a stopped process by doing the following:

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

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

Using the Ctrl-C Key Sequence:

End a stopped process by doing the following:

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

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

Logging In from a Remote Terminal or Host:

Log in remotely in either of two ways:

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

  ```
  tn YourSystemName
  ```

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

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

If you were not able to log in to the system from a remote terminal or host, go to “Restarting the System” on page 32 .

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

Ending Stalled Processes Remotely:

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

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

   ```
   ps -ef
   ```

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

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

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

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

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

   ```
   kill -9 ProcessID
   ```

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

If your process checks have not corrected the problem with your inactive system, go to “Restarting the System” on page 32 .

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

Restarting the System

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

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

This procedure involves the following:

- "Checking the State of the Boot Device"
- "Loading the Operating System"

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

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

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

Loading the Operating System: Load your operating system by doing the following:

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

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

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

System Hang Management

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

shconf Command

The **shconf** command is invoked when `System Hang Detection` is enabled. The **shconf** command configures which events are surveyed and what actions are to be taken if such events occur. You can specify any of the following actions, the priority level to check, the time out while no process or thread executes at a lower or equal priority, the terminal device for the warning action, and the **getty** command action:

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

For the **Launch a command** and **Give a special getty** options, system hang detection launches the special **getty** command or the specified command at the highest priority. The special **getty** command prints a warning message that it is a recovering **getty** running at priority 0. The following table captures the various actions and the associated default parameters for priority hang detection. Only one action is enabled for each type of detection.

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

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

For lost IO detection, you can set the time out value and enable the following actions:

Option	Enablement
Display a warning message	disabled
Reboot the system	disabled

Lost IO events are recorded in the AIX error log file.

shdaemon Daemon

The **shdaemon** daemon is a process that is launched by **init** and runs at priority 0 (zero). It is in charge of handling system hang detection by retrieving configuration information, initiating working structures, and starting detection times set by the user.

Changing the System Hang Detection Configuration

You can manage the system hang detection configuration from the SMIT management tool. SMIT menu options allow you to enable or disable the detection mechanism, display the current state of the feature, and change or show the current configuration. The fast paths for system hang detection menus are:

smit shd
: Manage System Hang Detection

smit shstatus
: System Hang Detection Status

smit shpriocfg
: Change/Show Characteristics of Priority Problem Detection

smit shreset
: Restore Default Priority Problem Configuration

smit shliocfg
: Change/Show Characteristics of Lost I/O Detection

smit shlioreset
Restore Default Lost I/O Detection Configuration

You can also manage system hang detection using the **shconf** command, which is documented in *AIX 5L Version 5.2 Commands Reference*.

Backing Up and Restoring Information

This chapter contains the following procedures for backing up and restoring the operating system, applications, and data:

Compressing Files

Several methods exist for compressing a file system:

- Use the **-p** flag with the **backup** command.
- Use the **compress** or **pack** commands.

Files are compressed for the following reasons:

- Saving storage and archiving system resources:
  - Compress file systems before making backups to preserve tape space.
  - Compress log files created by shell scripts that run at night; it is easy to have the script compress the file before it exits.
  - Compress files that are not currently being accessed. For example, the files belonging to a user who is away for extended leave can be compressed and placed into a **tar** archive on disk or to a tape and later restored.
- Saving money and time by compressing files before sending them over a network.

Procedure

To compress the **foo** file and write the percentage compression to standard error, type:

```
compress -v foo
```

See the **compress** command for details about the return values but, in general, the problems encountered when compressing files can be summarized as follows:

- The command might run out of working space in the file system while compressing. Because the **compress** command creates the compressed files before it deletes any of the uncompressed files, it needs extra space-from 50% to 100% of the size of any given file.
- A file might fail to compress because it is already compressed. If the **compress** command cannot reduce the file size, it fails.

Backing Up User Files or File Systems

Two procedures can be used to back up files and file systems: the SMIT fast paths **smit backfile** or **smit backfilesys**, and the **backup** command.

For additional information about backing up user files or file systems, see "Backing Up User Files or File Systems" in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Prerequisites

- If you are backing up by i-node file systems that may be in use, unmount them first to prevent inconsistencies.

  Attention: If you attempt to back up a mounted file system, a warning message is displayed. The **backup** command continues, but inconsistencies in the file system may occur. This warning does not apply to the root (**/**) file system.
- To prevent errors, make sure the backup device has been cleaned recently.

Backing Up User Files or File Systems Tasks

Task	*SMIT Fast Path*	*Command or File*
Back Up User Files	**smit backfile**	1. Log in to your user account. 2. Backup: **find . -print | backup -ivf /dev/rmt0**
Back Up User File Systems	**smit backfilesys**	1. Unmount files systems that you plan to back up. For example: **umount all** or **umount /home /filesys1** 2. Verify the file systems. For example: **fsck /home /filesys1** 3. Back up by i-node. For example: **backup -5 -uf/dev/rmt0 /home/libr** 4. Restore the files using the following command:[Note] **restore -t**

Note: 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.

Prerequisites: Before backing up the rootvg volume group:

- All hardware must already be installed, including external devices, such as tape and CD-ROM drives.
- This backup procedure requires the **sysbr** fileset, which is in the BOS System Management Tools and Applications software package. Type the following command to determine whether the **sysbr** fileset is installed on your system:

  ```
  lslpp -l bos.sysmgt.sysbr
  ```

  If your system has the **sysbr** fileset installed, continue the backup procedures.

  If the **lslpp** command does not list the **sysbr** fileset, install it before continuing with the backup procedure. See Installing Optional Software and Service Updates in the *AIX 5L Version 5.2 Installation Guide and Reference* for instructions.

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

  where `device` is the location of the software; for example,`/dev/rmt0` for a tape drive.

Before backing up a user-defined volume group:

- Before being saved, a volume group must be varied on and the file systems must be mounted.

  Attention: Executing the **savevg** command results in the loss of all material previously stored on the selected output medium.
- Make sure the backup device has been cleaned recently to prevent errors.

Backing Up Your System Tasks

Task	*SMIT Fast Path*	*Command or File*
Backing up the **rootvg** volume group	1. Log in as root. 2. Mount file systems for backup.[1] **smit mountfs** 3. Unmount any local directories that are mounted over another local directory. **smit umountfs** 4. Make at least 8.8MB of free disk space available in the **/tmp** directory.[2] 5. Back up: **smit mksysb** 6. Write-protect the backup media. 7. Record any backed-up root and user passwords.	1. Log in as root. 2. Mount file systems for backup.[1] See **mount** command. 3. Unmount any local directories that are mounted over another local directory. See **umount** command. 4. Make at least 8.8MB of free disk space available in the **/tmp** directory.[2] 5. Back up. See **mksysb** command. 6. Write-protect the backup media. 7. Record any backed-up root and user passwords.
Verify a Backup Tape[3]	**smit lsmksysb**	
Backing up a user-defined volume group[4]	**smit savevg**	1. Modify the file system size before backing up, if necessary.[5] **mkvgdata** *VGName* then edit **/tmp/vgdata/***VGName***/***VGName***.data** 2. Save the volume group. See the **savevg** command.

Notes:

1. The **mksysb** command does not back up file systems mounted across an NFS network.
2. The **mksysb** command requires this working space for the duration of the backup. Use the **df** command, which reports in units of 512-byte blocks, to determine the free space in the **/tmp** directory. Use the **chfs** command to change the size of the file system, if necessary.
3. This procedure lists the contents of a **mksysb** backup tape. The contents list verifies most of the information on the tape but does not verify that the tape can be booted for installations. The only way to verify that the boot image on a **mksysb** tape functions correctly is by booting from the tape.
4. If you want to exclude files in a user-defined volume group from the backup image, create a file named **/etc/exclude.***volume_group_name*, where *volume_group_name* is the name of the volume group that you want to back up. Then edit **/etc/exclude.***volume_group_name* and enter the patterns of file names that you do not want included in your backup image. The patterns in this file are input to the pattern matching conventions of the **grep** command to determine which files are excluded from the backup.
5. If you choose to modify the *VGName***.data** file to alter the size of a file system, you must not specify the **-i** flag or the **-m** flag with the **savevg** command, because the *VGName***.data** file is overwritten.

For more information about installing (or *restoring*) a backup image, see ″Installing BOS from a System Backup″ in the *AIX 5L Version 5.2 Installation Guide and Reference*.

Implementing Scheduled Backups

This procedure describes how to develop and use a script to perform a weekly full backup and daily incremental backups of user files. The script included in this procedure is intended only as a model and needs to be carefully tailored to the needs of the specific site.

Prerequisites

- The amount of data scheduled for backup cannot exceed one tape when using this script.
- Make sure the tape is loaded in the backup device before the **cron** command runs the script.
- Make sure the device is connected and available, especially when using scripts that run at night. Use the **lsdev -C | pg** command to check availability.
- Make sure the backup device has been cleaned recently to prevent errors.
- If you are backing up file systems that might be in use, unmount them first to prevent file system corruption.
- Check the file system before making the backup. Use the procedure “Verify File Systems” on page 89 or run the **fsck** command.

Back Up File Systems Using the cron Command

This procedure describes how to write a **crontab** script that you can pass to the **cron** command for execution. The script backs up two user file systems, **/home/plan** and **/home/run**, on Monday through Saturday nights. Both file systems are backed up on one tape, and each morning a new tape is inserted for the next night. The Monday night backups are full archives (level 0). The backups on Tuesday through Saturday are incremental backups.

1. The first step in making the **crontab** script is to issue the **crontab-e** command. This opens an empty file where you can make the entries that are submitted to the **cron** script for execution each night (the default editor is **vi**). Type:

   ```
   crontab -e
   ```

2. The following example shows the six **crontab** fields. Field 1 is for the minute, field 2 is for the hour on a 24-hour clock, field 3 is for the day of the month, and field 4 is for the month of the year. Fields 3 and 4 contain an * (asterisk) to show that the script runs every month on the day specified in the `day/wk` field. Field 5 is for the day of the week, and can also be specified with a range of days, for example, 1-6. Field 6 is for the shell command being run.

   ```
   min hr day/mo mo/yr day/wk       shell command

   0   2    *     *       1         backup -0 -uf /dev/rmt0.1 /home/plan
   ```

   The command line shown assumes that personnel at the site are available to respond to prompts when appropriate. The `-0` (zero) flag for the `backup` command stands for level zero, or full backup. The `-u` flag updates the backup record in the **/etc/dumpdates** file and the `f` flag specifies the device name, a raw magnetic tape device 0.1 as in the example above. See rmt Special File in the *AIX 5L Version 5.2 Files Reference* for information on the meaning of extension .1 and other extensions (1-7).

3. Type a line similar to that in step 2 for each file system backed up on a specific day. The following example shows a full script that performs six days of backups on two file systems:

   ```
   0 2 * * 1 backup -0 -uf/dev/rmt0.1 /home/plan
   0 3 * * 1 backup -0 -uf/dev/rmt0.1 /home/run
   0 2 * * 2 backup -1 -uf/dev/rmt0.1 /home/plan
   0 3 * * 2 backup -1 -uf/dev/rmt0.1 /home/run
   0 2 * * 3 backup -2 -uf/dev/rmt0.1 /home/plan
   0 3 * * 3 backup -2 -uf/dev/rmt0.1 /home/run
   0 2 * * 4 backup -3 -uf/dev/rmt0.1 /home/plan
   0 3 * * 4 backup -3 -uf/dev/rmt0.1 /home/run
   0 2 * * 5 backup -4 -uf/dev/rmt0.1 /home/plan
   0 3 * * 5 backup -4 -uf/dev/rmt0.1 /home/run
   0 2 * * 6 backup -5 -uf/dev/rmt0.1 /home/plan
   0 3 * * 6 backup -5 -uf/dev/rmt0.1 /home/run
   ```

4. Save the file you created and exit the editor. The operating system passes the **crontab** file to the **cron** script.

Create a Remote Archive

Running AIX systems cannot mount a remote tape device as if it were local to the system; however, data can be sent to a remote machine tape device using the **rsh** command. This section describes how to archive files to a remote tape device. The following procedure writes to a single tape only. Multiple-tape archives require specialized application software.

In the following procedure, assume the following:

blocksize
: Represents the target tape device blocksize.

remotehost
: Is the name of the target system (the system that has the tape drive).

sourcehost
: Is the name of the source system (the system being archived).

/dev/rmt0
: Is the name of the remote tape device

pathname
: Represents the full pathname of a required directory or file.

The following instructions assume that both the local and remote user is root.

1. Ensure you have access to the remote machine. The source machine must have access to the system with the tape drive. (The target system can be accessed using any of the defined users on that system, but the user name must have root authority to do many of the following steps.)
2. Using your favorite editor, create a file in the **/** (root) directory of the target system called **.rhosts** that allows the source system access to the target system. You need to add the authorized host name and user ID to this file. To determine the name of the source machine for the **.rhosts** file, you can use the following command:

   ```
   host SourceIPaddress
   ```

   For the purposes of this example, assume you add the following line to the **.rhosts** file:

   ```
   sourcehost.mynet.com   root
   ```
3. Save the file and then change its permissions using the following command:

   ```
   chmod 600 .rhosts
   ```
4. Use the **rsh** command to test your access from the source machine. For example:

   ```
   rsh remotehost
   ```

   If everything is set up correctly, you should be granted shell access to the remote machine. You should not see a login prompt asking for a user name. Type **exit** to log out of this test shell.
5. Decide on the appropriate tape device blocksize. The following are the recommended values:

9-track or 0.25-in. media blocksize:	512
8-mm or 4-mm media blocksize:	1024

   If you are unsure and want to check the current block size of the tape device, use the **tctl** command. For example:

   ```
   tctl -f /dev/rmt0 status
   ```

   If you want to change the tape blocksize, use the **chdev** command. For example:

   ```
   chdev -l rmt0 -a block_size=1024
   ```
6. Create your archive using one of the following methods:

   Backup by Name
   : To remotely create a backup archive by name, use the following command:

```
find pathname -print | backup -ivqf- | rsh remotehost \
    "dd of=/dev/rmt0 bs=blocksize conv=sync"
```

Backup by inode

To remotely create a backup archive by inode, first unmount your file system then use the **backup** command. For example:

```
umount /myfs
backup -0 -uf- /myfs | rsh remotehost \
     "dd of=/dev/rmt0 bs=blocksize conv=sync"
```

Create and Copy an Archive to Remote Tape

To create and copy an archive to the remote tape device, use the following command:

```
find pathname -print | cpio -ovcB | rsh remotehost \
    "dd ibs=5120 obs=blocksize of=/dev/rmt0"
```

Create a tar Archive

To remotely create a **tar** archive, use the following command:

```
tar -cvdf- pathname | rsh remotehost \
    "dd of=/dev/rmt0 bs=blocksize conv=sync"
```

Create a Remote Dump

To remotely create a remote dump of the /myfs file system, use the following command:

```
rdump -u -0 -f remotehost:/dev/rmt0 /myfs
```

The **-u** flag tells the system to update the current backup level records in the **/etc/dumpdates** file. The **-0** is the setting of the *Level* flag. Backup level 0 specifies that all the files in the /myfs directory are to be backed up. For more information, see the **rdump** command description in *AIX 5L Version 5.2 Commands Reference*.

7. Restore your remote archive using one of the following methods:

Restore a Backup by Name

To restore a remote backup archive by name, use the following command:

```
rsh remotehost "dd if=/dev/rmt0 bs=blocksize" | restore \
     -xvqdf- pathname
```

Restore a Backup by inode

To restore a remote backup archive by inode, use the following command:

```
rsh remotehost "dd if=/dev/rmt0 bs=blocksize" | restore \
    -xvqf- pathname
```

Restore a Remote cpio Archive

To restore a remote archive created with the **cpio** command, use the following command:

```
rsh remotehost "dd if=/dev/rmt0 ibs=blocksize obs=5120" | \
     cpio -icvdumB
```

Restore a tar Archive

To restore a remote **tar** archive, use the following command:

```
rsh remotehost "dd if=/dev/rmt0 bs=blocksize" | tar -xvpf- pathname
```

Restore a Remote Dump

To restore a remote dump of the /myfs file system, use the following command:

```
cd /myfs
rrestore -rvf remotehost:/dev/rmt0
```

Restoring from Backup Image Individual User Files

If you need to restore a backup image destroyed by accident, your most difficult problem is determining which of the backup tapes contains this file. The **restore -T** command can be used to list the contents of an archive. It is a good idea to restore the file in the **/tmp** directory so that you do not accidentally overwrite the user's other files.

If the backup strategy included incremental backups, then it is helpful to find out from the user when the file was most recently modified. This helps to determine which incremental backup contains the file. If this information cannot be obtained or is found to be incorrect, then start searching the incremental backups in reverse order (7, 6, 5, ...). For incremental file system backups, the **-i** flag (interactive mode) of the **restore** command is very useful in both locating and restoring the lost file. (Interactive mode is also useful for restoring an individual user's account from a backup of the **/home** file system.)

The procedures in the following table describe how to implement a level 0 (full) restoration of a directory or file system.

Prerequisites

Make sure the device is connected and available. To check availability, type:

```
lsdev -C | pg
```

Restoring from Backup Image Tasks		
Task	*SMIT Fast Path*	*Command or File*
Restore Individual User Files	**smit restfile**	See **restore** command.
Restoring a User File System	**smit restfilesys**	1. **mkfs /dev/hd1** 2. **mount /dev/hd1 /filesys** 3. **cd /filesys** 4. **restore -r**
Restoring a User Volume Group	**smit restvg**	See **restvg -q** command.

Changing System Environment Variables

The system environment is primarily the set of variables that define or control certain aspects of process execution. They are set or reset each time a shell is started. From the system-management point of view, it is important to ensure the user is set up with the correct values at login. Most of these variables are set during system initialization. Their definitions are read from the **/etc/profile** file or set by default.

Testing the System Battery

If your system is losing track of time, the cause might be a depleted or disconnected battery. To determine the status of your system battery, type the following **diag** command:

```
diag -B -c
```

When the Diagnostics main menu appears, select the **Problem Determination** option. If the battery is disconnected or depleted, a problem menu will be displayed with a service request number (SRN). Record the SRN on Item 4 of the Problem Summary Form and report the problem to your hardware service organization.

If your system battery is operational, your system time might have been reset incorrectly because either the **date** or **setclock** command was run incorrectly or unsuccessfully. Refer to "Resetting the System Clock" to correct the problem.

Resetting the System Clock

The system clock records the time of system events, allows you to schedule system events (such as running hardware diagnostics at 3:00 a.m.), and tells when you first created or last saved files. Use the **date** command to set your system clock. Use the **setclock** command to set the time and date by contacting a time server.

Using the date Command

The **date** command displays or sets the date and time. Enter the following command to determine what your system recognizes as the current date and time:

```
/usr/bin/date
```

Attention: Do not change the date when the system is running with more than one user.

The following formats can be used when setting the date with the *Date* parameter:

- *mmddHHMM*[*YYyy*] (default)
- *mmddHHMM*[*yy*]

The variables to the *Date* parameter are defined as follows:

mm	Specifies the number of the month.
dd	Specifies the number of the day in the month.
HH	Specifies the hour in the day (using a 24-hour clock).
MM	Specifies the minute number.
YY	Specifies the first two digits of a four-digit year.
yy	Specifies the last two numbers of the year.

With root authority, you can use the **date** command to set the current date and time. For example:

```
date 021714252002
```

Sets the date to Feb. 17, 2002, and time to 14:25. For more information about the **date** command, see its description in *AIX 5L Version 5.2 Commands Reference*.

Using the setclock Command

The **setclock** command displays or sets the time and date by requesting the current time from a time server on a network. To display your system's date and time, enter:

```
/usr/sbin/setclock
```

The **setclock** command takes the first response from the time server, converts the calendar clock reading found there, and shows the local date and time. If no time server responds, or if the network is not operational, the **setclock** command displays a message to that effect and leaves the date and time settings unchanged.

Note: Any host running the **inetd** daemon can act as a time server.

With root authority, you can use the **setclock** command to send an Internet TIME service request to a time server host and sets the local date and time accordingly. For example:

```
setclock TimeHost
```

Where *TimeHost* is the host name or IP address of the time server.

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. To change the message of the day, use your favorite editor to edit the **/etc/motd** file.

Enabling Dynamic Processor Deallocation

If your machine supports Dynamic Processor Deallocation, you can use SMIT or system commands to turn the feature **on** or **off**. Beginning with AIX 5.2, Dynamic Processor Deallocation is enabled by default during

installation, provided the machine has the correct hardware and firmware to support it. In previous versions of AIX, the feature is disabled by default, and if you try to enable it, a message alerts you when your machine cannot support this feature.

For additional information, see Enabling Dynamic Processor Deallocation in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

SMIT Fastpath Procedure

1. With root authority, 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

With root authority, you can use the following commands to work with the Dynamic Processor Deallocation:

- Use the **chdev** command to change the characteristics of the device specified. For information about using this command, see **chdev** in the *AIX 5L Version 5.2 Commands Reference, Volume 1*.
- If the processor deallocation fails for any reason, you can use the **ha_star** command to restart it after it has been fixed. For information about using this command, see **ha_star** in the *AIX 5L Version 5.2 Commands Reference, Volume 2*.
- Use the **errpt** command to generate a report of logged errors. For information about using this command, see **errpt** in the *AIX 5L Version 5.2 Commands Reference, Volume 2*.

Monitoring and Managing Processes

This section describes procedures that you, as the system administrator, can use to manage processes. See “Monitoring and Managing Processes” in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices* and see also *AIX 5L Version 5.2 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.

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 command lists, in descending order, the 15 most CPU-intensive processes other than those owned by you.

For more specialized uses, the following two tables are intended to simplify the task of choosing **ps** flags by summarizing the effects of the flags.

Process-Specifying Flags

	-A	**-a**	**-d**	**-e**	**-G -g**	**-k**	**-p**	**-t**	**-U -u**	**a**	**g**	**t**	**x**
All processes	Y	-	-	-	-	-	-	-	-	-	Y	-	-
Not processes group leaders and not associated with a terminal	-	Y	-	-	-	-	-	-	-	-	-	-	-
Not process group leaders	-	-	Y	-	-	-	-	-	-	-	-	-	-
Not kernel processes	-	-	-	Y	-	-	-	-	-	-	-	-	-
Members of specified-process groups	-	-	-	-	Y	-	-	-	-	-	-	-	-
Kernel processes	-	-	-	-	-	Y	-	-	-	-	-	-	-
Those specified in process number list	-	-	-	-	-	-	Y	-	-	-	-	-	-
Those associated with tty(s) in the list	-	-	-	-	-	-	-	Y (*n* ttys)	-	-	-	Y (1 tty)	-
Specified user processes	-	-	-	-	-	-	-	-	Y	-	-	-	-
Processes with terminals	-	-	-	-	-	-	-	-	-	Y	-	-	-
Not associated with a tty	-	-	-	-	-	-	-	-	-	-	-	-	Y

Column-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

Column-Selecting Flags

Default1	**-f**	**-l**	**-U -u**	**Default2**	**e**	**l**	**s**	**u**	**v**	
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	-	-	-
SIZE	-	-	-	-	-	-	-	-	Y	-
SZ	-	Y	-	-	-	Y	-	Y	-	-
WCHAN	-	-	Y	-	-	-	Y	-	-	-
RSS	-	-	-	-	-	-	Y	-	Y	Y
SSIZ	-	-	-	-	-	-	-	Y	-	-
%CPU	-	-	-	-	-	-	-	-	Y	Y
%MEM	-	-	-	-	-	-	-	-	Y	Y
PGIN	-	-	-	-	-	-	-	-	-	Y
LIM	-	-	-	-	-	-	-	-	-	Y
TSIZ	-	-	-	-	-	-	-	-	-	Y
TRS	-	-	-	-	-	-	-	-	-	Y
Environment (following the command)	-	-	-	-	-	Y	-	-	-	-

If **ps** is given with no flags or with a process-specifying flag that begins with a minus sign, the columns displayed are those shown for Default1. If the command is given with a process-specifying flag that does not begin with minus, Default2 columns are displayed. The **-u** or **-U** flag is both a process-specifying and column-selecting flag.

The following are brief descriptions of the contents of the columns:

PID Process ID
TTY Terminal or pseudo-terminal associated with the process
TIME Cumulative CPU time consumed, in minutes and seconds
CMD Command the process is running
USER Login name of the user to whom the process belongs
UID Numeric user ID of the user to whom the process belongs
PPID ID of the parent process of this process
C Recently used CPU time
STIME Time the process started, if less than 24 hours. Otherwise the date the process is started
F Eight-character hexadecimal value describing the flags associated with the process (see the detailed description of the **ps** command)
S/STAT Status of the process (see the detailed description of the **ps** command)

PRI	Current priority value of the process
NI/NICE	Nice value for the process
ADDR	Segment number of the process stack
SIZE	(**-v** flag) The virtual size of the data section of the process (in kilobytes)
SZ	(**-l** and **l** flags) The size in kilobytes of the core image of the process.
WCHAN	Event on which the process is waiting
RSS	Sum of the numbers of working-segment and code-segment pages in memory times 4
SSIZ	Size of the kernel stack
%CPU	Percentage of time since the process started that it was using the CPU
%MEM	Nominally, the percentage of real memory being used by the process, this measure does not correlate with any other memory statistics
PGIN	Number of page ins caused by page faults. Since all I/O is classified as page faults, this is basically a measure of I/O volume
LIM	Always **xx**
TSIZ	Size of the text section of the executable file
TRS	Number of code-segment pages times 4
Environment	Value of all the environment variables for the process

Altering Process-Priority

Basically, if you have identified a process that is using too much CPU time, you can reduce its effective priority by increasing its nice value with the **renice** command. For example:

renice +5 *ProcID*

The nice value of the *ProcID*'s would increase process from the normal 20 of a foreground process to 25. You must have root authority to reset the process *ProcID*'s nice value to 20. Type:

renice -5 *ProcID*

Terminating a Process

Normally, you use the **kill** command to end a process. The **kill** command sends a signal to the designated process. Depending on the type of signal and the nature of the program that is running in the process, the process might end or might keep running. The signals you send are:

SIGTERM	(signal 15) is a request to the program to terminate. If the program has a signal handler for SIGTERM that does not actually terminate the application, this **kill** may have no effect. This is the default signal sent by **kill**.
SIGKILL	(signal 9) is a directive to kill the process immediately. This signal cannot be caught or ignored.

It is typically better to issue SIGTERM rather than SIGKILL. If the program has a handler for SIGTERM, it can clean up and terminate in an orderly fashion. Type:

kill -term *ProcessID*

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

kill -kill *ProcessID*

You might notice occasional defunct processes, also called *zombies*, in your process table. These processes are no longer executing, have no system space allocated, but still retain their PID number. You can recognize a zombie process in the process table because it displays `<defunct>` in the CMD column. For example:

```
 UID   PID  PPID   C    STIME    TTY  TIME CMD
                          .
                          .
                          .
```

```
 lee 22392 20682   0   Jul 10      -  0:05 xclock
 lee 22536 21188   0   Jul 10  pts/0  0:00 /bin/ksh
 lee 22918 24334   0   Jul 10  pts/1  0:00 /bin/ksh
 lee 23526 22536  22                   0:00 <defunct>
 lee 24334 20682   0   Jul 10      ?  0:00 aixterm
 lee 24700     1   0   Jul 16      ?  0:00 aixterm
root 25394 26792   2   Jul 16  pts/2  0:00 ksh
 lee 26070 24700   0   Jul 16  pts/3  0:00 /bin/ksh
 lee 26792 20082   0   Jul 10  pts/2  0:00 /bin/ksh
root 27024 25394   2 17:10:44  pts/2  0:00 ps -ef
```

Zombie processes continue to exist in the process table until the parent process dies or the system is shut down and restarted. In the example shown above, the parent process (PPID) is the **ksh** command. When the Korn shell is exited, the defunct process is removed from the process table.

Sometimes a number of these defunct processes collect in your process table because an application has forked several child processes and has not exited. If this becomes a problem, the simplest solution is to modify the application so its **sigaction** subroutine ignores the **SIGCHLD** signal. For more information, see the **sigaction** subroutine in *AIX 5L Version 5.2 Technical Reference: Base Operating System and Extensions Volume 2*.

Binding or Unbinding a Process

On multiprocessor systems, you can bind a process to a processor or unbind a previously bound process from:

- Web-based System Manager
- SMIT
- command line

Note: While binding a process to a processor might lead to improved performance for the bound process (by decreasing hardware-cache misses), overuse of this facility could cause individual processors to become overloaded while other processors are underused. The resulting bottlenecks could reduce overall throughput and performance. During normal operations, it is better to let the operating system assign processes to processors automatically, distributing system load across all processors. Bind only those processes that you know can benefit from being run on a single processor.

Prerequisites

You must have root user authority to bind or unbind a process you do not own.

Binding or Unbinding a Process Tasks

Task	*SMIT Fast Path*	*Command or File*
Binding a Process	**smit bindproc**	**bindprocessor -q**
Unbinding a Process	**smit ubindproc**	**bindprocessor -u**

Fixing Stalled or Unwanted Processes

Stalled or unwanted processes can cause problems with your terminal. Some problems produce messages on your screen that give information about possible causes.

To perform the following procedures, you must have either a second terminal, a modem, or a network login. If you do not have any of these, fix the terminal problem by rebooting your machine.

Choose the appropriate procedure for fixing your terminal problem:

- “Free a Terminal Taken Over by Processes” on page 47

- “Respond to Screen Messages”

Free a Terminal Taken Over by Processes

Identify and stop stalled or unwanted processes by doing the following:

1. Determine the active processes running on the screen by typing the following **ps** command:

   ```
   ps -ef | pg
   ```

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

   Suspicious processes include system or user processes that use up excessive amounts of a system resource such as CPU or disk space. System processes such as **sendmail**, **routed**, and **lpd** frequently become runaways. Use the **ps -u** command to check CPU usage.

2. Determine who is running processes on this machine by using the **who** command:

   ```
   who
   ```

   The **who** command displays information about all users currently on this system, such as login name, workstation name, date, and time of login.

3. Determine if you need to stop, suspend, or change the priority of a user process.

   Note: You must have root authority to stop processes other than your own. If you terminate or change the priority of a user process, contact the process owner and explain what you have done.

   - Stop the process using the **kill** command. For example:

     ```
     kill 1883
     ```

     The **kill** command sends a signal to a running process. To stop a process, specify the process ID (PID), which is 1883 in this example. Use the **ps** command to determine the PID number of commands.

   - Suspend the process and run it in the background by using the ampersand (&). For example:

     ```
     /u/bin1/prog1 &
     ```

     The **&** signals that you want this process to run in the background. In a background process, the shell does not wait for the command to complete before returning the shell prompt. When a process requires more than a few seconds to complete, run the command in background by typing an **&** at the end of the command line. Jobs running in the background appear in the normal **ps** command.

   - Change the priority of the processes that have taken over by using the following **renice** command:

     ```
     renice 20 1883
     ```

     The **renice** command alters the scheduling priority of one or more running processes. The higher the number, the lower the priority with 20 being the lowest priority.

     In the previous example, **renice** reschedules process number 1883 to the lowest priority. It will run when there is a small amount of unused processor time available.

Respond to Screen Messages

Respond to and recover from screen messages by doing the following:

1. Make sure the **DISPLAY** environment variable is set correctly. Use either of the following methods to check the **DISPLAY** environment:

   - Use the **setsenv** command to display the environment variables.

     ```
     setsenv
     ```

     The **setsenv** command displays the protected state environment when you logged in.

     Determine if the **DISPLAY** variable has been set. In the following example, the **DISPLAY** variable does not appear, which indicates that the **DISPLAY** variable is not set to a specific value.

```
SYSENVIRON:
NAME=casey
TTY=/dev/pts/5
LOGNAME=casey
LOGIN=casey
```

OR

- Change the value of the **DISPLAY** variable. For example, to set it to the machine named `bastet` and terminal 0, enter:

  ```
  DISPLAY=bastet:0
  export DISPLAY
  ```

  If not specifically set, the **DISPLAY** environment variable defaults to `unix:0` (the console). The value of the variable is in the format *name*:*number* where *name* is the host name of a particular machine, and *number* is the X server number on the named system.

2. Reset the terminal to its defaults using the following **stty** command:

   ```
   stty sane
   ```

   The **stty sane** command restores the "sanity" of the terminal drivers. The command outputs an appropriate terminal resetting code from the **/etc/termcap** file (or **/usr/share/lib/terminfo** if available).

3. If the Return key does not work correctly, reset it by entering:

   ```
   ^J stty sane ^J
   ```

   The ^J represents the Ctrl-J key sequence.

RT_MPC and RT_GRQ

The use of multiple queues increases the processor affinity of threads, but there is a special situation where you might want to counteract this effect. When there is only one run queue, a thread that has been awakened (the waking thread) by another running thread (the waker thread) would normally be able to use the CPU immediately on which the waker thread was running. With multiple run queues, the waking thread may be on the run queue of another CPU which cannot notice the waking thread until the next scheduling decision. This may result in up to a 10 ms delay.

This is similar to scenarios in earlier releases of this operating system which migjht have occurred using the bindprocessor option. If all CPUs are constantly busy, and there are a number of interdependent threads waking up, there are two options available.

- The first option, which uses one run queue, is to set the environment variable RT_GRQ=ON which forces unbound selected threads to be dispatched off the global run queue.
- Alternatively, you can choose the real time kernel option (type the command `bosdebug -R on` and then `bosboot`) and the RT_MPC=ON environment variable for selected processes. It is essential to maintain a performance log of your systems to closely monitor the impact of any tuning you attempt.

Chapter 3. Physical and Logical Volume Storage Management Tasks

This chapter contains instructions for managing the logical structure of the AIX operating system. Tasks are collected into the following categories:

- "Physical and Logical Volumes"
- "Paging Space and Virtual Memory" on page 79

Physical and Logical Volumes

This section provides several procedures for configuring disk drives for use by the Logical Volume Manager (LVM), maintaining physical and logical volumes and volume groups, and troubleshooting problems you might encounter. Chapter 1, "How-To's for System Management Tasks," on page 1 provides scenarios for additional Logical Volume Manager (LVM) tasks, such as how to use the snapshot feature (available with AIX 5.2 and later versions) to protect the consistency of your mirrored volume groups from potential disk failure.

LVM Configuration Tasks

The Logical Volume Manager (LVM) is installed with the base operating system and needs no further configuration. However, disks must be configured and defined as a physical volume before the LVM can use them. If you want to set up raw logical volumes for use by an application, see "Define a Raw Logical Volume for an Application" on page 8.

This section provides instructions for the following configuration tasks:

- "Configuring a Disk"
- "Making an Available Disk a Physical Volume" on page 51

Configuring a Disk

You can configure a new disk in any of the following ways.

- If you can shut down and power off the system, use "Method 1." Whenever possible, it is always preferable to shut down and power off any system when you are attaching a physical disk to it.
- If you cannot shut down your system and you know details about the new disk, such as the subclass, type, parent name, and where it is connected, use "Method 2" on page 50.
- If you cannot shut down your system and you only know the location of the disk, use "Method 3" on page 50.

After a disk is configured, although it is generally available for use, the Logical Volume Manager requires that it is further identified as a physical volume.

Method 1: Use the following method when you can shut down and power off the system before attaching the disk:

1. Physically connect the new disk to the system and then power on the disk and system according to the documentation that came with your system.
2. During system boot, let the Configuration Manager (**cfgmgr**) automatically configure the disk.
3. After system boot, with root authority, type the **lspv** command at the command line to look for the new disk's name. The system returns an entry similar to one of the following:

   ```
   hdisk1  none                    none
   ```

   or:

   ```
   hdisk1  00005264d21adb2e        none
   ```

The first field identifies the system-assigned name of the disk. The second field displays the physical volume ID (PVID), if any. If the new disk does not appear in the **lspv** output, refer to the*AIX 5L Version 5.2 Installation Guide and Reference*.

At this point, the disk is usable by the system but it needs a PVID for use by the LVM. If the new disk does not have a PVID, then see “Making an Available Disk a Physical Volume” on page 51.

Method 2: Use the following method when you cannot shut down your system and you know the following information about the new disk:

- 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).

Do the following:

1. Physically connect the new disk to the system and then power on the disk and system according to the documentation that came with your system.
2. To configure the disk and ensure that it is available as a physical volume, use the **mkdev** command with the flags shown, as in the following example:

   ```
   mkdev -c disk -s scsi -t 2200mb -p scsi3 \
   -w 6,0 -a pv=yes
   ```

   This example adds a 2.2 GB disk with a SCSI ID of 6 and logical unit number of 0 to the scsi3 SCSI bus. The **-c** flag defines the class of the device. The **-s** flag defines the subclass. The **-t** flag defines the type of device. The **-p** flag defines the parent device name that you want to assign. The **-w** flag designates the disk’s location by SCSI ID and logical unit number. The **-a** flag specifies the device attribute-value pair, `pv=yes`, which 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).

At this point, the disk is defined both as an available device and as a physical volume. You can type the **lspv** command on the command line to list the new disk entry. If the new disk does not appear in the **lspv** output, refer to the *AIX 5L Version 5.2 Installation Guide and Reference*.

Method 3: Use the following method when you cannot shut down your system and you know only the location of the disk:

1. Physically connect the new disk to the system and then power on the disk and system according to the documentation that came with your system.
2. To check which physical disks are already configured on the system, type the **lspv** command on the command line. The output looks similar to the following:

   ```
   hdisk0       000005265ac63976    rootvg
   ```
3. Type **cfgmgr** on the command line to enter the Configuration Manager. The Configuration Manager automatically detects and configures all newly connected devices on the system, including the new disk.
4. To confirm that the new disk was configured, type the **lspv** command again. The output looks similar to one of the following:

   ```
   hdisk1    none                none
   ```

   OR

   ```
   hdisk1   00005264d21adb2e     none
   ```

   The first field identifies the system-assigned name of the disk. The second field displays the physical volume ID (PVID), if any. If the new disk does not appear in the **lspv** output, refer to the *AIX 5L Version 5.2 Installation Guide and Reference*.

At this point, the disk is usable by the system but it needs a PVID for use by the LVM. If the new disk does not have a PVID, then see “Making an Available Disk a Physical Volume.”

Making an Available Disk a Physical Volume

A disk must be configured as a physical volume before it can be assigned to volume groups and used by the LVM. Use the following instructions to configure a physical volume:

1. Ensure the disk is known to the operating system, is available, and is not being used by the operating system or any applications. Type the **lspv** command on the command line. The output looks similar to the following:

   ```
   hdisk1  none                    none
   ```

   Check the output for the following:

   - If the new disk’s name does not appear in command output, refer to “Configuring a Disk” on page 49.
   - If the second field of the output shows a system-generated physical volume identifier (PVID) (for example, `00005264d21adb2e`), the disk is already configured as a physical volume and you do not have to complete this procedure.
   - If the third field of the output shows a volume group name (for example, `rootvg`), the disk is currently being used and is not an appropriate choice for this procedure.

   If the new disk has no PVID and is not in use, continue with the next step.
2. To change an available disk to a physical volume, type the **chdev** command on the command line. For example:

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

   The **-l** flag specifies the device name of the disk. The **-a** flag specifies the device attribute-value pair, `pv=yes`, which 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).

At this point, the disk is defined as a physical volume. You can type the **lspv** command on the command line to list the new disk entry.

LVM Maintenance Tasks

The simplest tasks you might need when maintaining the entities that LVM controls (physical and logical volumes, volume groups, and file systems) are grouped within the following table. Instructions for additional maintenance tasks are located later in this section or in Chapter 1, “How-To’s for System Management Tasks,” on page 1. Instructions that are specific to file systems are located in Chapter 4, “File Systems Management Tasks,” on page 85.

You must have root authority to perform most of the following tasks. For your convenience, links to all the logical volume, physical volume, and volume group maintenance tasks are listed below:

- “Activating a Volume Group” on page 52
- “Adding Disks while the System Remains Available” on page 54
- “Adding a Fixed Disk Without Data to an Existing Volume Group” on page 52
- “Adding a Fixed Disk Without Data to a New Volume Group” on page 52
- “Adding a JFS to a Previously Defined Logical Volume Menu” on page 85
- “Adding a Logical Volume” on page 53
- “Adding and Activating a New Volume Group ” on page 53
- “Add a Removable Media Drive” on page 1
- “Adding a Volume Group” on page 53
- “Changing a Logical Volume to Use Data Allocation” on page 53
- “Changing a Volume Group to Nonquorum Status” on page 55

Table 2. Managing Logical Volumes and Storage Tasks

Task	*SMIT Fast Path*	*Command or File*
Activate a volume group	**smit varyonvg**	
Add a fixed disk without data to existing volume group	**smit extendvg**	
Add a fixed disk without data to new volume group	**smit mkvg**	

Table 2. Managing Logical Volumes and Storage Tasks (continued)

Task	*SMIT Fast Path*	*Command or File*
Add a logical volume[Note 1]	**smit mklv**	
Add a volume group	**smit mkvg**	
Add and activate a new volume group	**smit mkvg**	
Change a logical volume to use data allocation	**smit chlv1**	
Change the name of a volume group[Note 2]	1. **smit varyoffvg** 2. **smit exportvg** 3. **smit importvg** 4. **smit mountfs**	1. **varyoffvg** *OldVGName* 2. **exportvg** *OldVGName* 3. **importvg** *NewVGName* 4. **mount all**
Change a volume group to use automatic activation	**smit chvg**	
Change or set logical volume policies	**smit chlv1**	
Copy a logical volume to a new logical volume[Note 3]	**smit cplv**	
Copy a logical volume to an existing logical volume of the same size[Attn 1]	**smit cplv**	
Copy a logical volume to an existing logical volume of smaller size[Attn 1] [Note 3]	Do not use SMIT[Attn 2]	1. Create logical volume. For example: **mklv -y hdisk*N* vg00 4** 2. Create new file system on new logical volume. For example: **crfs -v jfs -d hdisk*N* -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[Attn 1]	**smit cplv**	
Deactivate a volume group	**smit varyoffvg**	
Enable write-verify and change scheduling policy	**smit chlv1**	
Increase the maximum size of a logical volume	**smit chlv1**	
Increase the size of a logical volume	**smit extendlv**	
List all logical volumes by volume group	**smit lslv2**	
List all physical volumes in system	**smit lspv2**	
List all volume groups	**smit lsvg2**	

Table 2. Managing Logical Volumes and Storage Tasks (continued)

Task	*SMIT Fast Path*	*Command or File*
List the status, logical volumes, or partitions of a physical volume	**smit lspv**	
List the contents of a volume group	**smit lsvg1**	
List a logical volume's status or mapping	**smit lslv**	
Mirror a logical volume with or without data allocation	**smit mklvcopy**	
Power off a removable disk	**smit offdsk**	Available with the hot-removability feature only
Power on a removable disk	**smit ondsk**	Available with the hot-removability feature only
Remove a disk with data from the operating system	**smit exportvgrds**	
Remove a disk without data from the operating system	**smit reducevgrds**	
Remove mirroring from a volume group	**smit unmirrorvg**	
Remove a volume group	**smit reducevg2**	
Reorganize a volume group	**smit reorgvg**	
Unconfigure and power off a disk	**smit rmvdsk1** or **smit rmvdsk** then **smit opendoor**	

Attention:

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

Notes:

1. After you create a logical volume, the state will be closed because 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 "Define a Raw Logical Volume for an Application" on page 8.
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.

Adding Disks while the System Remains Available

The following procedure describes how to turn on and configure a disk using the hot-removability feature, which lets you add disks without powering off the system. You can add a disk for additional storage or to correct a disk failure. To remove a disk using the hot-removability feature, see "Removing a Disk while the System Remains Available" on page 65. This feature is only available on certain systems.

1. Install the disk in a free slot of the cabinet. For detailed information about the installation procedure, see the service guide for your machine.
2. Power on the new disk by typing the following fast path on the command line:

   ```
   smit ondsk
   ```

At this point, the disk is added to the system but it is not yet usable. What you do next depends on whether the new disk contains data.

- If the disk has no data, add it as a physical volume to a volume group using one of the following:
  - To add the disk to an existing volume group, type the following fast path on the command line:

    ```
    smit extendvg
    ```
  - To add the disk to a new volume group, type the following fast path on the command line:

    ```
    smit mkvg
    ```
- If the disk contains data, import the data using the procedure in “Importing or Exporting a Volume Group” on page 61.

Changing a Volume Group to Nonquorum Status

You can change a volume group to nonquorum status to have data continuously available even when there is no quorum. This procedure is often used for systems with the following configurations:

- 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

When a volume group under these circumstances can operate in nonquorum status, then even if a disk failure occurs, the volume group remains active as long as one logical volume copy remains intact on a disk. For conceptual information about quorums, refer to *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

To make recovery of nonquorum groups possible, ensure the following:

- If your system uses JFS or JFS2 file systems, mirror the JFS log logical volume.
- Place mirrored copies on separate disks. If you are unsure of the configuration, type the following command to check the physical location (PV1, PV2, and PV3) of each logical partition. (To place the copies on separate disks, the PV1, PV2, and PV3 columns must contain different hdisk numbers.)

  ```
  lslv -m LVName
  ```

  If a logical volume has its only copies residing on the same disk, and that disk becomes unavailable, the volume will not be available to the user regardless of the quorum or nonquorum status of its volume group.

Both user-defined and rootvg volume groups can operate in nonquorum status, but their configuration and recovery methods are different.

Changing a User-Defined Volume Group to Nonquorum Status: Use the following procedure to change a user-defined volume group to nonquorum status:

1. Check whether the user-defined volume group is currently active (varied on) by typing the following command:

   ```
   lsvg -o
   ```

   If the group you want is *not* listed, continue with step 3. If the group you want *is* listed, continue with step 2.
2. If the group is active (varied on), type the following command:

   ```
   varyoffvg VGname
   ```

   Where *VGName* is the name of your user-defined volume group.
3. To change an inactive user-defined volume group to nonquorum status, type the following command:

   ```
   chvg -Qn VGName
   ```

   If the volume group is active, the change does not take effect until the next varyoff/varyon cycle completes.
4. To activate the volume group and cause the change to take effect, type the following command:

```
varyonvg VGName
```

Note: 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.

At this point, your user-defined volume group should be available even if a quorum of physical volumes is not available.

Changing the rootvg Volume Group to Nonquorum Status: The procedure to change a rootvg to nonquorum status requires shutting down your system and rebooting.

Attention: When a disk associated with the rootvg volume group is missing, avoid powering on the system 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. LVM must force the activation because the operating system cannot be brought up unless rootvg is activated. In other words, LVM makes a final attempt to activate (vary on) a nonquorum rootvg even if only a single disk is accessible.

1. To change the rootvg volume group to nonquorum status, type the following command:
   ```
   chvg -Qn rootvg
   ```
2. To shut down and reboot the system, which causes the change to nonquorum status to take effect, type:
   ```
   shutdown -Fr
   ```

At this point, the rootvg should remain available even if a quorum of physical volumes is not available.

Changing the Name of a Logical Volume

The following procedure describes how to rename a logical volume without losing data on the logical volume.

In the following examples, the logical volume name is changed from lv00 to lv33.

1. Unmount all file systems associated with the logical volume, by typing:
   ```
   unmount /FSname
   ```
   Where *FSname* is the full name of a file system.

   Notes:

   a. The **unmount** command fails if the file system you are trying to unmount is currently being used. The **unmount** command executes only if none of the file system's files are open and no user's current directory is on that device.

   b. Another name for the **unmount** command is **umount**. The names are interchangeable.
2. Rename the logical volume, by typing:
   ```
   chlv -n NewLVname OldLVname
   ```
   Where the **-n** flag specifies the new logical volume name (*NewLVname*) and *OldLVname* is the name you want to change. For example:
   ```
   chlv -n lv33 lv00
   ```

   Note: If you rename a JFS or JFS2 log, the system prompts you to run the **chfs** command on all file systems that use the renamed log device.
3. Remount the file systems you unmounted in step 1 by typing:
   ```
   mount /test1
   ```

At this point, the logical volume is renamed and available for use.

Copying a Logical Volume to Another Physical Volume

Depending on your needs, there are several ways to copy a logical volume to another physical volume while retaining file system integrity. The following sections describe your options.

Note: For the following scenarios to be successful in a concurrent volume group environment, AIX 4.3.2 or later must be installed on all concurrent nodes.

- "Copy a Logical Volume"
- "Copy a Logical Volume While Original Logical Volume Remains Usable"
- "Copy a Raw Logical Volume to Another Physical Volume" on page 58

This scenario offers multiple methods to copy a logical volume or JFS to another physical volume. Choose the method that best serves your purposes:

Copy a Logical Volume: The simplest method is to use the **cplv** command to copy the original logical volume and create a new logical volume on the destination physical volume.

1. Stop using the logical volume. Unmount the file system, if applicable, and stop any application that accesses the logical volume.
2. Select a physical volume that has the capacity to contain all of the data in the original logical volume.

   Attention: If you copy from a larger logical volume containing data to a smaller one, you can corrupt your file system because some data (including the superblock) might be lost.
3. Copy the original logical volume (in this example, it is named `lv00`) and create the new one, using the following command:

   Note: The following **cplv** command fails if it creates a new logical volume and the volume group is varied on in concurrent mode.

   ```
   cplv lv00
   ```
4. Mount the file systems, if applicable, and restart applications to begin using the logical volume.

At this point, the logical volume copy is usable.

Copy a Logical Volume While Original Logical Volume Remains Usable: If your environment requires continued use of the original logical volume, you can use the **splitlvcopy** command to copy the contents, as shown in the following example:

1. Mirror the logical volume, using the following SMIT fast path:

   ```
   smit mklvcopy
   ```
2. Stop using the logical volume. Unmount the file system, if applicable, and stop or put into quiescent mode any application that accesses the logical volume.

   Attention: The next step uses the **splitlvcopy** command. Always close logical volumes before splitting them and unmount any contained file systems before using this command. Splitting an open logical volume can corrupt your file systems and cause you to lose consistency between the original logical volume and the copy if the logical volume is accessed simultaneously by multiple processes.
3. With root authority, copy the original logical volume (`oldlv`) to the new logical volume (`newlv`) using the following command:

   ```
   splitlvcopy -y newlv oldlv
   ```

   The **-y** flag designates the new logical volume name. If the `oldlv` volume does not have a logical volume control block, the **splitlvcopy** command completes successfully but generates a message that the `newlv` volume has been created without a logical volume control block.
4. Mount the file systems, if applicable, and restart applications to begin using the logical volume.

At this point, the logical volume copy is usable.

Copy a Raw Logical Volume to Another Physical Volume: To copy a raw logical volume to another physical volume, do the following:

1. Create a mirrored copy of the logical volume on a new physical volume in the volume group using the following command:

   ```
   mklvcopy LogVol_name 2 new_PhysVol_name
   ```

2. Synchronize the partitions in the new mirror copy using the following command:

   ```
   syncvg -l LogVol_name
   ```

3. Remove the copy of the logical volume from the physical volume using the following command:

   ```
   rmlvcopy LogVol_name 1 old_PhysVol_name
   ```

At this point, the raw logical volume copy is usable.

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

A JFS or JFS2 *file system log* is a formatted list of file system transaction records. The log ensures file system integrity (but not necessarily data integrity) in case the system goes down before transactions have been completed. A dedicated disk is created on hd8 for rootvg when the system is installed. The following procedure helps you create a JFS log on a separate disk for other volume groups. When you create a JFS2 log, the procedure requires the following changes:

- The log device type is **jfs2log**.
- The **logform** command requires a **-V jfs2** option to specify a JFS2 log device.
- The **crfs** commands must specify **jfs2** instead of **jfs**.

Creating a file system log file for user-defined volume groups can 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.

To create a log file for user-defined volume groups, the easiest way is to use the Web-based System Manager wizard, as follows:

1. If Web-based System Manager is not already running, with root authority, type `wsm` on the command line.
2. Select a host name.
3. Select the **Volumes** container.
4. Select the **Logical Volumes** container.
5. In the Volumes menu, select **New Logical Volume** (Wizard). The wizard will guide you through the procedure. Online help is available if you need it.

Alternatively, you can use the following procedure, which creates a volume group (fsvg1) with two physical volumes (hdisk1 and hdisk2). The file system is on hdisk2 (a 256-MB file system mounted at **/u/myfs**) and the log is on hdisk1. By default, a JFS log size is 4 MB. You can place little-used programs, for example, **/blv**, on the same physical volume as the log without impacting performance.

The following instructions explain how to create a JFS log for a user-defined volume group using SMIT and the command line interface:

1. Add the new volume group (in this example, fsvg1) using the SMIT fast path:

   ```
   smit mkvg
   ```

2. Add a new logical volume to this volume group using the SMIT fast path:

   ```
   smit mklv
   ```

3. On the Add a Logical Volume screen, add your data to the following fields. For example:

   ```
   Logical Volumes NAME                    fsvg1log

   Number of LOGICAL PARTITIONS            1
   ```

```
PHYSICAL VOLUME names                   hdisk1

Logical volume TYPE                     jfslog

POSITION on Physical Volume             center
```

4. After you set the fields, press Enter to accept your changes and exit SMIT.
5. Type the following on a command line:

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

6. When you receive the following prompt, type **y** and press Enter:

   ```
   Destroy /dev/fsvg1log
   ```

   Despite the wording in this prompt, nothing is destroyed. When you respond **y** to this prompt, the system formats the logical volume for the JFS log so that it can record file-system transactions.
7. Add another logical volume using the following SMIT fast path:

   ```
   smit mklv
   ```

8. Type the name of the same volume group as you used in step 2 on page 58 (`fsvg1` in this example). In the Logical Volumes screen, add your data to the following fields. Remember to designate a different physical volume for this logical volume than you did in step 3 on page 58. For example:

   ```
   Logical Volumes NAME                    fslv1

   Number of LOGICAL PARTITIONS            64

   PHYSICAL VOLUME names                   hdisk2

   Logical volume TYPE                     jfs
   ```

   After you set the fields, press Enter to accept your changes and exit SMIT.
9. Add a file system to the new logical volume, designate the log, and mount the new file system, using the following sequence of commands:

   ```
   crfs -v jfs -d LogVolName -m FileSysName -a logname=FSLogPath

   mount FileSysName
   ```

   Where *LogVolName* is the name of the logical volume you created in step 7; *FileSysName* is the name of the file system you want to mount on this logical volume; and *FSLogPath* is the name of the volume group you created in step 2 on page 58. For example:

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

10. To verify that you have set up the file system and log correctly, type the following command (substituting your volume group name):

    ```
    lsvg -l fsvg1
    ```

    The output shows both logical volumes you created, with their file system types, as in the following example:

    ```
    LV NAME             TYPE    ...
    /dev/fsvg1log       jfslog  ...
    fslv1               jfs     ...
    ```

At this point, you have created a volume group containing at least two logical volumes on separate physical volumes, and one of those logical volumes contains the file system log.

Designating Hot Spare Disks

Beginning with AIX 5.1, you can designate hot spare disks for a volume group to ensure the availability of your system if a disk or disks start to fail. Hot spare disk concepts and policies are described in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*. The following procedures to enable hot spare disk support depend on whether you are designating hot spare disks to use with an existing volume group or enabling support while creating a new volume group.

Enable Hot Spare Disk Support for an Existing Volume Group: The following steps use Web-based System Manager to enable hot spare disk support for an existing volume.

1. Start Web-based System Manager (if not already running) by typing **wsm** on the command line.
2. Select the **Volumes** container.
3. Select the **Volume Groups** container.
4. Select the name of your target volume group, and choose **Properties** from the Selected menu.
5. Select the Hot Spare Disk Support tab and check beside `Enable hot spare disk support`.
6. Select the Physical Volumes tab to add available physical volumes to the Volume Group as hot spare disks.

At this point, your mirrored volume group has one or more disks designated as spares. If your system detects a failing disk, depending on the options you selected, the data on the failing disk can be migrated to a spare disk without interruption to use or availability.

Enable Hot Spare Disk Support while Creating a New Volume Group: The following steps use Web-based System Manager to enable hot spare disk support while you are creating a new volume group.

1. Start Web-based System Manager (if not already running) by typing **wsm** on the command line.
2. Select the **Volumes** container.
3. Select the **Volume Groups** container.
4. From the Volumes menu, select **New→Volume Group (Advanced Method)**. The subsequent panels let you choose physical volumes and their sizes, enable hot spare disk support, select unused physical volumes to assign as hot spares, then set the migration characteristics for your hot spare disk or your hot spare disk pool.

At this point, your system recognizes a new mirrored volume group with one or more disks designated as spares. If your system detects a failing disk, depending on the options you selected, the data on the failing disk can be migrated to a spare disk without interruption to use or availability.

Enabling and Configuring Hot Spot Reporting

Beginning with AIX 5.1, you can identify hot spot problems with your logical volumes and remedy those problems without interrupting the use of your system. A *hot-spot* problem occurs when some of the logical partitions on your disk have so much disk I/O that your system performance noticeably suffers.

The following procedures use Web-based System Manager to enable host spot reporting and manage the result.

Enabling Hot Spot Reporting at the Volume Group Level: The following steps use Web-based System Manager to enable hot spot reporting at the volume group level.

1. Start Web-based System Manager (if not already running) by typing **wsm** on the command line.
2. Select the **Volumes** container.
3. Select the **Volume Groups** container.
4. Select the name of your target volume group, and choose **Hot Spot Reporting...** from the Selected menu.
5. Check beside `Enable hot spot reporting` and `Restart the Statistics Counters`.

At this point, the hot spot feature is enabled. Use the pull-down or pop-up menu in Web-based System Manager to access the **Manage Hot Spots...** Sequential dialog. In the subsequent panels, you can define your reporting and statistics, display your statistics, select logical partitions to migrate, specify the destination physical partition, and verify the information before committing your changes.

Enabling Hot Spot Reporting at the Logical Volume Level: The following steps use Web-based System Manager to enable hot spot reporting at the logical volume level so you can avoid enabling it for an entire volume group.

1. Start Web-based System Manager (if not already running) by typing **wsm** on the command line.
2. Select the **Volumes** container.
3. Select the **Logical Volumes** container.
4. Select the name of your target logical volume and choose **Hot Spot Reporting...** from the Selected menu.
5. Check beside `Enable hot spot reporting` and `Restart the Statistics Counters`.

At this point, the hot spot feature is enabled. Use the pull-down or pop-up menu in Web-based System Manager to access the **Manage Hot Spots...** Sequential dialog. In the subsequent panels, you can define your reporting and statistics, display your statistics, select logical partitions to migrate, specify the destination physical partition, and verify the information before committing your changes.

Importing or Exporting a Volume Group

The following table explains how to use import and export to move a user-defined volume group from one system to another. (The rootvg volume group cannot be exported or imported.) The export procedure removes the definition of a volume group from a system. The import procedure serves to introduce the volume group to its new system.

You can also use the import procedure to reintroduce a volume group to the system when it once was associated with the system but had been exported. You can also use import and export to add a physical volume that contains data to a volume group by putting the disk to be added in its own volume group.

Attention: The **importvg** command changes the name of an imported logical volume if a logical volume of that name already exists on the new system. If the **importvg** command must rename a logical volume, it prints an error message to standard error. When there are no conflicts, the **importvg** command also creates file mount points and entries in the **/etc/filesystems** file.

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

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

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

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

Migrating the Contents of a Physical Volume

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, use the following instructions. You can also use this procedure to move data from a failing disk before replacing or repairing the failing disk. This procedure can be used on physical volumes in either the root volume group or a user-defined volume group.

Attention: When the boot logical volume is migrated from a physical volume, the boot record on the source must be cleared or it could cause a system hang. When you execute the **bosboot** command, you must also execute the **chpv -c** command described in step 4 on page 63 of the following procedure.

1. If you want to migrate the data to a new disk, do the following steps. Otherwise, continue with step 2.
   a. Check that the disk is recognizable by the system and available by typing:

      ```
      lsdev -Cc disk
      ```

      The output resembles the following:

      ```
      hdisk0 Available 10-60-00-8,0  16 Bit  LVD  SCSI Disk Drive
      hdisk1 Available 10-60-00-9,0  16 Bit  LVD  SCSI Disk Drive
      hdisk2 Available 10-60-00-11,0 16 Bit  LVD  SCSI Disk Drive
      ```

   b. If the disk is listed and in the available state, check that it does not belong to another volume group by typing:

      ```
      lspv
      ```

      The output looks similar to the following:

      ```
      hdisk0          0004234583aa7879       rootvg          active
      hdisk1          00042345e05603c1       none            active
      hdisk2          00083772caa7896e       imagesvg        active
      ```

      In the example, `hdisk1` can be used as a destination disk because the third field shows that it is not being used by a volume group.

      If the new disk is not listed or unavailable, refer to “Configuring a Disk” on page 49 or “Adding Disks while the System Remains Available” on page 54.

   c. Add the new disk to the volume group by typing:

      ```
      extendvg VGName diskname
      ```

      Where *VGName* is the name of your volume group and *diskname* is the name of the new disk. In the example shown in the previous step, *diskname* would be replaced by `hdisk1`.

2. The source and destination physical volumes must be in the same volume group. To determine whether both physical volumes are in the volume group, type:

   ```
   lsvg -p VGname
   ```

   Where *VGname* is the name of your volume group. The output for a root volume group looks similar to the following:

   ```
   rootvg:
   PV_NAME         PV STATE        TOTAL PPs   FREE PPs    FREE DISTRIBUTION
   hdisk0          active          542         85          00..00..00..26..59
   hdisk1          active          542         306         00..00..00..00..06
   ```

   Note the number of FREE PPs.

3. Check that you have enough room on the target disk for the source that you want to move:
   a. Determine the number of physical partitions on the source disk by typing:

      ```
      lspv SourceDiskName | grep "USED PPs"
      ```

      Where *SourceDiskName* is of the name of the source disk, for example, hdisk0. The output looks similar to the following:

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

      In this example, you need 159 FREE PPs on the destination disk to successfully complete the migration.

b. Compare the number of USED PPs from the source disk with the number of FREE PPs on the destination disk or disks (step 2 on page 62). If the number of FREE PPs is larger than the number of USED PPs, you have enough space for the migration.

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

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

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

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

   If you get output similar to the following:

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

   then run the following command:

   ```
   migratepv -l hd5 SourceDiskName DestinationDiskName
   ```

   You will receive a message warning you to perform the **bosboot** command on the destination disk. You must also perform a **mkboot -c** command to clear the boot record on the source. Type the following sequence of commands:

   ```
   bosboot -a -d /dev/DestinationDiskName
   bootlist -m normal DestinationDiskName
   mkboot -c -d /dev/SourceDiskName
   ```

5. Migrate your data by typing the following SMIT fast path:

   ```
   smit migratepv
   ```

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

At this point, the data now resides on the new (destination) disk. The original (source) disk, however, remains in the volume group. If the disk is still reliable, you could continue to use it as a hot spare disk (see “Designating Hot Spare Disks” on page 59). Especially when a disk is failing, it is advisable to do the following steps:

1. To remove the source disk from the volume group, type:

   ```
   reducevg VGNname SourceDiskName
   ```

2. To physically remove the source disk from the system, type:

   ```
   rmdev -l SourceDiskName -d
   ```

Mirroring a Volume Group

The following scenario explains how to mirror a normal volume group. If you want to mirror the root volume group (rootvg), see “Mirroring the Root Volume Group” on page 64.

The following instructions show you how to mirror a root volume group using the System Management Interface Tool (SMIT). You can also use Web-based System Manager (select a volume group in the **Volumes** container, then choose **Mirror** from the **Selected** menu). Experienced administrators can use the **mirrorvg** command.

Note: The following instructions assume you understand the mirroring and logical volume manager (LVM) concepts explained in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

1. With root authority, add a disk to the volume group using the following SMIT fast path:

   ```
   smit extendvg
   ```

2. Mirror the volume group onto the new disk by typing the following SMIT fast path:

   ```
   smit mirrorvg
   ```

3. In the first panel, select a volume group for mirroring.
4. In the second panel, you can define mirroring options or accept defaults. Online help is available if you need it.

Note: When you complete the SMIT panels and click OK or exit, the underlying command can take a significant amount of time to complete. The length of time is affected by error checking, the size and number of logical volumes in the volume group, and the time it takes to synchronize the newly mirrored logical volumes.

At this point, all changes to the logical volumes will be mirrored as you specified in the SMIT panels.

Mirroring the Root Volume Group

The following scenario explains how to mirror the root volume group (rootvg).

Notes:

1. Mirroring the root volume group requires advanced system administration experience. If not done correctly, you can cause your system to be unbootable.
2. Mirrored dump devices are supported in AIX 4.3.3 or later.

In the following scenario, the rootvg is contained on `hdisk01`, and the mirror is being made to a disk called `hdisk11`:

1. Check that `hdisk11` is supported by AIX as a boot device:

   ```
   bootinfo -B hdisk11
   ```

   If this command returns a value of 1, the selected disk is bootable by AIX. Any other value indicates that `hdisk11` is not a candidate for rootvg mirroring.

2. Extend rootvg to include `hdisk11`, using the following command:

   ```
   extendvg rootvg hdisk11
   ```

   If you receive the following error messages:

   ```
   0516-050 Not enough descriptor space left in this volume group, Either try
   adding a smaller PV or use another volume group.
   ```

   or a message similar to:

   ```
   0516-1162 extendvg: Warning, The Physical Partition size of 16 requires the
   creation of 1084 partitions for hdisk11. The limitation for volume group
   rootvg is 1016 physical partitions per physical volume. Use chvg command with
   the -t option to attempt to change the maximum physical partitions per Physical
   Volume for this volume group.
   ```

   You have the following options:

   - Mirror the rootvg to an empty disk that already belongs to the rootvg.
   - Use a smaller disk.
   - Change the maximum number of partitions supported by the rootvg, using the following procedure:
     a. Check the message for the number of physical partitions needed for the destination disk and the maximum number currently supported by rootvg.
     b. Use the **chvg -t** command to multiply the maximum number of partitions currently allowed in rootvg (in the above example, 1016) to a number that is larger than the physical partitions needed for the destination disk (in the above example, 1084). For example:

        ```
        chvg -t 2 rootvg
        ```

c. Reissue the **extendvg** command at the beginning of step 2 on page 64.

3. Mirror the rootvg, using the exact mapping option, as shown in the following command:

```
mirrorvg -m rootvg hdisk11
```

This command will turn off quorum when the volume group is rootvg. If you do not use the exact mapping option, you must verify that the new copy of the boot logical volume, hd5, is made of contiguous partitions.

4. Initialize all boot records and devices, using the following command:

```
bosboot -a
```

5. Initialize the boot list with the following command:

```
bootlist -m normal hdisk01 hdisk11
```

Notes:

a. Even though the **bootlist** command identifies hdisk11 as an alternate boot disk, it cannot guarantee the system will use hdisk11 as the boot device if hdisk01 fails. In such case, you might have to boot from the product media, select **maintenance**, and reissue the **bootlist** command without naming the failed disk.

b. If your hardware model does not support the **bootlist** command, you can still mirror the rootvg, but you must actively select the alternate boot disk when the original disk is unavailable.

Removing a Disk while the System Remains Available

The following procedure describes how to remove a disk using the hot-removability feature, which lets you remove the disk without turning the system off. This feature is only available on certain systems.

Hot removability is useful when you want to:

- Remove a disk that contains data in a separate non-rootvg volume group for security or maintenance purposes. (See “Removing a Disk with Data.”)
- Permanently remove a disk from a volume group. (See “Removing a Disk without Data” on page 66.)
- Correct a disk failure. (See “Recovering from Disk Failure while the System Remains Available” on page 75.)

Removing a Disk with Data: The following procedure describes how to remove a disk that contains data without turning the system off. The disk you are removing must be in a separate non-rootvg volume group. Use this procedure when you want to move a disk to another system.

1. To list the volume group associated with the disk you want to remove, type:

```
smit lspv
```

Your output looks similar to the following:

```
PHYSICAL VOLUME:    hdisk2                  VOLUME GROUP:     imagesvg
PV IDENTIFIER:      00083772caa7896e VG IDENTIFIER     0004234500004c00000000e9b5cac262
PV STATE:           active
STALE PARTITIONS:   0                       ALLOCATABLE:      yes
PP SIZE:            16 megabyte(s)          LOGICAL VOLUMES:  5
TOTAL PPs:          542 (8672 megabytes)    VG DESCRIPTORS:   2
FREE PPs:           19 (304 megabytes)      HOT SPARE:        no
USED PPs:           523 (8368 megabytes)
FREE DISTRIBUTION:  00..00..00..00..19
USED DISTRIBUTION:  109..108..108..108..90
```

The name of the volume group is listed in the VOLUME GROUP field. In this example, the volume group is `imagesvg`.

2. To verify that the disk is in a separate non-rootvg volume group, type:

```
smit lsvg
```

Then select the volume group associated with your disk (in this example, imagesvg). Your output looks similar to the following:

```
VOLUME GROUP:   imagesvg                VG IDENTIFIER:  0004234500004c00000000e9b5cac262
VG STATE:       active                  PP SIZE:        16 megabyte(s)
VG PERMISSION:  read/write              TOTAL PPs:      542 (8672 megabytes)
MAX LVs:        256                     FREE PPs:       19 (304 megabytes)
LVs:            5                       USED PPs:       523 (8368 megabytes)
OPEN LVs:       4                       QUORUM:         2
TOTAL PVs:      1                       VG DESCRIPTORS: 2
STALE PVs:      0                       STALE PPs:      0
ACTIVE PVs:     1                       AUTO ON:        yes
MAX PPs per PV: 1016                    MAX PVs:        32
LTG size:       128 kilobyte(s)         AUTO SYNC:      no
HOT SPARE:      no
```

In this example, the TOTAL PVs field indicates there is only one physical volume associated with imagesvg. Because all data in this volume group is contained on hdisk2, hdisk2 can be removed using this procedure.

3. To unmount any file systems on the logical volumes on the disk, type:

   ```
   smit umountfs
   ```

4. To deactivate and export the volume group in which the disk resides, unconfigure the disk and turn it off, type:

   ```
   smit exportvgrds
   ```

   When the procedure completes, the system displays a message indicating the cabinet number and disk number of the disk to be removed. If the disk is placed at the front side of the cabinet, the disk shutter automatically opens.

5. Look at the LED display for the disk you want to remove. Ensure the yellow LED is off (not lit).
6. Physically remove the disk. For more information about the removal procedure, see the service guide for your machine.

At this point, the disk is physically and logically removed from your system. If you are permanently removing this disk, this procedure is completed. You can also do one of the following:

- Import the removed disk to another system. See “Importing or Exporting a Volume Group” on page 61.
- Replace the removed disk with a new one. See “Adding Disks while the System Remains Available” on page 54.

Removing a Disk without Data:

The following procedure describes how to remove a disk that contains either no data or no data that you want to keep.

Attention: The following procedure erases any data that resides on the disk.

1. To unmount any file systems on the logical volumes on the disk, type:

   ```
   smit umountfs
   ```

2. To deactivate and export any volume group in which the disk resides, unconfigure the disk and turn it off, type:

   ```
   smit exportvgrds
   ```

   When the procedure completes, the system displays a message indicating the cabinet number and disk number of the disk to be removed. If the disk is placed at the front side of the cabinet, the disk shutter automatically opens.

3. Look at the LED display for the disk you want to remove. Ensure the yellow LED is off (not lit).
4. Physically remove the disk. For more information about the removal procedure, see the service guide for your machine.

At this point, the disk is physically and logically removed from your system. If you are permanently removing this disk, this procedure is completed. If you want to replace the removed disk with a new one, see “Adding Disks while the System Remains Available” on page 54.

Removing a Logical Volume

To remove a logical volume, you can use one of the following procedures. The primary difference between the following procedures is that the procedures to remove a logical volume by removing its file system remove the file system, its associated logical volume, and its record in the **/etc/filesystems** file. The procedures to remove a logical volume remove the logical volume and its file system, but not the file system's record in **/etc/filesystems**.

Removing a Logical Volume by Removing the File System:

Attention: When you remove a file system, you destroy all data in the specified file systems and logical volume.

The following procedure explains how to remove a JFS or JFS2 file system, its associated logical volume, its associated stanza in the **/etc/filesystems** file, and, optionally, the mount point (directory) where the file system is mounted. If you want to remove a logical volume with a different type of file system mounted on it or a logical volume that does not contain a file system, refer to “Removing a Logical Volume Only” on page 68.

To remove a journaled file system through Web-based System Manager, use the following procedure:

1. If Web-based System Manager is not already running, with root authority type `wsm` on the command line.
2. Select a host name.
3. Select the **File Systems** container.
4. Select the **Journaled File Systems** container.
5. Select the file system you want to remove.
6. From the **Selected** menu, select **Unmount**.
7. From the **Selected** menu, select **Delete**.

To remove a journaled file system through SMIT, use the following procedure:

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

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

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

   ```
   smit rmfs
   ```
3. Select the name of the file system you want to remove.
4. Go to the **Remove Mount Point** field and toggle to your preference. If you select **yes**, the underlying command will also remove the mount point (directory) where the file system is mounted (if the directory is empty).
5. Press Enter to remove the file system. SMIT prompts you to confirm whether you want to remove the file system.
6. Confirm you want to remove the file system. SMIT displays a message when the file system has been removed successfully.

At this point, the file system, its data, and its associated logical volume are completely removed from your system.

Removing a Logical Volume Only:

Attention: Removing a logical volume destroys all data in the specified file systems and logical volume.

The following procedures explain how to remove a logical volume and any associated file system. You can use this procedure to remove a non-JFS file system or a logical volume that does not contain a file system. After the following procedures describe how to remove a logical volume, they describe how to remove any non-JFS file system's stanza in the **/etc/filesystems** file.

To remove a logical volume through Web-based System Manager, use the following procedure:

1. If Web-based System Manager is not already running, with root authority, type `wsm` on the command line.
2. Select a host name.
3. If the logical volume does not contain a file system, skip to step 10.
4. Select the **File Systems** container.
5. Select the container for the appropriate file system type.
6. Select the file system you want to unmount.
7. From the **Selected** menu, select **Unmount**.
8. Select the appropriate file system container in the navigation area to list its file systems.
9. Note the logical volume name of the system you want to remove.
10. Select the **Volumes** container.
11. Select the **Logical Volumes** container.
12. Select the logical volume you want to remove.
13. From the **Selected** menu, select **Delete**.

To remove a logical volume through SMIT, use the following procedure:

1. If the logical volume does not contain a file system, skip to step 4 on page 69.
2. Unmount all file systems associated with the logical volume by typing:

   `unmount /FSname`

   Where */FSname* is the full path name of a file system.

   Notes:

   a. The **unmount** command fails if the file system you are trying to unmount is currently being used. The **unmount** command executes only if none of the file system's files are open and no user's current directory is on that device.

   b. Another name for the **unmount** command is **umount**. The names are interchangeable.
3. To list information you need to know about your file systems, type the following fast path:

   `smit lsfs`

   The following is a partial listing:

```
Name            Nodename   Mount Pt         ...

/dev/hd3        --         /tmp             ...

/dev/locallv    --         /adam/usr/local  ...
```

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

   `smit lslv2`

   The following is a partial listing:

```
imagesvg:
LV NAME             TYPE       LPs   PPs   PVs  LV STATE      MOUNT POINT
hd3                 jfs        4     4     1    open/syncd    /tmp
locallv             mine       4     4     1    closed/syncd  /adam/usr/local
```

4. To remove the logical volume, type the following fast path on the command line:

   ```
   smit rmlv
   ```

5. Select the name of the logical volume you want to remove.
6. Go to the **Remove Mount Point** field and toggle to your preference. If you select **yes**, the underlying command will also remove the mount point (directory) where the file system is mounted (if any, and if that directory is empty).
7. Press Enter to remove the logical volume. SMIT prompts you to confirm whether you want to remove the logical volume.
8. Confirm you want to remove the logical volume. SMIT displays a message when the logical volume has been removed successfully.
9. If the logical volume had a non-JFS file system mounted on it, remove the file system and its associated stanza in the **/etc/filesystems** file, as shown in the following example:

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

   Or, you can use the file system name as follows:

   ```
   rmfs /dev/locallv
   ```

At this point, the logical volume is removed. If the logical volume contained a non-JFS file system, that system's stanza has also been removed from the **/etc/filesystems** file.

Resize a RAID Volume Group

In AIX 5.2 and later versions, on systems that use a redundant array of independent disks (RAID), **chvg** and **chpv** command options provide the ability to add a disk to the RAID group and grow the size of the physical volume that LVM uses without interruptions to the use or availability of the system.

Notes:

1. This feature is not available while the volume group is activated in classic or in enhanced concurrent mode.
2. The rootvg volume group cannot be resized using the following procedure.
3. A volume group with an active paging space cannot be resized using the following procedure.

The size of all disks in a volume group is automatically examined when the volume group is activated (varyon). If growth is detected, the system generates an informational message.

The following procedure describes how to grow disks in a RAID environment:

1. To check for disk growth and resize if needed, type the following command:

   ```
   chvg -g VGname
   ```

   Where *VGname* is the name of your volume group. This command examines all disks in the volume group. If any have grown in size, it attempts to add physical partitions to the physical volume. If necessary, it will determine the appropriate 1016 limit multiplier and convert the volume group to a big volume group.
2. To turn off LVM bad block relocation on a RAID disk, type the following command:

   ```
   chpv -r ny PVname
   ```

   Where *PVname* is the name of your physical volume.

LVM Troubleshooting Tasks

The topics in this section provide diagnostics and recovery procedures to use if you encounter one of the following:

- “Disk Drive Problems”
- “Physical or Logical Volume Errors” on page 76
- “Volume Group Errors” on page 78

Disk Drive Problems

If your disk drive is running out of available space, see “Getting More Space on a Disk Drive.” If you suspect a disk drive is mechanically failing or has failed, run diagnostics on the disk use the following procedure:

1. With root authority, type the following SMIT fast path on the command line:
   ```
   smit diag
   ```
2. Select **Current Shell Diagnostics** to enter the AIX Diagnostics tool.
3. After you read the Diagnostics Operating Instructions screen, press Enter.
4. Select **Diagnostics Routines**.
5. Select **System Verification**.
6. Scroll down through the list to find and select the drive you want to test.
7. Select **Commit**.

Based on the diagnostics results, you should be able to determine the condition of the disk:

- If you detect the disk drive is failing or has failed, of primary importance is recovering the data from that disk. If the disk is still accessible, try completing the procedure in “Migrating the Contents of a Physical Volume” on page 61. Migration is the preferred way to recover data from a failing disk. The following procedures describe how to recover or restore data in logical volumes if migration cannot complete successfully.
- 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 71.
- If the disk drive must be reformatted or replaced, make a backup, if possible, and remove the disk drive from its volume group and system configuration before replacing it. Some data from single-copy file systems might be lost. See “Recovering Using a Reformatted or Replacement Disk Drive” on page 71.
- If your system supports the hot removability feature, see “Recovering from Disk Failure while the System Remains Available” on page 75.

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

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

Cleaning Up File Systems Automatically: Use the **skulker** command to clean up file systems by removing unwanted files. Type the following from the command line:

```
skulker -p
```

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

The **skulker** command is typically run daily, as part of an accounting procedure run by the **cron** command during off-peak hours. For more information about using the **skulker** command in a **cron** process, see “Fix Disk Overflows” on page 90.

For information on typical **cron** entries, see “Setting Up an Accounting System” on page 104.

Restricting Users from Certain Directories: Another way to release disk space and possibly to keep it free is to restrict and monitor disk usage.

- Restrict users from certain directories by typing:

  ```
  chmod 655 DirName
  ```

  This command sets read and write permissions for the owner (root) and sets read-only permissions for the group and others. *DirName* is the full path name of the directory you want to restrict,
- Monitor the disk usage of individual users. One way to do this is to add the following line to the **/var/spool/cron/crontabs/adm** file:

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

  This line executes the **dodisk** command at 2 a.m. (`0 2`) each Thursday (`4`). The **dodisk** command initiates disk-usage accounting. This command is usually run as part of an accounting procedure run by the **cron** command during off-peak hours. See "Setting Up an Accounting System" on page 104 for more information on typical **cron** entries.

Mounting Space from Another Disk Drive: Another way to get more space on a disk drive is to mount space from another drive. You can mount space from one disk drive to another in the following ways:

- 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 "Mount a JFS or JFS2" on page 86.

Recovering a Disk Drive without Reformatting: If you repair a bad disk and place it back in the system without reformatting it, you can let the system automatically activate and resynchronize the stale physical partitions on the drive at boot time. A stale physical partition contains data your system cannot use.

If you suspect a stale physical partition, type the following on the command line:

```
lspv -M PhysVolName
```

Where *PhysVolName* is the name of your physical volume. The **lspv** command output will list all partitions on your physical volume. The following is an excerpt from example output:

```
hdisk16:112     lv01:4:2        stale
hdisk16:113     lv01:5:2        stale
hdisk16:114     lv01:6:2        stale
hdisk16:115     lv01:7:2        stale
hdisk16:116     lv01:8:2        stale
hdisk16:117     lv01:9:2        stale
hdisk16:118     lv01:10:2       stale
```

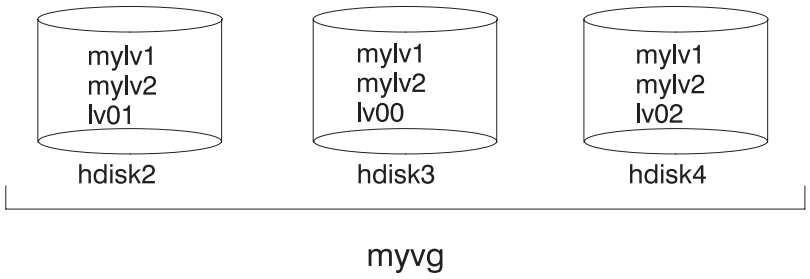
The first column displays the physical partitions and the second column displays the logical partitions. Any stale physical partitions are noted in the third column.

Recovering Using a Reformatted or Replacement Disk Drive: This section describes how to recover data from a failed disk drive when you must reformat or replace the failed disk.

Attention: Before you reformat or replace a disk drive, remove all references to nonmirrored file systems from the failing disk and remove the disk from the volume group and system configuration. If you do not, you create problems in the ODM (object data manager) and system configuration databases. Instructions for these essential steps are included in the following procedure, under "Before replacing or reformatting your failed or failing disk" on page 72.

The following procedure uses a scenario in which the volume group called **myvg** contains three disk drives called hdisk2, hdisk3, and hdisk4. In this scenario, hdisk3 goes bad. The nonmirrored logical volume **lv01** and a copy of the **mylv** logical volume is contained on hdisk2. The **mylv** logical volume is

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



This procedure is divided into the following key segments:

- The things you do to protect data before replacing or reformatting your failing disk
- The procedure you follow to reformat or replace the disk
- The things you do to recover the data after the disk is reformatted or replaced

Before replacing or reformatting your failed or failing disk:

1. Log in with root authority.
2. If you are not familiar with the logical volumes that are on the failing drive, use an operational disk to view the contents of the failing disk. For example, to use hdisk4 to look at hdisk3, type the following on the command line:

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

   The **lspv** command displays information about a physical volume within a volume group. The output looks similar to 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.
3. Back up all single-copy logical volumes on the failing device, if possible. For instructions, see “Backing Up and Restoring Information” on page 34.
4. If you have single-copy file systems, unmount them from the disk. (You can identify single-copy file systems from the output of the **lspv** command. Single-copy file systems have the same number of logical partitions as physical partitions on the output.) Mirrored file systems do not have to be unmounted.

   In the scenario, `lv00` on the failing disk `hdisk3` is a single-copy file system. To unmount it, type the following:

   ```
   unmount /dev/lv00
   ```

   If you do not know the name of the file system, assuming the **/etc/filesystems** file is not solely located on the failed disk, type **mount** on the command line to list all mounted file systems and find the name associated with your logical volume. You can also use the **grep** command on the **/etc/filesystems** file to list only the file system names, if any, associated with your logical volume. For example:

   ```
   grep lv00 /etc/filesystems
   ```

   The output looks similar to the following:

```
dev             = /dev/lv00
log             = /dev/loglv00
```

Notes:

a. The **unmount** command fails if the file system you are trying to unmount is currently being used. The **unmount** command executes only if none of the file system's files are open and no user's current directory is on that device.

b. Another name for the **unmount** command is **umount**. The names are interchangeable.

5. Remove all single-copy file systems from the failed physical volume by typing the **rmfs** command:

   ```
   rmfs /FSname
   ```

6. Remove all mirrored logical volumes located on the failing disk.

   Note: You cannot use **rmlvcopy** on the hd5 and hd7 logical volumes from physical volumes in the rootvg volume group. The system does not allow you to remove these logical volumes because there is only one copy of these.

   The **rmlvcopy** command removes copies from each logical partition. For example, type:

   ```
   rmlvcopy mylv 2 hdisk3
   ```

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

7. If the failing disk was part of the root volume group and contained logical volume hd7, remove the primary dump device (hd7) by typing the following on the command line

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

   The **sysdumpdev** command changes the primary or secondary dump device location for a running system. When you reboot, the dump device returns to its original location.

8. Remove any paging space located on the disk using the following command:

   ```
   rmps PSname
   ```

   Where *PSname* is the name of the paging space to be removed, which is actually the name of the logical volume on which the paging space resides.

   If the **rmps** command is not successful, you must use the **smit chps** fast path to deactivate the primary paging space and reboot before continuing with this procedure. The **reducevg** command in step 10 can fail if there are active paging spaces.

9. Remove any other logical volumes from the volume group, such as those that do not contain a file system, using the **rmlv** command. For example, type:

   ```
   rmlv -f lv00
   ```

10. Remove the failed disk from the volume group using the **reducevg** command. For example, type:

    ```
    reducevg -df myvg hdisk3
    ```

    If you cannot execute the reducevg command or if the command is unsuccessful, the procedure in step 13 on page 74 can help clean up the VGDA/ODM information after you reformat or replace the drive

Replacing or reformatting your failed or failing disk:

11. The next step depends on whether you want to reformat or replace your disk and on what type of hardware you are using:

    - If you want to reformat the disk drive, use the following procedure:

      a. With root authority, type the following SMIT fast path on the command line:

         ```
         smit diag
         ```

      b. Select **Current Shell Diagnostics** to enter the AIX Diagnostics tool.

      c. After you read the Diagnostics Operating Instructions screen, press Enter.

      d. Select **Task Selection**.

      e. Scroll down through the task list to find and select **Format Media**.

f. Select the disk you want to reformat. After you confirm that you want to reformat the disk, all content on the disk will be erased.

After the disk is reformatted, continue with step 12.

- If your system supports hot swap disks, use the procedure in “Recovering from Disk Failure while the System Remains Available” on page 75 then continue with step 13.
- If your system does not support hot swap disks, do the following:
  - Power off the old drive using the SMIT fast path **smit rmvdsk**. Change the KEEP definition in database field to No.
  - Contact your next level of system support to replace the disk drive.

After replacing or reformatting your failed or failing disk:

12. Follow the instructions in “Configuring a Disk” on page 49 and “Making an Available Disk a Physical Volume” on page 51.
13. If you could not use the **reducevg** command on the disk from the old volume group before the disk was formatted (step 10 on page 73), the following procedure can help clean up the VGDA/ODM information.
    a. If the volume group consisted of only one disk that was reformatted, type:

       ```
       exportvg VGName
       ```

       Where *VGName* is the name of your volume group.

    b. If the volume group consists of more than one disk, type the following on the command line:

       ```
       varyonvg VGName
       ```

       The system displays a message about a missing or unavailable disk, and the new (or reformatted) disk is listed. Note the physical volume identifier (PVID) of the new 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. For example:

       ```
       hdisk3 00083772caa7896e PVNOTFND
       ```

       Type:

       ```
       varyonvg -f VGName
       ```

       The missing disk is now displayed with the PVREMOVED label. For example:

       ```
       hdisk3 00083772caa7896e PVREMOVED
       ```

       Then, type the command:

       ```
       reducevg -df VGName PVID
       ```

       Where PVID is the physical volume identifier (in this scenario, 00083772caa7896e).
14. To add the new disk drive to the volume group, use the **extendvg** command. For example, type:

    ```
    extendvg myvg hdisk3
    ```
15. To re-create the single-copy logical volumes on the new (or reformatted) disk drive, use the **mklv** command. For example, type:

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

    This example recreates the lv00 logical volume on the hdisk3 drive. The `1` means that this logical volume is not mirrored.
16. To re-create the file systems on the logical volume, use the **crfs** command. For example, type

    ```
    crfs -v jfs -d lv00 -m /dev/lv00
    ```
17. To restore single-copy file system data from backup media, see “Restoring from Backup Image Individual User Files” on page 39.
18. To re-create the mirrored copies of logical volumes, use the **mklvcopy** command. For example, type:

    ```
    mklvcopy mylv 3 hdisk3
    ```

    This example creates a mirrored third partition of the **mylv** logical volume on hdisk3.

19. To synchronize the new mirror with the data on the other mirrors (in this example, hdisk2 and hdisk4), use the **syncvg** command. For example, type:

    ```
    syncvg -p hdisk3
    ```

At this point, 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 illustrates a specific instance. It is not intended as a general prototype on which to base any general recovery procedures.

1. The system manager, Jane, created a volume group called **workvg** on hdisk1, by typing:

   ```
   mkvg -y workvg hdisk1
   ```

2. She then created two more disks for this volume group, by typing:

   ```
   extendvg workvg hdisk2

   extendvg workvg hdisk3
   ```

3. Jane created a logical volume of 40 MB that has three copies. Each copy is on one of each of the three disks that comprise the **workvg** volume group. She used the following commands:

   ```
   mklv -y testlv workvg 10

   mklvcopy testlv 3
   ```

After Jane created the mirrored workvg volume group, hdisk2 failed. Therefore, she took the following steps to recover:

1. She removed the logical volume copy from hdisk2 by typing:

   ```
   rmlvcopy testlv 2 hdisk2
   ```

2. She detached hdisk2 from the system so that the ODM and VGDA are updated, by typing:

   ```
   reducevg workvg hdisk2
   ```

3. She removed hdisk2 from the system configuration to prepare for replacement by typing:

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

4. She chose to shut down the system, by typing:

   ```
   shutdown -F
   ```

5. She replaced the disk. The new disk did not have the same SCSI ID as the former hdisk2.
6. She rebooted the system.

   Because you have a new disk (the system sees that there is a new PVID on this disk), the system chooses the first *open* hdisk name. Because the **-d** flag was used in step 3, the name hdisk2 was released, so the system chose hdisk2 as the name of the new disk. If the **-d** flag had not been used, hdisk4 would have been chosen as the new name.

7. Jane added this disk into the **workvg** volume group by typing:

   ```
   extendvg workvg hdisk2
   ```

8. She created two mirrored copies of the logical volume by typing:

   ```
   mklvcopy testlv 3
   ```

   The Logical Volume Manager automatically placed the third logical volume copy on the new hdisk2.

Recovering from Disk Failure while the System Remains Available: The procedure to recover from disk failure using the hot removability feature is, for the most part, the same as described in “Recovering a Disk Drive without Reformatting” on page 71, with the following exceptions:

1. To unmount file systems on a disk, use the procedure “Mount a JFS or JFS2” on page 86.
2. To remove the disk from its volume group and from the operating system, use the procedure “Removing a Disk without Data” on page 66.
3. To replace the failed disk with a new one, you do not need to shut down the system. Use the following sequence of procedures:
   a. “Adding Disks while the System Remains Available” on page 54
   b. “Configuring a Disk” on page 49
   c. Continue with step 13 on page 74 of “Recovering Using a Reformatted or Replacement Disk Drive” on page 71.

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, use one of the following procedures:

- Add fixed disk without data to existing volume group
- Add fixed disk without data to new volume group
- “Migrating the Contents of a Physical Volume” on page 61

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

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

Physical or Logical Volume Errors

This section contains possible problems with and solutions for physical or logical volume errors.

Hot Spot Problems: If you notice performance degradation when accessing logical volumes, you might have hot spots in your logical volumes that are experiencing too much disk I/O. For more information, see *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices* and “Enabling and Configuring Hot Spot Reporting” on page 60.

LVCB Warnings: The logical volume control block (LVCB) is the first 512 bytes of a logical volume. This area holds important information such as the creation date of the logical volume, information about mirrored copies, and possible mount points in the JFS. Certain LVM commands are required to update the LVCB, as part of the algorithms in LVM. The old LVCB is read and analyzed to see if it is a valid. If the information is valid LVCB information, the LVCB is updated. If the information is not valid, the LVCB update is not performed, and you might receive the following message:

```
Warning, cannot write lv control block data.
```

Most of the time, this message results when database programs bypass the JFS and access raw logical volumes as storage media. When this occurs, the information for the database is literally written over the LVCB. For raw logical volumes, this is not fatal. After the LVCB is overwritten, the user can still:

- Expand a logical volume
- Create mirrored copies of the logical volume
- Remove the logical volume
- Create a journaled file system to mount the logical volume

There are limitations to deleting LVCBs. A logical volumes with a deleted LVCB might not import successfully to other systems. During an importation, the LVM **importvg** command scans the LVCBs of all defined logical volumes in a volume group for information concerning the logical volumes. If the LVCB does not exist, the imported volume group still defines the logical volume to the new system that is accessing this volume group, and the user can still access the raw logical volume. However, the following typically happens:

- Any JFS information is lost and the associated mount point is not imported to the new system. In this case, you must create new mount points, and the availability of previous data stored in the file system is not ensured.
- Some non-JFS information concerning the logical volume cannot be found. When this occurs, the system uses default logical volume information to populate the ODM information. Thus, some output from the **lslv** command might be inconsistent with the real logical volume. If any logical volume copies still exist on the original disks, the information is not be correctly reflected in the ODM database. Use the **rmlvcopy** and **mklvcopy** commands to rebuild any logical volume copies and synchronize the ODM.

Physical Partition Limits: In the design of Logical Volume Manager (LVM), each logical partition maps to one physical partition (PP). And, each physical partition maps to a number of disk sectors. The design of LVM limits the number of physical partitions that LVM can track per disk to 1016. In most cases, not all of the 1016 tracking partitions are used by a disk. When this limit is exceeded, you might see a message similar to the following:

```
0516-1162 extendvg: Warning, The Physical Partition Size of PPsize requires the
creation of TotalPPs partitions for PVname.  The limitation for volume group
VGname is LIMIT physical partitions per physical volume.  Use chvg command
with -t option to attempt to change the maximum Physical Partitions per
Physical volume for this volume group.
```

Where:

PPsize
: Is 1 MB to 1 GB in powers of 2.

Total PPs
: Is the total number of physical partitions on this disk, given the *PPsize*.

PVname
: Is the name of the physical volume, for example, hdisk3.

VGname
: Is the name of the volume group.

LIMIT Is 1016 or a multiple of 1016.

This limitation is enforced in the following instances:

1. When creating a volume group using the **mkvg** command, you specified a number of physical partitions on a disk in the volume group that exceeded 1016. To avoid this limitation, you can select from the physical partition size ranges of 1, 2, 4 (the default), 8, 16, 32, 64, 128, 256, 512 or 1024 MB and use the **mkvg -s** command to create the volume group. Alternatively, you can use a suitable factor that allows multiples of 1016 partitions per disk, and use the **mkvg -t** command to create the volume group.
2. When adding a disk to a pre-existing volume group with the **extendvg** command, the new disk caused the 1016 limitation violation. To resolve this situation, convert the existing volume group to hold multiples of 1016 partitions per disk using the **chvg -t** command. Alternatively, you can re-create the volume group with a larger partition size that allows the new disk, or you can create a standalone volume group consisting of a larger physical size for the new disk.

Partition Limitations and the rootvg: If the installation code detects that the rootvg drive is larger than 4 GB, it changes the **mkvg -s** value until the entire disk capacity can be mapped to the available 1016 tracks. This installation change also implies that all other disks added to rootvg, regardless of size, are also defined at that physical partition size.

Partition Limitations and RAID Systems: For systems using a redundant array of identical disks (RAID), the **/dev/hdiskX** name used by LVM may consist of many non-4 GB disks. In this case, the 1016

requirement still exists. LVM is unaware of the size of the individual disks that really make up **/dev/hdiskX**. LVM bases the 1016 limitation on the recognized size of **/dev/hdiskX**, and not the real physical disks that make up **/dev/hdiskX**.

Synchronizing the Device Configuration Database: A system malfunction can cause the device configuration database to become inconsistent with the LVM. When this happens, a logical volume command generates such error messages as:

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

OR

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

(where the logical volume called *LVname* is normally available).

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.

To synchronize the device configuration database with the LVM information, with root authority, type the following on the command line:

```
synclvodm -v VGName
```

Where *VGName* is the name of the volume group you want to synchronize.

Volume Group Errors

If the **importvg** command is not working correctly, try refreshing the device configuration database. See "Synchronizing the Device Configuration Database."

Overriding a Vary-On Failure:

Attention: Overriding a vary-on failure is an unusual operation; check all other possible problem sources such as hardware, cables, adapters, and power sources before proceeding. Overriding a quorum failure during a vary-on process is used only in an emergency and only as a last resort (for example, to salvage data from a failing disk). Data integrity cannot be guaranteed for management data contained in the chosen copies of the VGDA and the VGSA when a quorum failure is overridden.

When you choose to forcibly vary-on a volume group by overriding the absence of a quorum, the PV STATE of all physical volumes that are missing during this vary-on process will be changed to removed. This means that all the VGDA and VGSA copies are removed from these physical volumes. After this is done, these physical volumes will no longer take part in quorum checking, nor are they allowed to become active within the volume group until you return them to the volume group.

Under one or more of the following conditions, you might want to override the vary-on failure so that the data on the available disks in the volume group can be accessed:

- Unavailable physical volumes appear permanently damaged.
- You can confirm that at least one of the presently accessible physical volumes (which must also contain a good VGDA and VGSA copy) was online when the volume group was last varied on. Unconfigure and power off the missing physical volumes until they can be diagnosed and repaired.

Use the following procedure to avoid losing quorum when one disk is missing or might soon fail and requires repair:

1. To temporarily remove the volume from the volume group, type:

   ```
   chpv -vr PVname
   ```

When this command completes, the physical volume *PVname* is no longer factored in quorum checking. However, in a two-disk volume group, this command fails if you try the **chpv** command on the disk that contains the two VGDA/VGSAs. The command does not allow you to cause quorum to be lost.

2. If you need to remove the disk for repair, power off the system, and remove the disk. (For instructions, see "Disk Drive Problems" on page 70.) After fixing the disk and returning the disk to the system, continue with the next step.
3. To make the disk available again to the volume group for quorum checking, type:

   ```
   chpv -v PVname
   ```

   Note: The **chpv** command is used only for quorum-checking alteration. The data that resides on the disk is still there and must be moved or copied to other disks if the disk is not to be returned to the system.

VGDA Warnings: In some instances, the user experiences a problem adding a new disk to an existing volume group or in creating of a new volume group. The message provided by LVM is:

```
0516-1163 extendvg: VGname already has maximum physical volumes.  With the maximum
number of physical partitions per physical volume being LIMIT, the maximum
number of physical volumes for volume group VGname is MaxDisks.
```

Where:

VGname
: Is the name of the volume group.

LIMIT Is 1016 or a multiple of 1016.

MaxDisks
: Is the maximum number of disks in a volume group. For example, if there are 1016 physical partitions (PPs) per disk, then *MaxDisk* is 32; if there are 2032, then *MaxDisk* is 16.

You can modify the **image.data** file and then use alternate disk installation, or restore the system using the **mksysb** command to re-create the volume group as a big volume group. For more information, see the *AIX 5L Version 5.2 Installation Guide and Reference*.

On older AIX versions when the limit was smaller than 32 disks, the exception to this description of the maximum VGDA was the **rootvg**. To provide users with more free disk space, when rootvg was created, the **mkvg -d** command used the number of disks selected in the installation menu as the reference number. This **-d** number is 7 for one disk and one more for each additional disk selected. For example, if two disks are selected, the number is 8 and if three disks are selected, the number is 9, and so on.

Paging Space and Virtual Memory

This section provides several procedures for configuring, maintaining, and troubleshooting paging space and virtual memory. For concepts and background information, see Paging Space and Virtual Memory in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Paging Space Configuration Tasks

This section provides instructions for the following paging space configuration tasks:

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

Adding and Activating Paging Space

To make paging space available to your system, you must add and activate the paging space. The total amount of paging space is often determined by trial and error. One commonly used guideline is to double the RAM size and use that figure as a paging space target. To use the Web-based System Manager wizard to increase paging space, select the **Volumes** container, then the **Paging Space** container. From the Selected menu, choose **Increase Paging Space→ Wizard**.

If you prefer to use SMIT, type one of the following fast paths on the command line:

- To list your current paging space, type: **smit lsps**
- To add paging space, type: **smit mkps**
- To activate paging space, type: **smit swapon**

Configuring Paging Space to Improve Performance

To improve paging performance, use multiple paging spaces and locate them on separate physical volumes whenever possible. However, more than one paging 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 the rootvg volume group unless you are thoroughly familiar with your system.

Setting the PSALLOC Environment Variable for Early Allocation Mode

The operating system uses the **PSALLOC** environment variable to determine the mechanism used for memory and paging space allocation. The default setting is `late`. For a description of the early and late alternatives for the **PSALLOC** environment variable, see Comparing Late and Early Paging Space Allocation in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

The following examples show different ways to change the **PSALLOC** environment variable to `early`. The method you choose depends on how broadly you want to apply the change.

- Type the following command on a shell command line:

  ```
  PSALLOC=early;export PSALLOC
  ```

  This command causes all subsequent commands run from that shell session to run in early allocation mode.
- Add the following command in a shell resource file (**.shrc** or **.kshrc**):

  ```
  PSALLOC=early;export PSALLOC
  ```

  This entry causes all processes in your login session, with the exception of the login shell, to run under early allocation mode. This method also protects the processes from the **SIGKILL** signal mechanism.
- With root authority, add the following entry to the **/etc/environment** file:

  ```
  PSALLOC=early
  ```

  This entry causes all processes in the system, except the **init** process (process ID 1) to run in the early allocation mode. This method also protects the processes from the **SIGKILL** signal mechanism.
- Insert the **putenv** subroutine inside a program to set the **PSALLOC** environment variable to `early`. Using this method, the early allocation behavior takes effect at the next call to the **exec** subroutine.

Paging Space Maintenance Tasks

After paging space is created and activated, use the tasks in this section to maintain or remove it. This section is divided depending on the type of paging space you want to affect:

- To manage user-added paging space, see “Changing or Removing a Paging Space.”
- To manage the default paging logical volume (hd6), see “Resizing or Moving the hd6 Paging Space” on page 81

Changing or Removing a Paging Space

Changing the characteristics of a paging space can be done with Web-based System Manager, or you can type the following SMIT fast path on the command line: **smit chps**.

The procedure to remove a paging space is more risky, especially if the paging space you want to remove is a default paging space, such as hd6. A special procedure is required for removing the default paging spaces, because they 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.

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

To remove an existing paging space, use the following procedure:

1. With root authority, deactivate the paging space by typing the following SMIT fast path on the command line: **smit swapoff**.
2. If the paging space you are removing is the default dump device, you must change the default dump device to another paging space or logical volume before removing the paging space. To change the default dump device, type the following command:

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

3. Remove the paging space by typing the following fast path: **smit rmps**.

Resizing or Moving the hd6 Paging Space

You might want to reduce or move the default paging space in order to accomplish the following:

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

Whether moving the paging space or reducing its size, the rationale is the same: move paging space activity to disks that are less busy. The installation default creates a paging logical volume (hd6) on drive hdisk0, that contains part or all of the busy **/** (root) and **/usr** file systems. If the minimum inter-disk 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 can significantly improve performance. Even if the maximum inter-disk allocation policy is implemented and both **/** and **/usr** are distributed across multiple physical volumes, your hdisk2 (assuming three disks) likely contains fewer logical partitions belonging to the busiest file systems. (For more information on inter-disk allocation policies, see Choosing an Inter-Disk Allocation Policy for Your System in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

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.

Making the hd6 Paging Space Smaller: The following procedure uses the **chps** command to shrink existing paging spaces, including the primary paging space and the primary and secondary dump device. This command calls the **shrinkps** script, which safely shrinks the paging space without leaving the system in an unbootable state. Specifically, the script does the following:

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

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

Note: If the following procedure encounters an I/O error, the system might require immediate shutdown and rebooting.

1. Check your logical volume and file system distribution across physical volumes by typing the following command:

   ```
   lspv -l hdiskX
   ```

   Where *hdiskX* is the name of your physical volume.
2. To shrink the paging space size, type the following on the command line:

   ```
   smit chps
   ```

Note: The primary paging space is hardcoded in the boot record. Therefore, the primary paging space will always be activated when the system is restarted. The **chps** command cannot deactivate the primary paging space.

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

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

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

Moving the hd6 Paging Space within the Same Volume Group: Moving the default paging space from hdisk0 to a different disk within the same volume group does not require the system to shut down and reboot.

With root authority, type the following command to move the default (hd6) paging space from hdisk0 to hdisk2:

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

Attention: Moving a paging space with the name hd6 from rootvg to another volume group is not recommended because the name is hardcoded in several places, including the second phase of the boot process and the process that accesses the root volume group when booting from removable media. Only the paging spaces in rootvg are active during the second phase of the boot process, and having no paging space in rootvg could severely affect system boot performance. If you want the majority of paging space on other volume groups, it is better to make hd6 as small as possible (the same size as physical memory) and then create larger paging spaces on other volume groups (see “Adding and Activating Paging Space” on page 80).

Paging Space Troubleshooting

The total amount of paging space is often determined by trial and error. One commonly used guideline is to double the RAM size and use that figure as a paging space target. The most common problem regarding paging space is caused by running out of allocated space. If paging space runs low, processes can be lost, and if paging space runs out, the system can panic. The following signal and error information can help you monitor and resolve or prevent paging space problems.

The operating system monitors the number of free paging space blocks and detects when a paging-space shortage exists. When the number of free paging-space blocks falls below a threshold known as the *paging-space warning level*, the system informs all processes (except **kprocs**) of this condition by sending the **SIGDANGER** signal. If the shortage continues and falls below a second threshold known as the *paging-space kill level*, the system sends the **SIGKILL** signal to processes that are the major users of paging space and that do not have a signal handler for the **SIGDANGER** signal. (The default action for the **SIGDANGER** signal is to ignore the signal.) The system continues sending **SIGKILL** signals until the number of free paging-space blocks is above the paging-space kill level.

Note: If the **low_ps_handling** parameter is set to 2 (under the **vmo** command) and if no process was found to kill (without the **SIGDANGER** handler), the system will send the **SIGKILL** signal to the youngest processes that have a signal handler for the **SIGDANGER** signal.

Processes that dynamically allocate memory can ensure that sufficient paging space exists by monitoring the paging-space levels with the **psdanger** subroutine or by using special allocation routines. You can use the **disclaim** subroutine to prevent processes from ending when the paging-space kill level is reached. To do this, define a signal handler for the **SIGDANGER** signal and release memory and paging-space resources allocated in their data and stack areas and in shared memory segments.

If you get error messages similar to the following, increase the paging space:

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

OR

```
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.
```

To increase the size of your paging space, see “Changing or Removing a Paging Space” on page 80 or “Resizing or Moving the hd6 Paging Space” on page 81.

Chapter 4. File Systems Management Tasks

This section provides several procedures for configuring and maintaining file systems and directories, and for troubleshooting problems you might encounter. Chapter 1, “How-To’s for System Management Tasks,” on page 1 provides scenarios for additional file system tasks, such as how to use the snapshot feature (available with AIX 5.2 and later versions) to protect the integrity of your file systems from potential disk failure.

This chapter describes tasks for journaled file systems (JFS), enhanced journaled file systems (JFS2), and CD-ROM file systems. For your convenience, pointers to file system tasks are listed below:

File Systems Configuration Tasks

When adding or configuring file systems, you can select options in the File Systems container of Web-based System Manager or use the SMIT fast paths provided in the following table.

Table 3. Managing Logical Volumes and File Systems Tasks

Task	*SMIT Fast Path*
Add a JFS or JFS2	**smit crfs**
Add a JFS2 to an existing logical volume	**smit crjfs2lvstd**
Add a JFS to a previously defined logical volume menu	Create logical volume, then **smit crjfslv**
Change the attributes of a JFS or a JFS2 Note 1	**smit chfs**
Check size of a file system	**smit fs**
Increase size of a file system	JFS: **smit chjfs** JFS2: **smit chjfs2**

File Systems Maintenance Tasks

The simplest tasks you might need when maintaining file systems are grouped within the following table. Instructions for additional maintenance tasks are located later in this section or in Chapter 1, “How-To’s for System Management Tasks,” on page 1.

Table 4. Maintaining File Systems Tasks

Task	*SMIT Fast Path*	*Command or File*
Backup by name files or directories	**smit backfile**	**backup** Note 1
Create and backup a JFS2 snapshot image	**smit backsnap**	**backsnap** Note 1
List all file systems on a disk	**smit lsmntdsk**	
List file systems on a removable disk	**smit lsmntdsk**	
List mounted file systems	**smit fs**	
Mount a Group of File Systems Note 5	**smit mountg**	**mount -t** *GroupName*
Mount a JFS or JFS2 Note 3	**smit mountfs**	**mount**
Mount a JFS2 snapshot	**smit mntsnap**	**mount -v jfs2 -o snapshot** *Device MountPoint*
Remove a JFS or JFS2	**smit rmfs**	
Remove a JFS2 Snapshot	**smit rmsnap**	**snapshot -d** *SnapshotDevice*
Unmount a File System Note 4	**smit umountfs**	
Unmount a File System on a Removable Disk Note 4	**smit umntdsk**	
Unmount a Group of File Systems Note 5	**smit umountg**	**umount -t** *GroupName*

Notes:

1. For options, see the command description in *AIX 5L Version 5.2 Commands Reference*.
2. Do 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 hd*n* convention, start at hd10.
3. Check the file systems before mounting by using the procedure “Verify File Systems” on page 89 or running the **fsck** command.
4. 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 find out which user or process might be causing the failure.
5. A file system group is a collection of file systems which have the same value for the **type=** identifier in the **/etc/filesystems** file.

Recover One or More Files from an Online JFS2 Snapshot

When a file becomes corrupted, you can replace it if you have an accurate copy in an online JFS2 snapshot. Use the following procedure to recover one or more files from a JFS2 snapshot image:

1. Mount the snapshot. For example:
   ```
   mount -v jfs2 -o snapshot /dev/mysnaplv /home/aaa/mysnap
   ```
2. Change to the directory that contains the snapshot. For example:
   ```
   cd /home/aaa/mysnap
   ```
3. Copy the accurate file to overwrite the corrupted one. For example:
   ```
   cp myfile /home/aaa/myfs
   ```

copies only the file named `myfile`. The following example copies all files at once:

```
cp -R home/aaa/mysnap /home/aaa/myfs
```

For more examples, see the **cp** or **cpio** command descriptions in the *AIX 5L Version 5.2 Commands Reference*.

Use File Systems on CD-ROM and DVD Disks

Beginning with AIX 5.2, CDs and DVDs are automatically mounted by default but this feature can be disabled. If the feature has been disabled, use the **cdmount** command to mount the CDRFS or UDFS file system, for example:

```
cdmount cd0
```

When a DVD is automounted, the UDFS file system is read-only by default. If you want the automount feature or the cdmount command to automatically mount a read/write UDFS, edit the **cdromd.conf** file. You can also manually mount a read/write UDFS with the following command:

```
mount -V udfs DevName MtPt
```

Where *DevName* is the name of the DVD drive and *MtPt* is the mount point for the file system.

Use File Systems on Read/Write Optical Media

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

- CDRFS
- JFS

A CD-ROM file system (CDRFS) can be stored on read/write optical media, provided that the optical media is write-protected, as well as on a CD-ROM. The following table tells you how to add, mount, or unmount a CDRFS on read/write optical media. 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.

CDRFS on Optical Media Tasks		
Task	*SMIT Fast Path*	*Command or File*
Adding a CDRFS [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 CDRFS[2]	1. Unmount the file system: **smit umountfs** 2. Remove the file system: **smit rmcdrfs**	1. Unmount the file system: **umount** *FileSystem* 2. Remove the file system: **rmfs** *MountPoint*

Notes:

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

A JFS provides a read/write file system on optical media 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

Automatic mount
Specifies whether the file system will be mounted automatically at system restart

Notes:

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

JFS on Optical Media Tasks		
Task	*SMIT Fast Path*	*Command or File*
Add a JFS	1. Insert optical disk into drive. 2. Create a volume group (if necessary): **smit mkvg** 3. Create a journaled file system: **smit crfs**	1. Insert optical disk into drive. 2. Create a volume group (if necessary): **mkvg -f -y** *VGName* **-d 1** *DeviceName* 3. Create a journaled file system: **crfs -v jfs -g** *VGName* **-a size=***SizeFileSystem* **-m** *MountPoint* **-A** *AutomaticMount* **-p rw** 4. Mount the file system: **mount** *MountPoint*
Accessing previously created JFS[Note 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 JFS[Note 2]	1. Unmount the file system: **smit umountfs** 2. Remove the file system: **smit rmjfs**	1. Unmount the file system: **umount** *FileSystem* 2. Remove the file system: **rmfs** *MountPoint*

Notes:

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

Verify File Systems

Inconsistencies can occur in file systems when the system is stopped while file systems remained mounted or when a disk is damaged. In such circumstances, it is important to verify file systems before mounting them. Also verify your file systems in the following circumstances:

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

Check a User-Defined File System

1. Unmount the user-defined file system being checked.
2. Ensure you have write permission on files in the file system. Otherwise, the **fsck** cannot repair damaged files even if you answer Yes to repair prompts.
3. Use the **smit fsck** fast path to access the Verify a File System menu.
4. Do one of the following:
   a. Specify the name of an individual file system to check in the **NAME of file system** field, or
   b. Select a general file system type to check, such as a journaled file system (JFS) in the **TYPE of file system** field.
5. If you want to limit your check to the most likely candidates, specify Yes in the **FAST check?** field. The fast-check option checks only those file systems that are likely to have inconsistencies such as the file systems that were mounted when the system stopped at some point in the past.
6. Specify the name of a temporary file on a file system not being checked in the **SCRATCH file** field.
7. Start the file system check.

Check Root and /usr File Systems

To run the **fsck** command on **/** or **/usr** file system, you must shut down the system and reboot it from removable media because the **/** (root) and **/usr** file systems cannot be unmounted from a running system. The following procedure describes how to run **fsck** on the **/** and **/usr** file systems from the maintenance shell.

1. With root authority, shut down your system.
2. Boot from your installation media.
3. From the Welcome menu, choose the **Maintenance** option.
4. From the Maintenance menu, choose the option to access a volume group.
5. Choose the rootvg volume group. A list of logical volumes that belong to the volume group you selected is displayed.
6. Choose **2** to access the volume group and to start a shell before mounting file systems.

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

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

   The **-y** flag is recommended for less experienced users (see the **fsck** command).
8. To check the /usr file system, type the following:

   ```
   $ fsck -y /dev/hd2
   ```
9. To check other file systems in the rootvg, type the **fsck** command with the appropriate device names. The device for **/tmp** is **/dev/hd3**, and the device for **/var** is **/dev/hd9var**.
10. When you have completed checking the file systems, reboot the system.

File Systems Troubleshooting Tasks

The topics in this section provide diagnostics and recovery procedures to use if you encounter one of the following:

Fix 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:

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

- "Identify Problem Processes"
- "Terminate the Process"
- "Reclaim File Space without Terminating the Process"
- "Fix a / (root) Overflow" on page 91
- "Fix a /var Overflow" on page 92
- "Fix a User-Defined File System Overflow" on page 93
- "Fix Other File Systems and General Search Techniques" on page 93

Identify Problem Processes

Use the following procedure to isolate problem processes.

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

   ```
   ps -ef | pg
   ```

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

   Check for system or user processes that are using excessive amounts of a system resource, such as CPU time. System processes such as **sendmail**, **routed**, and **lpd** seem to be the system processes most prone to becoming runaways.
2. To check for user processes that use more CPU than expected, type:

   ```
   ps -u
   ```
3. Note the process ID (PID) of each problem process.

Terminate the Process

Use the following procedure to terminate a problem process:

1. Terminate the process that is causing the problem by typing:

   ```
   kill -9 PID
   ```

   Where PID is the ID of the problem process.
2. Remove the files the process has been making by typing:

   ```
   rm file1 file2 file3
   ```

   Where *file1 file2 file3* represents names of process-related files.

Reclaim File Space without Terminating the Process

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

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

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

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

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

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

Fix a / (root) Overflow

Check the following when the root file system (/) has become full:

- Use the following command to read the contents of the **/etc/security/failedlogin** file:

  ```
  who /etc/security/failedlogin
  ```

  The condition of TTYs respawning too rapidly can create failed login entries. To clear the file after reading or saving the output, execute the following command:

  ```
  cp /dev/null /etc/security/failedlogin
  ```

- Check the **/dev** directory for a device name that is typed incorrectly. If a device name is typed incorrectly, such as `rmto` instead of `rmt0`, a file will be created in **/dev** called **rmto**. The command will normally proceed until the entire root file system is filled before failing. **/dev** is part of the root (**/**) file system. Look for entries that are not devices (that do not have a major or minor number). To check for this situation, use the following command:

  ```
  cd /dev
  ls -l | pg
  ```

  In the same location that would indicate a file size for an ordinary file, a device file has two numbers separated by a comma. For example:

  ```
  crw-rw-rw-   1 root     system    12,0 Oct 25 10:19 rmt0
  ```

  If the file name or size location indicates an invalid device, as shown in the following example, remove the associated file:

  ```
  crw-rw-rw-   1 root     system   9375473 Oct 25 10:19 rmto
  ```

  Notes:

  1. Do not remove valid device names in the **/dev** directory. One indicator of an invalid device is an associated file size that is larger than 500 bytes.
  2. If system auditing is running, the default **/audit** directory can rapidly fill up and require attention.

- Check for very large files that might be removed using the **find** command. For example, to find all files in the root (/) directory larger than 1 MB, use the following command:

  ```
  find / -xdev -size  +2048 -ls |sort -r  +6
  ```

  This command finds all files greater than 1 MB and sorts them in reverse order with the largest files first. Other flags for the find command, such as **-newer**, might be useful in this search. For detailed information, see the command description for the **find** command.

Note: When checking the root directory, major and minor numbers for devices in the **/dev** directory will be interspersed with real files and file sizes. Major and minor numbers, which are separated by a comma, can be ignored.

Before removing any files, use the following command to ensure a file is not currently in use by a user process:

```
fuser filename
```

Where *filename* is the name of the suspect large file. If a file is open at the time of removal, it is only removed from the directory listing. The blocks allocated to that file are not freed until the process holding the file open is killed.

Fix a /var Overflow

Check the following when the **/var** file system has become full:

- You can use the find command to look for large files in the **/var** directory. For example:

  ```
  find /var -xdev -size  +2048 -ls| sort -r  +6
  ```

  For detailed information, see the command description for the **find** command.
- Check for obsolete or leftover files in **/var/tmp**.
- Check the size of the **/var/adm/wtmp** file, which logs all logins, rlogins and telnet sessions. The log will grow indefinitely unless system accounting is running. System accounting clears it out nightly. The **/var/adm/wtmp** file can be cleared out or edited to remove old and unwanted information. To clear it, use the following command:

  ```
  cp /dev/null  /var/adm/wtmp
  ```

  To edit the **/var/adm/wtmp** file, first copy the file temporarily with the following command:

  ```
  /usr/sbin/acct/fwtmp < /var/adm/wtmp >/tmp/out
  ```

  Edit the **/tmp/out** file to remove unwanted entries then replace the original file with the following command:

  ```
  /usr/sbin/acct/fwtmp -ic < /tmp/out > /var/adm/wtmp
  ```
- Clear the error log in the **/var/adm/ras** directory using the following procedure. The error log is never cleared unless it is manually cleared.

  Note: Never use the **cp /dev/null** command to clear the error log. A zero-length **errlog** file disables the error logging functions of the operating system and must be replaced from a backup.

  1. Stop the error daemon using the following command:

     ```
     /usr/lib/errstop
     ```
  2. Remove or move to a different filesystem the error log file by using one of the following commands:

     ```
     rm /var/adm/ras/errlog
     ```

     or

     ```
     mv /var/adm/ras/errlog filename
     ```

     Where *filename* is the name of the moved errlog file.

     Note: The historical error data is deleted if you remove the error log file.
  3. Restart the error daemon using the following command:

     ```
     /usr/lib/errdemon
     ```

  Note: Consider limiting the errlog by running the following entries in **cron**:

  ```
  0 11 * * * /usr/bin/errclear -d S,O 30
  0 12 * * * /usr/bin/errclear -d H 90
  ```
- Check whether the **trcfile** file in this directory is large. If it is large and a trace is not currently being run, you can remove the file using the following command:

  ```
  rm /var/adm/ras/trcfile
  ```

- If your dump device is set to hd6 (which is the default), there might be a number of **vmcore*** files in the **/var/adm/ras** directory. If their file dates are old or you do not want to retain them, you can remove them with the **rm** command.
- Check the **/var/spool** directory, which contains the queueing subsystem files. Clear the queueing subsystem using the following commands:

```
stopsrc -s qdaemon
rm /var/spool/lpd/qdir/*
rm /var/spool/lpd/stat/*
rm /var/spool/qdaemon/*
startsrc -s qdaemon
```

- Check the **/var/adm/acct** directory, which contains accounting records. If accounting is running, this directory may contain several large files. Information on how to manage these files is in “System Accounting” on page 104.
- Check the **/var/preserve** directory for terminated **vi** sessions. Generally, it is safe to remove these files. If a user wants to recover a session, you can use the **vi -r** command to list all recoverable sessions. To recover a specific session, use**vi -r** *filename*.
- Modify the **/var/adm/sulog** file, which records the number of attempted uses of the **su** command and whether each was successful. This is a flat file and can be viewed and modified with a favorite editor. If it is removed, it will be recreated by the next attempted **su** command. Modify the **/var/tmp/snmpd.log**, which records events from the **snmpd** daemon. If the file is removed it will be recreated by the **snmpd** daemon.

  Note: The size of the **/var/tmp/snmpd.log** file can be limited so that it does not grow indefinitely. Edit the **/etc/snmpd.conf** file to change the number (in bytes) in the appropriate section for size.

Fix a User-Defined File System Overflow

Use this procedure to fix an overflowing user-defined 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 104.

Fix Other File Systems and General Search Techniques

Use the **find** command with the **-size** flag to locate large files or, if the file system recently overflowed, use the **-newer** flag to find recently modified files. To produce a file for the **-newer** flag to find against, use the following touch command:

```
touch mmddhhmm filename
```

Where *mm* is the month, *dd* is the date, *hh* is the hour in 24–hour format, *mm* is the minute, and *filename* is the name of the file you are creating with the **touch** command.

After you have created the touched file, you can use the following command to find newer large files:

```
find /filesystem_name -xdev -newer touch_filename -ls
```

You can also use the **find** command to locate files that have been changed in the last 24 hours, as shown in the following example:

```
find /filesystem_name -xdev -mtime 0 -ls
```

Fix a Damaged File System

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

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

Procedure

1. With root authority, unmount the damaged file system using one of the following SMIT fast paths: **smit unmountfs** (for a file system on a fixed disk drive) or **smit unmntdsk** (for a file system on a removeable disk).
2. 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/myfilelv** device:

   ```
   fsck /dev/myfilelv
   ```

   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 description in *AIX 5L Version 5.2 Commands Reference* for a list of inconsistences that this command checks for.
3. If the file system cannot be repaired, restore it from backup.

   Attention: Restoring a file system from a backup destroys and replaces any file system previously stored on the disk.

   To restore the file system from backup, use the SMIT fastpath **smit restfilesys** or the series of commands shown in the following example:

   ```
   mkfs /dev/myfilelv
   mount /dev/myfilelv /myfilesys
   cd /myfilesys
   restore -r
   ```

   In this example, the **mkfs** command makes a new file system on the device named **/dev/myfilelv** and initializes the volume label, file system label, and startup block. The **mount** command establishes **/dev/myfilelv** as the mountpoint for **myfilesys** and the **restore** command extracts the file system from the backup.

   If your backup was made using incremental file system backups, you must restore the backups in increasing backup-level order (for example, 0, 1, 2). For more information about restoring a file system from backup, refer to ″Restoring from Backup Image Individual User Files″.

   When using **smit restfilesys** 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.

Chapter 5. Resource Scheduling Management Tasks

This chapter contains instructions for managing resources within the AIX operating system. Tasks are grouped within the following tools:

Workload Manager

Workload Manager (WLM) gives system administrators more control over how the scheduler and the virtual memory manager (VMM) allocate resources to processes. Using WLM, you can prevent different classes of jobs from interfering with each other and you can allocate resources based on the requirements of different groups of users.

This section contains procedures for configuring WLM with classes and rules that are appropriate for your site and suggestions for troubleshooting unexpected resource consumption behavior. Also, "Configure Workload Manager (WLM) to Consolidate Workloads" on page 2 provides instructions for creating an example configuration.

The tasks in this section assume you are familiar with WLM concepts provided in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Attention: Efficient use of WLM requires extensive knowledge of existing system processes and performance. If the system administrator configures WLM with extreme or inaccurate values, performance will be significantly degraded.

Workload Manager Configuration Tasks

Workload Manager is part of the base operating system and is installed with the base operating system, but it is an optional service. It must be configured to suit your system environment, started when you want to use it, and stopped when you want to suspend or end WLM service.

This section provides instructions for the following configuration tasks:

Instructions for creating an example WLM configuration are in "Configure Workload Manager (WLM) to Consolidate Workloads" on page 2.

Starting and Stopping WLM

WLM is an optional service that must be started and stopped. It is recommended that you use one of the system management interfaces, Web-based System Manager or SMIT, to start or stop WLM.

- To start or stop WLM using Web-based System Manager, select the Workload Manager icon from the session window.
- To start or stop WLM using SMIT, use the **smit wlmmanage** fast path.

The key difference between these options is permanence. In Web-based System Manager or SMIT, you can start or stop WLM three ways:

current session
If you request to stop WLM with this option, WLM will be stopped for this session only and restarted at next reboot. If you request a start with this option, WLM will be started for this session only and not restarted at next reboot.

next reboot
If you request to stop WLM with this option, WLM will remain running for this session only and *will not be* restarted at next reboot. If you request a start with this option, WLM will not be available for this session, but will be started at next reboot.

both If you request to stop WLM with this option, WLM will be stopped for this session only and *will not be* restarted at next reboot. If you request a start with this option, WLM will be started for this session only *and* will be restarted at next reboot.

You can also use the **wlmcntrl** command, but the **wlmcntrl** command allows you to start or stop WLM for the current session only. If you want to use the command line interface and you want the change to remain in effect when the machine is rebooted, you must edit the **/etc/inittab** file.

WLM can be used to regulate resource consumption as per-class percentages, per-class totals, or per-process totals. Regulation for all resource types can be enabled by running WLM in *active* mode. Optionally, you can start a mode of WLM that classifies new and existing processes and monitors the resource usage of the various classes, without attempting to regulate this usage. This mode is called the *passive* mode. If CPU time is the only resource that you are interested in regulating, you can choose to run WLM in active mode for CPU and passive mode for all other resources. This mode is called *cpu only* mode.

All processes existing in the system before WLM is started are classified according to the newly loaded assignment rules, and are monitored by WLM.

Specifying WLM Properties

You can specify the properties for the WLM configuration by using the Web-based System Manager, SMIT, the WLM command line interface, or by creating flat ASCII files. The Web-based System Manager and SMIT interfaces use the WLM commands to record the information in the same flat ASCII files, called *property files*.

A set of WLM property files defines a WLM configuration. You can create multiple sets of property files, defining different configurations of workload management. These configurations are located in subdirectories of **/etc/wlm**. The WLM property files describing the superclasses of the *Config* configuration are the file's *classes*, *description*, *limits*, *shares* and *rules* in **/etc/wlm/Config**. Then, the property file's describing the subclasses of the superclass *Super* of this configuration are the file's *classes*, *limits*, *shares* and *rules* in directory **/etc/wlm/Config/Super**. Only the root user can start or stop WLM, or switch from one configuration to another.

The property files are named as follows:

classes	Class definitions
description	Configuration description text
groupings	Attribute value groupings
limits	Class limits
shares	Class target shares
rules	Class assignment rules

The command to submit the WLM property files, **wlmcntrl**, and the other WLM commands allow users to specify an alternate directory name for the WLM properties files. This allows you to change the WLM properties without altering the default WLM property files.

A symbolic link, **/etc/wlm/current**, points to the directory containing the current configuration files. Update this link with the **wlmcntrl** command when you start WLM with a specified configuration or configuration set. The sample configuration files shipped with the operating system are in **/etc/wlm/standard**.

Creating an Attribute Value Grouping

You can group attribute values and represent them with a single value in the **rules** file. These*attribute value grouping* are defined in a **groupings** file within the WLM configuration directory.

By default, a configuration has no **groupings** file. There is no command or management interface to create one. To create and use attribute value groupings, use the following procedure:

1. With root authority, change to the appropriate configuration directory, as shown in the following example:

   ```
   cd /etc/wlm/MyConfig
   ```

2. Use your favorite editor to create and edit a file named **groupings**. For example:

   ```
   vi groupings
   ```

3. Define attributes and their associated values using the following format:

   attribute = *value*, *value*, ...

   All values must be separated by commas. Spaces are not significant. Ranges and wild cards are allowed. For example:

   ```
   trusted = user[0-9][0-9], admin*
   nottrusted = user23, user45
   shell = /bin/?sh, \
           /bin/sh, \
           /bin/tcsh
   rootgroup=system,bin,sys,security,cron,audit
   ```

4. Save the file.

5. To use attribute groupings within the selection criteria for a class, edit the **rules** file. The attribute grouping name must be preceded by a dollar sign ($) to include the corresponding values or the exclamation point (!) to exclude the values. The exclamation point cannot be used in the members of the group (step 3), and it is the only modifier that can be used in front of the grouping in this rules file. In the following example, the asterisk (*) signals a comment line:

   ```
   *class  resvd  user                  group       application       type  tag
   classA  -      $trusted,!$nottrusted  -           -                 -     -
   classB  -      -                     -           $shell,!/bin/zsh  -     -
   classC  -      -                     $rootgroup  -                 -     -
   ```

6. Save the file.

At this point, your classification rules includes attribute value groupings. When the rules are parsed, if an element beings with a $, the system looks for that element within the **groupings** file. If an element is syntactically invalid or if the **groupings** file does not exist, the system displays a warning message and continues processing other rules.

Creating a Time-Based Configuration Set

You can create a set of specialty configurations and assign each configuration within the set to days and times when you want a specific configuration to be in effect. These sets, called time-based *configuration sets*, are completely separate from but compatible with your normal configuration. You can use the **wlmcntrl -u** command to switch between a configuration set and your normal configuration as needed.

When using a configuration set, you associate existing named configurations, typically with a specific time range. Because only one configuration can be used at any given time, each specified time range must be unique; time ranges cannot overlap or be duplicated.

The **wlmd** daemon alerts WLM when a specified configuration goes out of time range and another configuration needs to be used. Only the root user can manage these time ranges, which are specified within the configuration set's directory in an ASCII file called **.times**.

Use the following procedure to create a time-based configuration set:

1. With root authority, create a configuration set directory then change to that directory. For example:

   ```
   mkdir /etc/wlm/MyConfigSet
   cd /etc/wlm/MyConfigSet
   ```

2. Use your favorite editor to create the configuration set's **.times** file and specify the configuration and time ranges in the following format:

   ```
   ConfigurationName:
               time = "N-N,HH:MM-HH:MM"
   ```

   or

   ```
   ConfigurationName:
                time = - (no  time  value  specified)
   ```

   Where *N* is a numeral representing a day of the week in the range of 0 (Sunday) through 6 (Saturday), *HH* represents the hour in the range of 00 (midnight) to 23 (11 p.m.), and *MM* represents the minutes in the range of 00 to 59. You can specify the day only or not at all. An hour value of 24 is valid for the ending hour of the day, provided that the minute value is 00. If you type a dash (-) instead of a time range for a particular configuration, that configuration will be used when the other configurations' time ranges are not in effect. Only one configuration can be specified without a time range.

   For example:

   ```
   conf1:
       time =
   conf2:
       time = "1-5,8:00-17:00"
   conf2
       time = "6-0,14:00-17:00"
   conf3
       time = "22:00-6:00"
   ```

3. Use the **wlmcntrl -u** command to update WLM with the new configuration set. For example:

   ```
   wlmcntrl -u /etc/wlm/MyConfigSet
   ```

At this point, WLM's current configuration is your new time-based configuration set.

You can also use the **confsetcntrl** and **lswlmconf** commands to create and manipulate configuration sets. For example:

To create the `confset1` configuration set with a default configuration of `conf1`, use the following command:

```
confsetcntrl -C confset1 conf1
```

To add `conf2` to `confset1` and make it the active configuration from 8:00 AM to 5:00 PM daily, use the following command:

```
confsetcntrl -d confset1 -a conf2 "0-6,08:00-17:00"
```

To make this configuration set the active configuration, use the following command:

```
wlmcntrl -d confset1
```

Creating a Resource Set

Using resource sets (rsets) is an effective way to isolate workloads from one another as far as the CPU is concerned. By separating two different workloads into two classes and giving each class a different subset

of the CPUs, you can make sure that the two workloads never compete with each other for CPU resources, even though they still compete for physical memory and I/O bandwidth.

The simplest way to create a resource set is to use the SMIT interface (**smit addrsetcntl** fast path) or the **mkrset** command.

For instructional purposes, the following example illustrates each step of creating and naming a resource set on a 4-way system. Its goal is to create a resource set containing processors 0 to 2, and use it in WLM configuration to restrict all processes of a superclass to these three processors.

1. With root authority, view the available building blocks (from which to create the resource sets) using the following command:

   ```
   lsrset -av
   ```

   The output for this example is the following:

   ```
   T  Name               Owner   Group   Mode    CPU  Memory  Resources
   r  sys/sys0           root    system  r-----    4   98298  sys/sys0
   r  sys/node.00000     root    system  r-----    4   98298  sys/sys0
   r  sys/mem.00000      root    system  r-----    0   98298  sys/mem.00000
   r  sys/cpu.00003      root    system  r-----    1       0  sys/cpu.00003
   r  sys/cpu.00002      root    system  r-----    1       0  sys/cpu.00002
   r  sys/cpu.00001      root    system  r-----    1       0  sys/cpu.00001
   r  sys/cpu.00000      root    system  r-----    1       0  sys/cpu.00000
   ```

   In the output, **sys/sys0** represents the whole system (in this case, a 4-way SMP). When a WLM class does not specify an **rset** attribute, this is the default set that its processes potentially can access.

2. Create and name the resource set using the following SMIT fast path:

   ```
   smit addrsetcntl
   ```

   For this example, fill in the fields as follows:

   Name Space
   admin

   Resource Set Name
   proc0_2

   Resources
   Select from the list those lines that correspond to the memory and CPUs 0 to 2 (sys/cpu.00000 to sys.cpu.00002).

   All other fields
   Select from the lists.

   When you finish entering the fields and exit SMIT, the **admin/proc0_2** rset is created in **/etc/rsets**.

3. To use the new rset, add it into the kernel data structures using the following SMIT fast path:

   ```
   smit reloadrsetcntl
   ```

   This menu gives you the option to reload the data base `now`, `at next boot` or `both`. Because this is the first time you are using the new resource set, select `both` so that this rset will be loaded now and after each reboot. (If you had changed an existing rset, you would probably have selected `now`.)

4. Add the new rset to a WLM class using the following SMIT fast path:

   ```
   smit wlmclass_gal
   ```

   Select the class (in this example, **super1**) then select **admin/proc0_2** from the list available for the Resource Set field. After you make your selection and exit SMIT, the **classes** file on disk is changed.

5. Do one of the following:
   - If WLM is running, update the configuration using the following SMIT fast path:

```
smit wlmupdate
```

- If WLM is not running, start it using the following SMIT fast path:

```
smit wlmstart
```

6. Monitor the effect of the new resource set on the class. For example:
   a. Start 90 CPU loops (program executing an infinite loop) in class **super1**.
   b. Type **wlmstat** on the command line. The output for this example is the following:

```
                CLASS CPU MEM BIO
        Unclassified   0   0   0
           Unmanaged   0   0   0
             Default   8   0   0
              Shared   0   0   0
              System   0   0   0
              super1  75   0   0
              super2   0   0   0
    super2.Default     0   0   0
     super2.Shared     0   0   0
       super2.sub1     0   0   0
       super2.sub2     0   0   0
```

   This output shows that the 90 CPU bound processes, which otherwise unconstrained would take up 100% of the CPU, now use only 75% because the resource set limits them to run on CPUs 0 to 2.

   c. To verify what resource set a process (identified by its PID) has access to, use the following SMIT fast path:

```
smit lsrsetproc
```

   Enter the PID of the process you are interested in or select it from the list. The following output is for one of the loop processes:

```
CPU  Memory  Resources
  3   98298  sys/mem.00000 sys/cpu.00002 sys/cpu.00001 sys/cpu.00000
```

   Compare this with a process from a class without a specified **rset** attribute. (When no rset is specified for a class, it uses the **Default** resource set.) The following output is from the **init** process, which is in a class that does not specify a resource set:

```
CPU  Memory  Resources
  4   98298  sys/sys0
```

At this point, your resource set exists and is being used by at least one class within WLM. For additional information see the **lsrset** command description in the *AIX 5L Version 5.2 Commands Reference*.

Note: WLM will not set its rset attachment for a process that currently has a **bindprocessor** subroutine binding or another rset attachment. When the other attachment no longer exists, WLM will assign its rset automatically.

WLM Troubleshooting Guidelines

If you are not seeing the desired behavior with your current configuration, you might need to adjust your WLM configuration. The consumption values for each class can be monitored using tools such as **wlmstat**, **wlmmon** or **wlmperf**. This data can be collected and analyzed to help determine what changes might need to be made to the configuration. After you update the configuration, update the active WLM configuration using the **wlmcntrl -u** command.

The following guidelines can help you decide how to change your configuration:

- If the number of active shares in a tier varies greatly over time, you can give a class no shares for a resource so it can have a consumption target that is independent from the number of active shares. This technique is useful for important classes that require high-priority access to a resource.

- If you need to guarantee access to a certain amount of a resource, specify minimum limits. This technique is useful for interactive jobs that do not consume a lot of resources, but must respond quickly to external events.
- If you need to limit access to resources but shares do not provide enough control, specify maximum limits. In most cases, soft maximum limits are adequate, but hard maximums can be used for strict enforcement. Because hard maximum limits can result in wasted system resources, and they can increase paging activity when used for memory regulation, you should impose minimum limits for the other classes before imposing any hard limits.
- If less-important jobs are interfering with more-important jobs, put the less-important jobs in a lower tier. This technique ensures less-important jobs have lower priority and cannot compete for available resources while the more-important jobs are running.
- If a class cannot reach its consumption target for a resource, check whether this condition is caused by contention for another resource. If so, change the class allocation for the resource under contention.
- If processes within a class vary greatly in their behaviors or resource consumption, create more classes to gain more granular control. Also, it might be desirable to create a separate class for each important application.
- If your analysis shows the resource required by one class is dependent on the consumption of another class, reallocate your resources accordingly. For example, if the amount of resource required by ClassZ is dependent on the number of work requests that can be handled by ClassA, then ClassA must be guaranteed access to enough resources to provide what ClassZ needs.
- If one or more applications are consistently not receiving enough resources to perform adequately, your only option might be to reduce the workload on the system.

Note: You can define an adminuser for a superclass to reduce the amount of work that is required of the WLM administrator. After the top-level configuration has been tested and tuned, subsequent changes (including creating and configuring subclasses) can be made by the superclass adminusers to suit their particular needs.

System Resource Controller and Subsystems

This section contains procedures for starting and stopping, tracing, and obtaining status of the System Resource Controller (SRC) subsystems, including:

Starting the System Resource Controller

The System Resource Controller (SRC) is started during system initialization with a record for the **/usr/sbin/srcmstr** daemon in the **/etc/inittab** file. The default **/etc/inittab** file already contains such a record, so this procedure might be unnecessary. You can also start the SRC from the command line, a profile, or a shell script, but there are several reasons for starting it during initialization:

- Starting the SRC from the **/etc/inittab** file allows the **init** command to restart the SRC if it stops for any reason.
- The SRC is designed to simplify and reduce the amount of operator intervention required to control subsystems. Starting the SRC from any source other than the **/etc/inittab** file is counterproductive to that goal.
- The default **/etc/inittab** file contains a record for starting the print scheduling subsystem (**qdaemon**) with the **startsrc** command. Typical installations have other subsystems started with **startsrc**

commands in the **/etc/inittab** file as well. Because the **srcmstr** command requires the SRC be running, removing the **srcmstr** daemon from the **/etc/inittab** file causes these **startsrc** commands to fail.

See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- Reading and writing the **/etc/inittab** file requires root user authority.
- The **mkitab** command requires root user authority.
- The **srcmstr** daemon record must exist in the **/etc/inittab** file.

Procedure

Note: This procedure is necessary only if the **/etc/inittab** file does not already contain a record for the **srcmstr** daemon.

1. Make a record for the **srcmstr** daemon in the **/etc/inittab** file using the **mkitab** command. For example, to make a record identical to the one that appears in the default **/etc/inittab** file, type:

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

   The **-i fbcheck** flag ensures that the record is inserted before all subsystems records.
2. Tell the **init** command to reprocess the **/etc/inittab** file by typing:

   ```
   telinit q
   ```

   When **init** revisits the **/etc/inittab** file, it processes the newly entered record for the **srcmstr** daemon and starts the SRC.

Starting or Stopping a Subsystem, Subsystem Group, or Subserver

Use the **startsrc** command to start a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver. The **startsrc** command can be used:

- From the **/etc/inittab** file so the resource is started during system initialization
- From the command line
- With SMIT.

When you start a subsystem group, all of its subsystems are also started. When you start a subsystem, all of its subservers are also started. When you start a subserver, its parent subsystem is also started if it is not already running.

Use the **stopsrc** command to stop an SRC resource such as a subsystem, a group of subsystems, or a subserver. When you stop a subsystem, all its subservers are also stopped. However, when you stop a subserver, the state of its parent subsystem is not changed.

Both the **startsrc** and **stopsrc** commands contain flags that allow requests to be made on local or remote hosts.See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- To start or stop an SRC resource, the SRC must be running. The SRC is normally started during system initialization. The default **/etc/inittab** file, which determines what processes are started during initialization, contains a record for the **srcmstr** daemon (the SRC). To see if the SRC is running, type **ps -A** and look for a process named **srcmstr**.
- The user or process starting an SRC resource must have root user authority. The process that initializes the system (**init** command) has root user authority.
- The user or process stopping an SRC resource must have root user authority.

Starting/Stopping a Subsystem Tasks

Task	*SMIT Fast Path*	*Command or File*
Start a Subsystem	**smit startssys**	**/bin/startsrc -s** *SubsystemName* OR edit **/etc/inittab**
Stop a Subsystem	**smit stopssys**	**/bin/stopsrc -s** *SubsystemName*

Displaying the Status of a Subsystem or Subsystems

Use the **lssrc** command to display the status of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

All subsystems can return a short status report that includes which group the subsystem belongs to, whether the subsystem is active, and what its process ID (PID) is. If a subsystem does not use the signals communication method, it can be programmed to return a long status report containing additional status information.

The **lssrc** command provides flags and parameters for specifying the subsystem by name or PID, for listing all subsystems, for requesting a short or long status report, and for requesting the status of SRC resources either locally or on remote hosts.

See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Displaying the Status of Subsystems Tasks

Task	*SMIT Fast Path*	*Command or File*
Display the status of a subsystem (long format)	**smit qssys**	**lssrc -l -s** *SubsystemName*
Display the status of all subsystems	**smit lsssys**	**lssrc -a**
Display the status of all subsystems on a particular host		**lssrc -h***HostName* **-a**

Refreshing a Subsystem or Subsystem Group

Use the **refresh** command to tell a System Resource Controller (SRC) resource such as a subsystem or a group of subsystems to refresh itself.

The **refresh** command provides flags and parameters for specifying the subsystem by name or PID. You can also use it to request a subsystem or group of subsystems be refreshed, either locally or on remote hosts. See the **srcmstr** command for the configuration requirements to support remote SRC requests.

Prerequisites

- The SRC must be running. See “Starting the System Resource Controller” on page 101 for details.
- The resource you want to refresh must not use the signals communications method.
- The resource you want to refresh must be programmed to respond to the refresh request.

Refreshing a Subsystem or Subsystem Group

Task	**SMIT Fast Path**	**Command or File**
Refresh a Subsystem	**smit refresh**	**refresh -s Subsystem**

Turning On or Off Subsystem, Subsystem Group, or Subserver Tracing

Use the **traceson** command to turn on tracing of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

Use the **tracesoff** command to turn off tracing of a System Resource Controller (SRC) resource such as a subsystem, a group of subsystems, or a subserver.

The **traceson** and **traceoff** commands can be used to remotely turn on or turn off tracing on a specific host. See the **srcmstr** command for the configuration requirements for supporting remote SRC requests.

Prerequisites

- To turn the tracing of an SRC resource either on or off , the SRC must be running. See “Starting the System Resource Controller” on page 101 for details.
- The resource you want to trace must not use the signals communications method.
- The resource you want to trace must be programmed to respond to the trace request.

Turning On/Off Subsystem, Subsystem Group, or Subserver Tasks

Task	*SMIT Fast Path*	*Command or File*
Turn on Subsystem Tracing (short format)	**smit tracessyson**	**traceson -s Subsystem**
Turn on Subsystem Tracing (long format)	**smit tracessyson**	**traceson -l -s Subsystem**
Turn off Subsystem Tracing	**smit tracessysoff**	**tracesoff -s Subsystem**

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 section are:

Setting Up an Accounting System

Prerequisites

You must have root authority to complete this procedure.

Procedure

The following is an overview of the steps you must take to set up an accounting system. Refer to the commands and files noted in these steps for more specific information.

1. Use the **nulladm** command to ensure that each file has the correct access permission: read (r) and write (w) permission for the file owner and group and read (r) permission for others by typing:

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

   This provides access to the **pacct** and **wtmp** files.
2. Update the **/etc/acct/holidays** file to include the hours you designate as prime time and to reflect your holiday schedule for the year.

   Note: Comment lines can appear anywhere in the file as long as the first character in the line is an asterisk (*).

   a. To define prime time, fill in the fields on the first data line (the first line that is not a comment), using a 24-hour clock. This line consists of three 4-digit fields, in the following order:
      - Current year
      - Beginning of prime time (*hhmm*)
      - End of prime time (*hhmm*)

      Leading blanks are ignored. You can enter midnight as either 0000 or 2400.

      For example, to specify the year 2000, with prime time beginning at 8:00 a.m. and ending at 5:00 p.m., enter:

      ```
      2000  0800  1700
      ```

   b. To define the company holidays for the year on the next data line. Each line contains four fields, in the following order:
      - Day of the year
      - Month
      - Day of the month
      - Description of holiday

      The day-of-the-year field contains the number of the day on which the holiday falls and must be a number from 1 through 365 (366 on leap year). For example, February 1st is day 32. The other three fields are for information only and are treated as comments.

      A two-line example follows:

      ```
        1  Jan  1  New Year's Day
      332  Nov 28  Thanksgiving Day
      ```
3. Turn on process accounting by adding the following line to the **/etc/rc** file or by deleting the comment symbol (#) in front of the line if it exists:

   ```
   /usr/bin/su - adm -c /usr/sbin/acct/startup
   ```

   The **startup** procedure records the time that accounting was turned on and cleans up the previous day's accounting files.
4. Identify each file system you want included in disk accounting by adding the following line to the stanza for the file system in the **/etc/filesystems** file:

   ```
   account = true
   ```
5. Specify the data file to use for printer data by adding the following line to the queue stanza in the **/etc/qconfig** file:

   ```
   acctfile = /var/adm/qacct
   ```
6. As the adm user, create a **/var/adm/acct/nite**, a **/var/adm/acct/fiscal**, a and **/var/adm/acct/sum** directory to collect daily and fiscal period records:

   ```
   su - adm
   cd /var/adm/acct
   mkdir nite fiscal sum
   exit
   ```

7. Set daily accounting procedures to run automatically by editing the **/var/spool/cron/crontabs/root** file to include the **dodisk**, **ckpacct**, and **runacct** commands. For example:

```
0 2 * * 4 /usr/sbin/acct/dodisk
5 * * * * /usr/sbin/acct/ckpacct
0 4 * * 1-6 /usr/sbin/acct/runacct
             2>/var/adm/acct/nite/accterr
```

   The first line starts disk accounting at 2:00 a.m. (`0 2`) each Thursday (4). The second line starts a check of the integrity of the active data files at 5 minutes past each hour (`5 *`) every day (`*`). The third line runs most accounting procedures and processes active data files at 4:00 a.m. (`0 4`) every Monday through Saturday (`1-6`). If these times do not fit the hours your system operates, adjust your entries.

   Note: You must have root user authority to edit the **/var/spool/cron/crontabs/root** file.

8. Set the monthly accounting summary to run automatically by including the **monacct** command in the **/var/spool/cron/crontabs/root** file. For example, type:

```
15 5 1 * * /usr/sbin/acct/monacct
```

   Be sure to schedule this procedure early enough to finish the report. This example starts the procedure at 5:15 a.m. on the first day of each month.

9. To submit the edited **cron** file, type:

```
crontab /var/spool/cron/crontabs/root
```

Generating System Accounting Reports

Once accounting has been configured on the system, daily and monthly reports are generated. The **runacct** command produces the daily reports and the **monact** command produces the monthly reports.

Daily Accounting Reports

To generate a daily report, use the **runacct** command. This command summarizes data into an ASCII file named **/var/adm/acct/sum/rprtMMDD**. **MMDD** specifies the month and day the report is run. The report covers the following:

- Daily Report
- Daily Usage Report
- Daily Command Summary
- Monthly Total Command Summary
- Last Login

Daily Report: The first line of the Daily Report begins with the start and finish times for the data collected in the report, a list of system-level events including any existing shutdowns, reboots, and run-level changes. The total duration is also listed indicating the total number of minutes included within the accounting period (usually 1440 minutes, if the report is run every 24 hours). The report contains the following information:

LINE	Console, tty, or pty In use
MINUTES	Total number of minutes the line was in use
PERCENT	Percentage of time in the accounting period that the line was in use
# SESS	Number of new login sessions started
# ON	Same as **# SESS**
# OFF	Number of logouts plus interrupts made on the line

Daily Usage Report: The Daily Usage Report is a summarized report of system usage per user ID during the accounting period. Some fields are divided into prime and non-prime time, as defined by the accounting administrator in the **/usr/lib/acct/holidays** directory. The report contains the following

information:

UID	User ID
LOGIN NAME	User name
CPU (PRIME/NPRIME)	Total CPU time for all of the user's processes in minutes
KCORE (PRIME/NPRIME)	Total memory used by running processes, in kilobyte-minutes
CONNECT (PRIME/NPRIME)	Total connect time (how long the user was logged in) in minutes
DISK BLOCKS	Average total amount of disk space used by the user on all filesystems for which accounting is enabled
FEES	Total fees entered with **chargefee** command
# OF PROCS	Total number of processes belonging to this user
# OF SESS	Number of distinct login sessions for this user
# DISK SAMPLES	Number of times disk samples were run during the accounting period. If no DISK BLOCKS are owned the value will be zero

Daily Command Summary: The Daily Command Summary report shows each command executed during the accounting period, with one line per each unique command name. The table is sorted by TOTAL KCOREMIN (described below), with the first line including the total information for all commands. The data listed for each command is cumulative for all executions of the command during the accounting period. The columns in this table include the following information:

COMMAND NAME	Command that was executed
NUMBER CMDS	Number of times the command executed
TOTAL KCOREMIN	Total memory used by running the command, in kilobyte-minutes
TOTAL CPU-MIN	Total CPU time used by the command in minutes
TOTAL REAL-MIN	Total real time elapsed for the command in minutes
MEAN SIZE-K	Mean size of memory used by the command per CPU minute
MEAN CPU-MIN	Mean numbr of CPU minutes per execution of the command
HOG FACTOR	Measurement of how much the command hogs the CPU while it is active. It is the ratio of **TOTAL CPU-MIN** over **TOTAL REAL-MIN**
CHARS TRNSFD	Number of characters transferred by the command with system reads and writes
BLOCKS READ	Number of physical block reads and writes performed by the command

Monthly Total Command Summary:

The Monthly Total Command Summary , created by the **monacct** command, provides information about all commands executed since the previous monthly report. The fields and information mean the same as those in the Daily Command Summary.

Last Login: The Last Login report displays two fields for each user ID. The first field is YY-MM-DD and indicates the most recent login for the specified user. The second field is the name of the user account. A date field of 00-00-00 indicates that the user ID has never logged in.

Fiscal Accounting Reports

The Fiscal Accounting Reports generally collected monthly by using the **monacct** command. The report is stored in **/var/adm/acct/fiscal/fiscrptMM** where **MM** is the month that the **monacct** command was executed. This report includes information similar to the daily reports summarized for the entire month.

Generating Reports on System Activity

To generate a report on system activity, use the **prtacct** command. This command reads the information in a total accounting file (**tacct** file format) and produces formatted output. Total accounting files include the daily reports on connect time, process time, disk usage, and printer usage.

Prerequisites

The **prtacct** command requires an input file in the **tacct** file format. This implies that you have an accounting system set up and running or that you have run the accounting system in the past. See "Setting Up an Accounting System" on page 104 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 104 for guidelines

Procedure

The purpose of the **sa** command is to summarize process accounting information and to display or store that information. The simplest use of the command displays a list of statistics about every process that has run during the life of the **pacct** file being read. To produce such a list, type:

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

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

```
/usr/sbin/sa -s
```

The **sa** command offers many additional flags that specify how the accounting information is processed and displayed. See the **sa** command description for more information.

Starting the runacct Command

Prerequisites

1. You must have the accounting system installed.
2. You must have root user or adm group authority.

Notes:

1. If you call the **runacct** command with no parameters, the command assumes that this is the first time that the command has been run today. Therefore, you need to include the *mmdd* parameter when you restart the **runacct** program, so that the month and day are correct. If you do not specify a state, the **runacct** program reads the **/var/adm/acct/nite/statefile** file to determine the entry point for processing. To override the **/var/adm/acct/nite/statefile** file, specify the desired state on the command line.
2. When you perform the following task, you might need to use the full path name **/usr/sbin/acct/runacct** rather than the simple command name, **runacct**.

Procedure

To start the **runacct** command, type the following:

```
nohup runacct 2> \
/var/adm/acct/nite/accterr &
```

This entry causes the command to ignore all **INTR** and **QUIT** signals while it performs background processing. It redirects all standard error output to the **/var/adm/acct/nite/accterr** file.

Restarting the runacct Command

Prerequisites

1. You must have the accounting system installed.
2. You must have root user or adm group authority.

Note: The most common reason why the **runacct** command can fail are because:

- The system goes down.
- The **/usr** file system runs out of space.
- The **/var/adm/wtmp** file has records with inconsistent date stamps.

Procedure

If the **runacct** command is unsuccessful, do the following:

1. Check the **/var/adm/acct/nite/active** *mmdd* file for error messages.
2. If both the active file and lock files exist in **acct/nite**, check the **accterr** file, where error messages are redirected when the **cron** daemon calls the **runacct** command.
3. Perform any actions needed to eliminate errors.
4. Restart the **runacct** command.
5. To restart the **runacct** command for a specific date, type the following:

   ```
   nohup runacct 0601 2>> \
   /var/adm/acct/nite/accterr &
   ```

   This restarts the **runacct** program for June 1 (`0601`). The **runacct** program reads the **/var/adm/acct/nite/statefile** file to find out with which state to begin. All standard error output is appended to the **/var/adm/acct/nite/accterr** file.
6. To restart the **runacct** program at a specified state, for example, the MERGE state, type the following:

   ```
   nohup runacct 0601 MERGE 2>> \
   /var/adm/acct/nite/accterr &
   ```

Showing System Activity

You can display formatted information about system activity with the **sar** command.

Prerequisites

To display system activity statistics, the **sadc** command must be running.

Note: The typical method of running the **sadc** command is to place an entry for the **sa1** command in the root **crontab** file. The **sa1** command is a shell-procedure variant of the **sadc** command designed to work with the **cron** daemon.

Procedure

To display basic system-activity information, type:

```
sar 2 6
```

where the first number is the number of seconds between sampling intervals and the second number is the number of intervals to display. The output of this command looks something like this:

```
    arthurd 2 3 000166021000    05/28/92

14:03:40    %usr    %sys    %wio   %idle
14:03:42       4       9       0      88
14:03:43       1      10       0      89
14:03:44       1      11       0      88
14:03:45       1      11       0      88
14:03:46       3       9       0      88
14:03:47       2      10       0      88

Average        2      10       0      88
```

The **sar** command also offers a number of flags for displaying an extensive array of system statistics. To see all available statistics, use the **-A** flag. For a list of the available statistics and the flags for displaying them, see the **sar** command.

Note: To have a daily system activity report written to **/var/adm/sa/sa***dd*, include an entry in the root **crontab** file for the **sa2** command. The **sa2** command is a shell procedure variant for the **sar** command designed to work with the **cron** daemon.

Showing System Activity While Running a Command

You can use the **time** and **timex** commands to display formatted information about system activity while a particular command is running.

Prerequisites

The **-o** and **-p** flags of the **timex** command require that system accounting be turned on.

Procedure

- To display the elapsed time, user time, and system execution time for a particular command, type:

  ```
  time CommandName
  ```

  OR

  ```
  timex CommandName
  ```

- To display the total system activity (all the data items reported by the **sar** command) during the execution of a particular command, type:

  ```
  timex -s CommandName
  ```

The **timex** command has two additional flags. The **-o** flag reports the total number of blocks read or written by the command and all of its children. The **-p** flag lists all of the process accounting records for a command and all of its children.

Showing Process Time

You can display formatted reports about the process time of active processes with the **ps** command or of finished processes with the **acctcom** command.

Prerequisites

The **acctcom** command reads input in the total accounting record form (**acct** file format). This implies that you have process accounting turned on or that you have run process accounting in the past. See “Setting Up an Accounting System” on page 104 for guidelines.

Display the Process Time of Active Processes

The **ps** command offers a number of flags to tailor the information displayed. To produce a full list of all active processes except kernel processes, type:

```
ps -ef
```

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

```
ps -al
```

Both of these usages display a number of columns for each process, including the current CPU time for the process in minutes and seconds.

Display the Process Time of Finished Processes

The process accounting functions are turned on with the **startup** command, which is typically started at system initialization with a call in the **/etc/rc** file. When the process accounting functions are running, a record is written to **/var/adm/pacct** (a total accounting record file) for every finished process that includes the start and stop time for the process. You can display the process time information from a **pacct** file with the **acctcom** command. This command has a number of flags that allow flexibility in specifying which processes to display.

For example, to see all processes that ran for a minimum number of CPU seconds or longer, use the **-O** flag, type:

```
acctcom -O 2
```

This displays records for every process that ran for at least 2 seconds. If you do not specify an input file, the **acctcom** command reads input from the **/var/adm/pacct** directory.

Showing CPU Usage

You can display formatted reports about the CPU usage by process or by user with a combination of the **acctprc1**, **acctprc2**, and **prtacct** commands.

Prerequisites

The **acctprc1** command requires input in the total accounting record form (**acct** file format). This implies that you have process accounting turned on or that you have run process accounting in the past. See “Setting Up an Accounting System” on page 104 for guidelines.

Show CPU Usage for Each Process

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

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

This information will be useful in some situations, but you might also want to summarize the CPU usage by user. The output from this command is used in the next procedure to produce that summary.

Show CPU Usage for Each User

1. Produce an output file of CPU usage by process by typing:

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

   The **/var/adm/pacct** file is the default output for process accounting records. You might want to specify an archive **pacct** file instead.
2. Produce a binary total accounting record file from the output of the previous step by typing:

   ```
   acctprc2 <out.file >/var/adm/acct/nite/daytacct
   ```

   Note: The **daytacct** file is merged with other total accounting records by the **acctmerg** command to produce the daily summary record, **/var/adm/acct/sum/tacct**.
3. Display a formatted report of CPU usage summarized by user by typing:

   ```
   prtacct </var/adm/acct/nite/daytacct
   ```

Showing Connect Time Usage

You can display the connect time of all users, of individual users, and by individual login with the **ac** command.

Prerequisites

The **ac** command extracts login information from the **/var/adm/wtmp** file, so this file must exist. If the file has not been created, the following error message is returned:

```
No /var/adm/wtmp
```

If the file becomes too full, additional **wtmp** files are created; you can display connect-time information from these files by specifying them with the **-w** flag.

Procedure

- To display the total connect time for all users, type:

  ```
  /usr/sbin/acct/ac
  ```

  This command displays a single decimal number that is the sum total connect time, in minutes, for all users who have logged in during the life of the current **wtmp** file.
- To display the total connect time for one or more particular users, type:

  ```
  /usr/sbin/acct/ac User1 User2 ...
  ```

  This command displays a single decimal number that is the sum total connect time, in minutes, for the user or users you specified for any logins during the life of the current **wtmp** file.
- To display the connect time by individual user plus the total connect time, type:

  ```
  /usr/sbin/acct/ac -p User1 User2 ...
  ```

  This command displays as a decimal number for each user specified equal to the total connect time, in minutes, for that user during the life of the current **wtmp** file. It also displays a decimal number that is the sum total connect time for all the users specified. If no user is specified in the command, the list includes all users who have logged in during the life of the **wtmp** file.

Showing Disk Space Utilization

You can display disk space utilization information with the **acctmerg** command.

Prerequisites

To display disk space utilization information, the **acctmerg** command requires input from a **dacct** file (disk accounting). The collection of disk-usage accounting records is performed by the **dodisk** command. Placing an entry for the **dodisk** command in a **crontabs** file is part of the procedure described in “Setting Up an Accounting System” on page 104.

Procedure

To display disk space utilization information, type:

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

This command displays disk accounting records, which include the number of 1 KB blocks utilized by each user.

Note: The **acctmerg** command always reads from standard input and can read up to nine additional files. If you are not piping input to the command, you must redirect input from one file; the rest of the files can be specified without redirection.

Showing Printer Usage

You can display printer or plotter usage accounting records with the **pac** command.

Prerequisites

- To collect printer usage information, you must have an accounting system set up and running. See “Setting Up an Accounting System” on page 104 for guidelines.
- The printer or plotter for which you want accounting records must have an `acctfile=` clause in the printer stanza of the **/etc/qconfig** file. The file specified in the `acctfile=` clause must grant read and write permissions to the root user or printq group.
- If the **-s** flag of the **pac** command is specified, the command rewrites the summary file name by appending **_sum** to the path name specified by the `acctfile=` clause in the **/etc/qconfig** file. This file must exist and grant read and write permissions to the root user or printq group.

Procedure

- To display printer usage information for all users of a particular printer, type:

  ```
  /usr/sbin/pac -PPrinter
  ```

  If you do not specify a printer, the default printer is named by the **PRINTER** environment variable. If the **PRINTER** variable is not defined, the default is **lp0**.
- To display printer usage information for particular users of a particular printer, type:

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

The **pac** command offers other flags for controlling what information gets displayed.

Fixing tacct Errors

If you are using the accounting system to charge user for system resources, the integrity of the **/var/adm/acct/sum/tacct** file is quite important. Occasionally, mysterious **tacct** records appear that contain negative numbers, duplicate user numbers, or a user number of 65,535.

Prerequisites

You must have root user or adm group authority.

Patch a tacct File

1. Move to the **/var/adm/acct/sum** directory by typing:

   ```
   cd /var/adm/acct/sum
   ```
2. Use the **prtacct** command to check the total accounting file, **tacctprev**, by typing:

   ```
   prtacct tacctprev
   ```

   The **prtacct** command formats and displays the **tacctprev** file so that you can check connect time, process time, disk usage, and printer usage.
3. If the **tacctprev** file looks correct, change the latest **tacct .***mmdd* file from a binary file to an ASCII file. In the following example, the **acctmerg** command converts the **tacct.***mmdd* file to an ASCII file named `tacct.new`:

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

   > **Note:** The **acctmerg** command with the **-a** flag also produces ASCII output. The **-v** flag produces more precise notation for floating-point numbers.

   The **acctmerg** command is used to merge the intermediate accounting record reports into a cumulative total report (**tacct**). This cumulative total is the source from which the **monacct** command produces the ASCII monthly summary report. Since the **monacct** command procedure removes all the **tacct.***mmdd* files, you recreate the **tacct** file by merging these files.

4. Edit the **tacct.new** file to remove the bad records and write duplicate user number records to another file by typing:

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

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

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

Fixing wtmp Errors

The **/var/adm/wtmp**, or ″who temp″ file, might cause problems in the day-to-day operation of the accounting system. When the date is changed and the system is in multiuser mode, date change records are written to the **/var/adm/wtmp** file. When a date change is encountered, the **wtmpfix** command adjusts the time stamps in the **wtmp** records. Some combinations of date changes and system restarts may slip past the **wtmpfix** command and cause the **acctcon1** command to fail and the **runacct** command to send mail to the **root** and **adm** accounts listing incorrect dates.

Prerequisites

You must have root user or adm group authority.

Procedure

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

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

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

   ```
   fwtmp < wtmp.mmdd > wtmp.new
   ```

   The **fwtmp** command converts **wtmp** from binary to ASCII.

3. Edit the ASCII **wtmp.new** file to delete damaged records or all records from the beginning of the file up to the needed date change by typing:

   ```
   vi wtmp.new
   ```

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

   ```
   fwtmp -ic < wtmp.new > wtmp.mmdd
   ```

5. If the **wtmp** file is beyond repair, use the **nulladm** command to create an empty **wtmp** file. This prevents any charges in the connect time.

   ```
   nulladm wtmp
   ```

   The **nulladm** command creates the file specified with read and write permissions for the file owner and group, and read permissions for other users. It ensures that the file owner and group are **adm**.

Fixing General Accounting Problems

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

This section describes how to fix general accounting problems:

- “Fixing Incorrect File Permissions” on page 115
- “Fixing Errors” on page 115
- “Fixing Errors Encountered When Running the runacct Command” on page 116
- “Updating an Out-of-Date Holidays File” on page 118

Prerequisites

You must have root user or adm group authority.

Fixing Incorrect File Permissions

To use the accounting system, file ownership and permissions must be correct. The **adm** administrative account owns the accounting command and scripts, except for **/var/adm/acct/accton** which is owned by root.

1. To check file permissions using the **ls** command, type:

   ```
   ls -l /var/adm/acct

   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/fiscal
   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/nite
   -rws--x--- 1 adm adm 14628 Mar 19 08:11 /var/adm/acct/sum
   ```

2. Adjust file permissions with the **chown** command, if necessary. The permissions are 755 (all permissions for owner and read and execute permissions for all others). Also, the directory itself should be write-protected from others. For example:

   a. Move to the **/var/adm/acct** directory by typing:

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

   b. Change the ownership for the **sum**, **nite**, and **fiscal** directories to **adm** group authority by typing:

      ```
      chown adm sum/* nite/* fiscal/*
      ```

      To prevent tampering by users trying to avoid charges, deny write permission for others on these files. Change the **accton** command group owner to **adm**, and permissions to 710, that is, no permissions for others. Processes owned by **adm** can execute the **accton** command, but ordinary users can not.

3. The **/var/adm/wtmp** file must also be owned by **adm**. If **/var/adm/wtmp** is owned by root, you will see the following message during startup:

   ```
   /var/adm/acct/startup: /var/adm/wtmp: Permission denied
   ```

   To correct the ownership of **/var/adm/wtmp**, change ownership to the **adm** group by typing the following command:

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

Fixing Errors

Processing the **/var/adm/wtmp** file night produce some warnings mailed to root. The **wtmp** file contains information collected by **/etc/init** and **/bin/login** and is used by accounting scripts primarily for calculating connect time (the length of time a user is logged in). Unfortunately, date changes confuse the program that processes the **wtmp** file. As a result, the **runacct** command sends mail to root and adm complaining of any errors after a date change since the last time accounting was run.

1. Determine if you received any errors.

   The **acctcon1** command outputs error messages that are mailed to adm and root by the **runacct** command. For example, if the **acctcon1** command stumbles after a date change and fails to collect connect times, adm might get mail like the following mail message:

   ```
   Mon Jan 6 11:58:40 CST 1992
   acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
   new: Mon Jan 6 11:57:59 1992
   acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
   new: Mon Jan 6 11:57:59 1992
   acctcon1: bad times: old: Tue Jan 7 00:57:14 1992
   new: Mon Jan 6 11:57:59 1992
   ```

2. Adjust the **wtmp** file by typing:

   ```
   /usr/sbin/acct/wtmpfix wtmp
   ```

   The **wtmpfix** command examines the **wtmp** file for date and time-stamp inconsistencies and corrects problems that could make **acctcon1** fail. However, some date changes slip by **wtmpfix**. See “Fixing wtmp Errors” on page 114.

3. Run accounting right before shutdown or immediately after startup.

   Using the **runacct** command at these times minimizes the number of entries with bad times. The **runacct** command continues to send mail to the root and adm accounts, until you edit the **runacct** script, find the `WTMPFIX` section, and comment out the line where the file log gets mailed to the **root** and **adm** accounts.

Fixing Errors Encountered When Running the runacct Command:

The **runacct** command processes files that are often very large. The procedure involves several passes through certain files and consumes considerable system resources while it is taking place. That is why the **runacct** command is normally run early in the morning when it can take over the machine and not disturb anyone.

The **runacct** command is a scrip divided into different stages. The stages allow you to restart the command where it stopped, without having to rerun the entire script.

When the **runacct** encounters problems, it sends error messages to different destinations depending on where the error occurred. Usually it sends a date and a message to the console directing you to look in the **active***MMDD* file (such as **active0621** for June 21st) which is in the **/usr/adm/acct/nite** directory. When the **runacct** command aborts, it moves the entire **active** file to **active***MMDD* and appends a message describing the problem.

1. Review the following error message tables for errors you have encountered when running the **runacct** command.

Notes:

1. The abbreviation *MMDD* stands for the month and day, such as 0102 for January 2. For example, a fatal error during the CONNECT1 process on January 2 creates the file **active0102** containing the error message.
2. The abbreviation ″SE message″ stands for the standard error message such as:

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

Preliminary State and Error Messages from the runnacct Command

State	Command	Fatal?	Error Message	Destinations
pre	**runacct**	yes	`* 2 CRONS or ACCT PROBLEMS * ERROR: locks found, run aborted`	console, mail, active
pre	**runacct**	yes	`runacct: Insufficient space in /usr ( nnn blks); Terminating procedure`	console, mail, active
pre	**runacct**	yes	`SE message; ERROR: acctg already run for 'date': check lastdate`	console, mail, active*MMDD*
pre	**runacct**	no	`* SYSTEM ACCOUNTING STARTED *`	console
pre	**runacct**	no	`restarting acctg for 'date' at STATE`	console active, console

Preliminary State and Error Messages from the runnacct Command

State	Command	Fatal?	Error Message	Destinations
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

States and Error Messages from the runacct Command

State	Command	Fatal?	Error Message	Destinations
MERGEACCT	**acctmerg**	no	`WARNING: recreating sum/tacct`	active
MERGEACCT	**acctmerg**	no	`updated sum/tacct`	active
CMS	**runacct**	no	`WARNING: recreating sum/cms`	active
CMS	**acctcms**	no	`command summaries complete`	active
CLEANUP	**runacct**	no	`system accounting completed at 'date'`	active
CLEANUP	**runacct**	no	`*SYSTEM ACCOUNTING COMPLETED*`	console
<wrong>	**runacct**	yes	`SE message; ERROR: invalid state, check STATE`	console, mail, active*MMDD*

Note: The label `<wrong>` in the previous table does not represent a state, but rather a state other than the correct state that was written in the state file **/usr/adm/acct/nite/statefile**.

Summary of Message Destinations

Destination	Description
console	The **/dev/console** device
mail	Message mailed to **root** and **adm** accounts
active	The **/usr/adm/acct/nite/active** file
activeMMDD	The **/usr/adm/acct/nite/active***MMDD* file
wtmperrMMDD	The **/usr/adm/acct/nite/wtmperror***MMDD* file
STATE	Current state in **/usr/adm/acct/nite/statefile** file
fd2log	Any other error messages

Updating an Out-of-Date Holidays File

The **acctcon1** command (started from the **runacct** command) sends mail to the **root** and **adm** accounts when the **/usr/lib/acct/holidays** file gets out of date. The holidays file is out of date after the last holiday listed has passed or the year has changed.

Update the out-of-date holidays file by editing the **/var/adm/acct/holidays** file to differentiate between prime and nonprime time.

Prime time is assumed to be the period when your system is most active, such as workdays. Saturdays and Sundays are always nonprime times for the accounting system, as are any holidays that you list.

The holidays file contains three types of entries: comments, the year and prime-time period, and a list of holidays as in the following example:

```
* Prime/Non-Prime Time Table for Accounting System
*
*   Curr       Prime             Non-Prime
*   Year       Start             Start
    1992       0830              1700
*
*   Day of     Calendar          Company
```

```
*   Year       Date             Holiday
*
*   1          Jan 1            New Year's Day
*   20         Jan 20           Martin Luther King Day
*   46         Feb 15           President's Day
*   143        May 28           Memorial Day
*   186        Jul 3            4th of July
*   248        Sep 7            Labor Day
*   329        Nov 24           Thanksgiving
*   330        Nov 25           Friday after
*   359        Dec 24           Christmas Eve
*   360        Dec 25           Christmas Day
*   361        Dec 26           Day after Christmas
```

The first noncomment line must specify the current year (as four digits) and the beginning and end of prime time, also as four digits each. The concept of prime and nonprime time only affects the way that the accounting programs process the accounting records.

If the list of holidays is too long, the **acctcon1** command generates an error, and you will need to shorten your list. You are safe with 20 or fewer holidays. If you want to add more holidays, just edit the holidays file each month.

Chapter 6. Documentation Library Service Tasks

The Documentation Library Service allows you to read, search, and print online HTML or PDF 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.

You can register additional 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” on page 128.

By default, the library’s components are installed with the base operating system. To use the library service, it must be configured. You can configure a computer to be a documentation server and install documents on that computer; or you can configure a computer to be a client that gets all of its documents from a documentation server. If the computer is to be a documentation server, the search engine and documentation must also be manually installed.

The library service must be fully configured because it is the library service for the operating system manuals and the Web-based System Manager documentation. Even if you do not need the operating system manuals, you should still configure the documentation library service because it is expected that other applications may use it as the library function for their own online documentation. For instructions on how to install and configure the documentation library service, see Installing and Configuring the Documentation Library Service and Online Documentation in *AIX 5L Version 5.2 Installation Guide and Reference*.

The rest of this chapter contains information on changing the configuration of the library service after installation, adding or removing your own documents from the library, and problem determination.

Changing the Configuration of the Documentation Library Service

This section provides information about changing the configuration of the Documentation Library Service after it has been initially installed and configured. For instructions on how to set up the library service for the first time on a computer, see Installing the Online Documentation in *AIX 5L Version 5.2 Installation Guide and Reference*.

Viewing the Current Configuration

This process shows the default system documentation server settings. If users have specified different settings in the **.profile** file in their home directories, they are not affected by the default settings.

You can view the configuration of the documentation library service by using either of the system management tools (Web-based System Manager or SMIT).

Using Web-based System Manager

1. Change to the root user.
2. At the command line, type: `wsm`, then double-click on **System Environment**.
3. In the System Environments window, double-click on **Settings**.
4. When the contents are displayed, double-click on the **Default Browser** icon. This shows the current command that is used to launch the default browser that displays the library application.

   Double-click on the **Documentation Server** icon to view the current settings for the documentation server for this computer.

Using SMIT

1. Change to the root user.
2. At the command line, type: `smit web_configure`
3. From the Web Configuration menu, select **Show Documentation and Search Server** to display the current configuration information.

Changing the Default Remote Documentation Library Service of a Client Computer

This configuration process changes the default system documentation server. If users have specified a different server in their own **.profile** file in their home directories, they will not be affected by the default settings.

You can view the configuration of the documentation library service by using either of the system management tools (Web-based System Manager or SMIT).

Using Web-based System Manager

1. Change to the root user.
2. At the command line, type: `wsm`, then double-click on **System Environment**.

   This opens the **System Environments** container.
3. In the System Environments window, double-click on the **Settings** icon to open it, then double-click on **Documentation Server**.
4. Click on the **Remote server host name** radio button, then type the name of the documentation server computer in the field to the right. This is the server computer that contains the documents that you want this client computer to be able to access and search.
5. In the **Server port** field, type the port number the web server software is using. The most commonly used port is 80. Your client computer will now be reconfigured to use the new server.

Using SMIT

1. Change to the root user.
2. On a command line, type: `smit web_configure`
3. From the web configuration screen, select **Change Documentation and Search Server**. From the List menu, select **Remote computer**.
4. In **NAME of remote documentation server**, type the name or IP address of the new server and the appropriate port number. The reconfiguration is complete when the output window shows the message `Documentation server configuration completed.`

Selecting the Documentation Search Server for a Single User

All users on a computer do not have to use the same documentation server. The system administrator sets the default server for users, but users can choose to use a different server. There are two ways users can specify the documentation server they want to use:

- "Changing the Personal Default Documentation Server" on page 123
- "Manually Going to a Documentation Server" on page 123

Changing the Personal Default Documentation Server

A user's default documentation server is the documentation server that is used when he or she starts the Documentation Library Service. System administrators set up a default server for all users logged into a system. A user who does not want to use the default documentation server can specify a different personal default documentation server.

To specify their own personal default documentation server, users can do the following:

1. Insert the following two lines in the **.profile** file in their home directory:

   ```
   export DOCUMENT_SERVER_MACHINE_NAME=servername
   export DOCUMENT_SERVER_PORT=portnumber
   ```

2. Replace *servername* with the name of the documentation search server computer they want to use.
3. Replace *portnumber* with the number of the port that the web server on the server uses. In most cases this will be 80. An exception is the Lite NetQuestion web server, which **must** use port 49213.
4. Log out, then log back in to activate the changes.

Once these two lines are placed in the **.profile** file in their home directory, changes that the system administrator makes to the system-wide default settings do not affect these users. If these users want to resume using the system-wide default server, they can remove the two lines inserted in step 1 from their profile, log out, then log back in.

Manually Going to a Documentation Server

When users do not want to change their default documentation server but want to use the documents on another documentation server, they can type the following into the URL location field of their 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 **must** use port 49213.)

In the following example, if a user wants to search the documents on a document server named `hinson`, and the web server on `hinson` uses the standard port 80, the user can enter the following URL:

```
http://hinson/cgi-bin/ds_form
```

A library application would open in the user's browser to display the documents registered on the server `hinson`. Once the library application from a document server is displayed in the user's browser, the user can create a bookmark that goes back to the server. The system administrator of a web server can also create a web page that contains links to all the different documentation servers in an organization.

Converting a Client System to a Documentation Server System

In this case, you have a client computer that is using a remote documentation server to access documents. You want to convert this client computer to be a documentation server so that the documents stored on this computer can be read and searched by the users on this computer or by remote users.

See the Installing and Configuring the Documentation Library Service and Installing Documentation in *AIX 5L Version 5.2 Installation Guide and Reference* for instructions for installing and configuring a documentation service. Choose the procedures that configure a system as a documentation server.

Disabling or Uninstalling the Documentation Library Service

Use one of the following procedures:

- "Temporarily Disabling a Server" on page 124
- "Permanently Uninstalling a Server" on page 124

Temporarily Disabling a Server

There are several different techniques:

- On the documentation server, turn off the web server software or turn off the web server access permissions for all or some users.

  If you are using the Lite NetQuestion web server software, it is automatically restarted each time you reboot the computer. To turn off the Lite NetQuestion web server until the next reboot, kill the **httpdlite** process. To prevent the web server software from being automatically restarted each time the computer reboots, edit the **/etc/inittab** file and remove or comment out the following line:

  ```
  httpdlite:2:once:/usr/IMNSearch/httpdlite -r \
  /etc/IMNSearch/httpdlite/httpdlite.conf >/dev/console 2>&1
  ```

  To restore automatic startup of the lite server, reinsert or uncomment the same line in **/etc/inittab**.

  To manually start the Lite NetQuestion server, type the following command (there is a single space before and after the **-r** flag):

  ```
  /usr/IMNSearch/httpdlite/httpdlite -r /etc/IMNSearch/httpdlite/httpdlite.conf
  ```

- To disable the library service but leave the web server functioning, go to the CGI directory of the web server. Find the file names **ds_form**, **ds_rslt**, and **ds_print**. Turn off these files' execution permissions. This turns off access to all the documentation library service functions. An error message is displayed whenever users try to access the library service on this documentation server.
- To disable the searching of a specific index without removing the documents or index from the documentation sever, unregister the index.

  Note: To re-register the index, you must record the index registry information before you remove it.

  To delete an index:

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

     ```
     /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -l -x index_name
     ```

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

     ```
     /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -d -x index_name
     ```

  If you ever want to re-register this same index, you must complete the following steps:

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

     ```
     /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -c -x index_name -sp \
      document path -ti "title"
     ```

     where you insert the index name, document path, and title values you recorded previously.

Permanently Uninstalling a Server

If you are sure you want to permanently remove the documentation library service functions, do the following:

Note: In each of the following steps make sure you uninstall using SMIT instead of deleting software. Deleting does not correctly clean up the system.

1. Uninstall the documentation library service package (*bos.docsearch*). If you want this computer to be a client of another search server, leave the Docsearch Client software installed and just uninstall the Docsearch Server component.
2. Uninstall the documentation service search engine (IMNSearch package). Uninstall both **IMNSearch.bld** (**NetQuestion Index Buildtime**), and **IMNSearch.rte** (**NetQuestion Search Runtime**).
3. Uninstall the web server software if it is not being used for some other purpose.

Note: If you are using the Lite NetQuestion web server software, you can remove it by uninstalling the fileset **IMNSearch.rte.httpdlite** (**NetQuestion Local HTTP Daemon**).

4. Uninstall the documentation and indexes.

   Note: The operating system documents can be read directly from the documentation CDs by opening the readme file in the top directory of the CDs. However, the search functions will not work.

5. Unregister any indexes that were not automatically unregistered during the uninstall process. This will included any indexes that you manually registered.

To unregister an index:

1. Login as the root user or a search administrator.
2. At the command line, type the following:

   `rm -r /usr/docsearch/indexes/`*`index name`*

   where *index name* is the name of the index you want to remove.

All of the documentation server functions should now be disabled. If the users of this computer were using this computer as their documentation server, start SMIT and change the name of the default documentation server to another computer. See “Changing the Default Remote Documentation Library Service of a Client Computer” on page 122.

Converting a Standalone Documentation Server into a Public Documentation Remote Server

The difference between a stand alone documentation server and a public remote server is that the remote server allows people on other machines to access and search the documents stored on the remote server. After a standalone server is connected to a network, modify the web server software's security configuration controls to allow users on other computers to access the documents on this computer. Consult the web server documentation for instructions on how to alter these access permissions.

Note: If you are using the Lite NetQuestion web server software for your standalone documentation server, you must replace the lite server with a more full-functioned web server software package that can serve remote users. The lite web server can only serve local users. After you install the new server you must reconfigure the documentation service to use the new server. For more instructions on reconfiguration, see “Changing the Web Server Software on A Documentation Server” on page 126.

Changing the Default Browser

This procedure changes the default browser that is used by applications that use the **defaultbrowser** command to open a browser window. The default browser is the browser that is launched when users use the **docsearch** command or the Documentation Library icon on the Help subpanel in the CDE desktop. You can change the default browser by using either of the system management tools, Web-based System Manager (see “Using Web-based System Manager”) or SMIT (see “Using SMIT” on page 126).

Using Web-based System Manager

1. Change to the root user on the client computer.
2. On a command line, type: `wsm`, then double-click on **System Environment**.

   to open the **System Environments** container.
3. In the System Environments window, double-click on the **Settings** icon to open it.
4. In **Settings**, double-click on the **Default Browser** icon.
5. In the Browser command field, type the command that launches the browser that you want to be the default browser for all users on this computer. Include any flags that are required when a URL is included in the command. For example, if you type `wonderbrowser -u http://www.ibm.com` at a command line to open your wonderbrowser with the www.ibm.com page open inside, type `wonderbrowser -u` in this field. Many browsers (for example, Netscape) do not require a flag.

6. Click **OK**. You can now close Web-based System Manager. The browser change will take effect the next time users log back into the computer.

Using SMIT

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

   ```
   smit web_configure
   ```

3. From the `Web Configuration` screen, select **Change/Show Default Browser**. On the next screen, type in the field the command that launches your new web browser. Include any flags that are required when a URL is included in the command. For example, if you type:

   ```
   wonderbrowser -u http://www.ibm.com
   ```

   to open your wonderbrowser with the www.ibm.com page open inside, you would type `wonderbrowser -u` in the field. Many browsers (for example, Netscape) do not require a flag. The browser change will take effect the next time users log back into the computer.

Changing the Web Server Software on A Documentation Server

Use the following procedure if you have already configured a documentation server and you now want to change the web server software that it is using.

1. Uninstall the current web server.
2. Install the new web server. For instructions see Install the Web Server Software in the *AIX 5L Version 5.2 Installation Guide and Reference*.
3. Configure and start your new web server software. Consult the documentation that came with your web server software and configure and start your web server software. Write down the full pathnames of the web server directories where the server starts looking for HTML documents and CGI programs. If you are going to use the Lite NetQuestion web server or the IBM HTTP Webserver, and you installed them in their default location, you can skip this step. Also, some web servers might not automatically create these directories. If not, you must create them before you continue.

   If your computer is going to serve documents to remote users, you must also configure your web server software to allow access from the users and remote computers that are using this computer as their documentation search server.

   Note: If you are using the Lite NetQuestion web server software you do not need to do this step because the lite server can only be used for standalone documents services. It does not support access by remote users.
4. Reconfigure the documentation library service to use the new web server by using either of the system management tools, Web-based System Manager (see “Using Web-based System Manager”) or SMIT (see “Using SMIT” on page 127).

Using Web-based System Manager

1. Change to the root user.
2. On the command line, type: `wsm`, then double-click on **System Environments**.
3. In the System Environments window, double-click on the **Settings** icon to open it.
4. Next, double-click on the **Documentation Server** icon. In this dialog, the **This computer server** radio button is already selected.
5. To the right of the heading **Location of documents and CGI programs**, select your new web server software. If the name of your webserver software is not listed, select **Other**.

   Note: If your web server software is listed by name, but you installed it in a non-default location on your system, or if you set up the web servers to use non-standard locations for their cgi-bin or HTML directories, you must select **Other**.
6. If you selected **Other**, type in the full pathname of the CGI and Documents directories. If you selected one of the default web server packages, skip to the next step.

7. In the **Server port** field, type the port number the web server software is using. The standard default port is 80. An exception is the Lite NetQuestion server, which must use port 49213.
8. Click **OK**. The documentation service on this computer is now reconfigured to use the new webserver software. Any users who were logged in when configuration was completed must log out, and then log back in to reactivate the library service.

Using SMIT

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

   ```
   smit web_configure
   ```
3. From the `Web Configuration` screen, select **Change Documentation and Search Server**.
4. In the `Documentation and Search Server` dialog, select **local - this computer** for server location. From the `Web Server Software` screen, select **List**, then choose the web server software you are using.
5. Enter the full pathnames of the directories and choose the appropriate port number. The standard default port is 80. An exception is the Lite NetQuestion server, which must use port 49213. SMIT now configures your system. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service.

Changing the Documentation Language

By default, if a user opens the library using the **docsearch** command, the **Documentation Library** icon in the Common Desktop Environment, or the **Base Library** icon, the library application displays in the same language as the current locale of the user's client computer. However, there may be reasons that users want to see the documentation in a language other than current default locale of the computer. The documentation language can be changed for all users on a computer, or it can be changed for a single user.

Notes:

1. These techniques do not affect the language that is used if you are opening a document or search form from an HTML link inside a document. These techniques only affect what language is used when you use the desktop icons or the **docsearch** command.
2. Before a computer can serve documents in a language, the locale (language environment) for that language and the library service messages for the language must be installed on the documentation server. For instructions, see Chapter 7. Installing and Configuring Documentation Library Service and Online Documentation in *AIX 5L Version 5.2 Installation Guide and Reference*.

Changing the Default Documentation Language for All Users

To change the default documentation language for all users on a computer, the system administrator (as **root**) can use the Web-based System Manager (see "Using Web-based System Manager:") or SMIT (see "Using SMIT:").

Using Web-based System Manager:

1. Change to the root user.
2. On the command line, type: `wsm`, then double-click on **System Environment**.
3. In the `System Environments` window, double-click on the **Settings** icon to open it.
4. In the next view, double-click on the **Documentation Server** icon.
5. Scroll down until you see the **Start Up Web Page** language field, then select your new language.
6. Click **OK**. The documentation service on this computer is now reconfigured to use the new language default. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service with the new default language.

Using SMIT:

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

```
smit web_configure
```

3. From the web configuration screen, select the `Change/Show Documentation Language` choice.
4. In the **Language** dialog, select the new language. The documentation service on the computer is now reconfigured to use the new language default. Any users who were logged in when configuration was done must log out, and then log back in to reactivate the library service with the new default language.

To Change Documentation Language for a Single User

A system administrator might assign a single user a documentation language that is different than the default language of the user's computer. This is done by running the following command as **root**:

```
/usr/bin/chdoclang [-u UID|username] locale
```

where *locale* is replaced by the locale that will be the new language and *username* is replaced with the user's username. Locale names can be found in the Language Support Table.

Running the command as described adds the following line to the user's **$HOME/.profile** file:

```
export DOC_LANG=<locale>
```

where *locale* is the locale that will be the new default documentation viewing and searching language.

For example, to change the documentation language of user **fred** to be Spanish (es_ES), type the following command:

```
/usr/bin/chdoclang -u fred es_ES
```

Note: If the `DOC_LANG` environment variable is defined in a user's **.profile**, it takes precedence over any global `DOC_LANG` setting in the **/etc/environment** file on the user's computer. Also, for the Common Desktop Environment (CDE), you must uncomment the `DTSOURCEPROFILE=true` line in the **$HOME/.dtprofile** file, which causes the **$HOME/.profile** file to be read during CDE login. The change to a user's documentation language takes effect the next time the user logs out and then logs back in.

To Remove a Documentation Language Setting

If the documentation language has been set, you can delete the setting. To delete the global system default documentation language setting, run the following command as **root**:

```
/usr/bin/chdoclang -d
```

To delete a single user's language setting, run the following command:

```
/usr/bin/chdoclang -d [UID|username]
```

For example, to remove the user **fred**'s personal language setting to use the system default language, run the following command:

```
/usr/bin/chdoclang -d fred
```

Documents and Indexes

This section covers system management operations on documents and indexes for the documentation search service.

Registering Documents for Online Searching

Not all documents on a documentation server can be read and searched within the library service application. Two things must occur before a document can be accessed using the Documentation Library Service:

1. The document and its index must be created or installed on the document server.
2. The document and its index must be registered with the library service.

You can register documents two ways:

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

This section provides an overview of the steps to register a document and create an index of the document. When you are ready to actually do this work, see the chapter on the documentation library service in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs* for the detailed instructions on completing these steps.

1. Write your document in HTML.
2. Create the index of the document.
3. If you are an application developer who is creating this index for inclusion in an installp package, see the chapter on the documentation library service in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*. Follow the steps to include the index in your installation package and do automatic registration of your indexes during your package's post-installation process.

   If you are the system administrator of a documentation server, the next step is to register the new indexes on the server.
4. Now register the index. After your indexes are registered, they are displayed for reading and searching in the global Documentation Library Service application that is launched by typing the **docsearch** command or by opening the **Documentation Library Service** icon in the CDE Desktop. You can also create your own custom library application that only shows a subset of all registered documents on a documentation sever. For example, you might want a library application that only shows accounting documents. For instructions, see the chapter on the documentation library service in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.

   For detailed instructions on creating and registering a document and index, see Creating Indexes of your Documentation in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.

Deleting or Uninstalling Documents

If a document and its index were automatically registered when an application was installed on the documentation server, you must use normal software uninstall tools of the operating system to remove the document. If you simply delete a registered document or its index, it will still be registered with the library service. This generates error messages during searches since the search service still tries to search the missing index.

Note: If you uninstall a package and it does not correctly remove all of its indexes, use the following procedure to clean up your system.

If you want to delete a document that was manually registered by the system administrator, follow the instructions in Removing Indexes in Your Documentation in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.

Updating Documents

If the contents of a document change, the index of the document must be updated to reflect the changes to the contents of the document. If you are installing an updated application and it automatically registers its documents, it automatically updates the old indexes with the new ones. If you are updating a document that a user created, you have to manually update the index for the document.

1. Unregister and delete the old index. You **cannot** just delete an index. This leaves the search service corrupted. Follow the procedure in Removing Indexes in Your Documentation in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.

2. Rebuild the index. See Building the Index in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs* for more information.

Moving Documents

Do not move application documents that were automatically installed with an application. For example, do not move operating system base documentation after it is installed. If you move automatically registered documents, the search service is unable to find the documents and errors occur.

You can move documents that you wrote and manually indexed and registered. However, when you move a document, you must tell the search service how that document path has changed so that the service can find the document.

The first part of a document path is stored in the index registration table, and the last part is stored inside the index for that document. There are two methods for changing a document path depending on which part of the path you are changing.

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

1. Type:

   ```
   /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -l -x index_name
   ```

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

   The output of the command looks similar to:

   ```
   Index index_name - index_title,
   documents in: path
   function completed
   ```

   The *path* in the output shows you the part of your document path that is stored in the registration table. If you are only changing the names of directories that are listed within the *path*, you can use the first move method in the following. Write down the current *index_name*, *index_title*, and *path*. Then skip to the next numbered step to change this part of the document path.

   However, if you need to change any part of the path that is lower (to the right) of the part of the path shown in the output, you must update the index instead. This is because the lower part of the path is stored inside the index. To update the index, go back to the “Updating Documents” on page 129 section and complete all the instructions in that section. Also, go to that section if you need to make changes in both the upper and lower parts of the document path. In either case, you do not need to do any other steps in this section.

2. To change the upper part of the document path in the index registration table, type the following command:

   ```
   /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -u -x index_name -sp \
   path -ti "index_title"
   ```

   Note: There must be a trailing slash (/) in the *path*.

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

   For example, if your documents are in the **acctn3en English** index and the index title is ″Accounting Documents″, you can move the document tree from the **/doclink/en_US/engineering** directory into the **/doc_link/en_US/accounting** directory by typing the following:

   ```
   /usr/IMNSearch/bin/itedomap -p /var/docsearch/indexes -u -x acctn3en -sp \
   /doc_link/en_US/accounting/ -ti "Accounting Documents"
   ```

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

Changing the document's library service location is now complete. If you have not already done so, you can now move your documents. Next, test your changes by searching for a word that is inside the moved documents. The document's link in the search results page correctly displays the document.

Security

Follow your normal security procedures for the documents on the documentation server. In addition, a documentation server also has the added security elements of the document indexes and the web server software.

Indexes are treated as files that include a list of all the words in the original documents. If the documents contain confidential information, then the indexes themselves are treated with the same care as the documents.

There are three levels of security you can set up for indexes:

- **No Restrictions**

  By default, the permissions on the indexes directory are set so that all web server users can both search and read all index files.

- **Search, but not read**

  All web server users can search inside indexes for key words, but cannot open an index file to directly read its contents. This makes it more difficult for users to obtain confidential data, but a person can sometimes still gain a lot of information just by knowing if certain key words are inside a document. Assuming you store all your indexes in the standard location, you can set this level of security by setting the permissions of the **/usr/docsearch/indexes** directory. It is set to the user:group **imnadm:imnadm** with all permissions for others disabled so that only members of the imnadm search administration group can read the index files. To set these permissions type the following two commands:

  ```
  chown -R imnadm:imnadm /usr/docsearch/indexes
  chmod -R o-rwx /usr/docsearch/indexes
  ```

  Note: The user imnadm must always be able to read and execute the directory where you store indexes. This is because the search engine runs as user **imnadm** when it searches inside indexes.

- **No search, no read**

  This is done by setting the permissions as in ″Search, but not read″ to prevent reading of index files. In addition, a user's permission to use the search service web server is disabled (this prevents searches). The user is unable to search indexes because the web server does not let the user open the search form. This security level is set up using the administration functions in your web server software to turn off a user's permission to use the web server. See the documentation that came with your web server to determine how to configure your web server software to prevent access by specific users.

Documentation Library Service Advanced Topics

Search Service Administrators Authority

Only root and members of the **imnadm** (IMN administration) user group have the authority to perform administrative tasks for the Documentation Library Service. This includes tasks such as creating document indexes, registering indexes, and unregistering indexes. If you want users to be able to perform these functions, add them to the **imnadm** group using one of the administration tools.

Note: If you add users to the **imnadm** group, they are able to read the contents of all indexes on the system. See "Security" for more information.

Creating Custom Library Applications

When you open the global library application, all documents that are registered with the global view set are displayed. You might want to create a custom library application that only shows a subset of the documents on a documentation server. For example, you may want to put a ″library″ or ″search″ link inside the ″Project X Plan″ HTML document. When a user clicks on one of these links, a library opens and displays a list of the documents for Project X. You can then read or search these documents.

For instructions on how to create your own custom library applications, see the chapter on the documentation library service in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs* for more information.

Documentation Library Service 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 Documentation Library Service, and your web browser is using a cache, that error message page is stored in your web browser cache. This means that even if you fix the problem that caused the error, the error message continues to be displayed if you repeat the exact same search that caused the error in the first place. Therefore, it is important that you clear out the contents of the browser cache before you retest the search after you have done a fix. Usually, there is a **clear cache** function in the `Options` screen of the browser.

Problems That Don’t Generate Error Messages

- **When the search form is displayed it is not in the correct language.**

  The language of the search form is possibly being set by the document that is opening the search form. For example, if the document was written in Spanish, the author may have specified that when the Search link in the document is clicked, the search service provides the search form in Spanish. Look at the Search link and see if it is specifying a language.

  The web server software might not be reading the locale value correctly. Try restarting your web server to see if it picks up the correct locale.

Error Message Listings

- **ds_form: Error**

  ```
  There was a request to open a viewset named 'XXX'. Either there is no viewset
  named 'XXX', or there is no configuration file named '/usr/docsearch/views
  /<locale>/XXX/config' for the viewset. If you want to continue now, you
  can use the generic search page, which will allow you to search all volumes.

  Use generic page
  ```

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

  In this message XXX indicates the name of the viewset. If the viewset given in the message does not match the name of the desired viewset, edit the HTML link being used to call the search form and change the viewset given.

- **ds_form: Error EhwStartSession 70**

  ```
  There was a problem communicating with the search program.

  Retry your search. If you repeatedly get this error, contact the system administrator of the search
  server computer. They may want to try restarting the search program.
  ```

  This error occurs if the search engine is not running.

To start the search engine, you must be root or a member of the group **imnadm**. To start the search engine type:

```
itess -start search
```

- **ds_form: Error**

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

  This error occurs if the CGIs are passed a language for which the documentation server does not have the locale installed.

  In this message xx_XX is the language for which there was no locale installed. If it is available, the locale for the language can be installed. Otherwise, specify a language for which there is a locale installed by using the *lang* parameter.

- **ds_form: Error EhwSearch 77**

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

  This error occurs if the file permissions for an index are incorrectly set on files or directories that are part of that index.

  Where *indexname* is the name of an index, the index files, or links to them, can be found in:

  ```
  /usr/docsearch/indexes/indexname/data
  /usr/docsearch/indexes/indexname/work
  ```

  Make sure all index file permissions adhere to the following rules:

  – All index files and directories are readable by the user **imnadm**.
  – The work directory and all files in it are writable by the user **imnadm**.
  – In the data directory the **iteadmtb.dat** and **iteiq.dat** files are writable.
  – All index files and directories have **imnadm** as owner and group.

- **ds_rslt: Error EhwSearch 32**

  ```
  The search program reported an unexpected error condition.
  ```

  The most likely cause of this error is that the file permissions for one or more indexes are incorrectly set.

  Where *indexname* is the name of an index, the index files, or links to them, can be found in:

  ```
  /usr/docsearch/indexes/indexname/data
  /usr/docsearch/indexes/indexname/work
  ```

  – All index files and directories are readable by the user **imnadm**.
  – The work directory and all files in it are writable by the user **imnadm**.
  – In the data directory the **iteadmtb.dat** and **iteiq.dat** files are writable.
  – All index files and directories have **imnadm** as owner and group.

- **ds_rslt: Error EhwSearch 8**

  ```
  One or more of the indexes for the selected volumes contain errors that make them unsearchable.

  Error 76 in index indexname

  The requested function is in error.

  Contact the system administrator of the search server computer.
  ```

  This error occurs when one or more of the indexes being searched needs to be reset.

  To reset an index you must be root or a member of the group **imnadm**. Reset the index with the **itectrix** command by typing:

  ```
  /usr/IMNSearch/bin/itectrix -s server -x indexname -reset
  ```

- **ds_rslt: Error EhwSearch 76**

  ```
  The requested function is in error.

  Contact the system administrator of the search server computer.
  ```

  This error occurs when all of the indexes being searched need to be reset.

To reset an index you must be root or a member of the group **imnadm**. Reset the index with the **itectrix** command by typing:

```
/usr/IMNSearch/bin/itectrix -s server -x indexname -reset
```

- **Cannot run ds_form**

  A web server error message saying it cannot run **ds_form**. The exact wording of the message varies across different web server software. For example, the message might say something like:

  ```
  ds_form is not an executable
  ```

  or

  ```
  Cannot locate ds_form
  ```

  The web server software cannot find the search service **ds_form** CGI program because the server has not been configured correctly. See “Changing the Configuration of the Documentation Library Service” on page 121 to make sure that the Documentation Library Service is installed and configured correctly on the server computer.

Chapter 7. Device Management Tasks

This chapter provides procedures for managing tape drives and other devices, such as printers and disk drives.

Tape Drives

This section covers system management functions related to tape drives. Many of these functions change or get information from the device configuration database that contains information about the devices on your system. The device configuration database consists of the predefined configuration database that contains information about all possible types of devices supported on the system, and the customized configuration database that contains information about the particular devices currently on the system. For the operating system to make use of a tape drive, or any other device, the device must be defined in the customized configuration database and must have a device type defined in the predefined configuration database.

See the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices* for the following related topics:

Basic tasks for tape drives are shown in the following table:

Tape Drive Tasks

Task	SMIT Fast Path	Command or File
List All Defined Tape Drives	**smit lsdtpe**	**lsdev -C -c tape -H**
List All Supported Tape Drives	**smit lsstpe**	**lsdev -P -c tape -F "*type subclass description*" -H**
Add New Tape Drives Automatically	**smit cfgmgr**	**cfgmgr**
Add a User-Specified Tape Drive	**smit mktpe**Note 1	**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**Note 2
Change Attributes of a Tape Drive	**smit chgtpe**	**chdev -l rmt0 -a block_size='512' -a mode=no**Note 2
Remove a Tape Drive	**smit rmvtpe**	**rmdev -l 'rmt0'**Note 2
Generate an Error Report for a Tape Drive	**smit errpt**	See Error Logging Tasks in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.
Trace a Tape Drive	**smit trace_link**	See Starting the Trace Facility in *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*.

Notes:

1. This fast path applies to parallel SCSI devices only (scsi subclass), not to Fibre Channel devices (fcp subclass).

2. Where `rmt0` is the logical name of a tape drive.

Tape Drive Attributes

The following describes tape drive attributes you can adjust to meet the needs of your system. The attributes can be displayed or changed using the Web-based System Manager Devices application, SMIT, or commands (in particular, the **lsattr** and the **chdev** commands).

Each type of tape drive only uses a subset of all the attributes.

General Information about Each Attribute

Block Size: The block size attribute indicates the block size to use when reading or writing the tape. Data is written to tape in blocks of data, with inter-record gaps between blocks. Larger records are useful when writing to unformatted tape, because the number of inter-record gaps is reduced across the tape, allowing more data to be written. A value of **0** indicates variable length blocks. The allowable values and default values vary depending on the tape drive.

Device Buffers: Setting the Device Buffers attribute (the **mode** attribute for the **chdev** command) to the Yes value indicates an application is notified of write completion after the data has been transferred to the data buffer of the tape drive, but not necessarily after the data is actually written to the tape. If you specify the No value, an application is notified of write completion only after the data is actually written to the tape. Streaming mode cannot be maintained for reading or writing if this attribute is set to the No value. The default value is Yes.

With the No value, the tape drive is slower but has more complete data in the event of a power outage or system failure and allows better handling of end-of-media conditions.

Extended File Marks: Setting the Extended File Marks attribute (the **extfm** attribute for the **chdev** command) to the No value writes a regular file mark to tape whenever a file mark is written. Setting this attribute to the Yes value writes an extended file mark. For tape drives, this attribute can be set on. The default value is No. For example, extended filemarks on 8 mm tape drives use 2.2 MB of tape and can take up to 8.5 seconds to write. Regular file marks use 184 K and take approximately 1.5 seconds to write.

When you use an 8 mm tape in append mode, use extended file marks for better positioning after reverse operations at file marks. This reduces errors.

Retension: Setting the Retension attribute (the **ret** attribute for the **chdev** command) to Yes instructs the tape drive to retension a tape automatically whenever a tape is inserted or the drive is reset. *Retensioning* a tape means to wind to the end of the tape and then rewind to the beginning of the tape to even the tension throughout the tape. Retensioning the tape can reduce errors, but this action can take several minutes. If you specify the No value, the tape drive does not automatically retension the tape. The default value is Yes.

Density Setting #1 and Density Setting #2: Density Setting #1 (the **density_set_1** attribute for the **chdev** command) sets the density value that the tape drive writes when using special files **/dev/rmt***, **/dev/rmt*.1**, **/dev/rmt*.2**, and **/dev/rmt*.3**. Density Setting #2 (for the **density_set_2** attribute of the **chdev** command) sets the density value that the tape drive writes when using special files **/dev/rmt*.4**, **/dev/rmt*.5**, **/dev/rmt*.6**, and **/dev/rmt*.7**. See “Special Files for Tape Drives” on page 144 for more information.

The density settings are represented as decimal numbers in the range 0 to 255. A zero (0) setting selects the default density for the tape drive, which is usually the drive’s high density setting. Specific permitted values and their meanings vary with different types of tape drives. These attributes do not affect the ability

of the tape drive to read tapes written in all densities supported by the tape drive. It is customary to set Density Setting #1 to the highest density possible on the tape drive and Density Setting #2 to the second highest density possible on the tape drive.

Reserve Support: For tape drives that use the Reserve attribute (the **res_support** attribute for the **chdev** command), specifying the Yes value causes the tape drive to be reserved on the SCSI bus while it is open. If more than one SCSI adapter shares the tape device, this ensures access by a single adapter while the device is open. Some SCSI tape drives do not support the reserve or release commands. Some SCSI tape drives have a predefined value for this attribute so that the reserve and release commands are always supported.

Variable Length Block Size: The Variable Length Block Size attribute (the **var_block_size** attribute for the **chdev** command) specifies the block size required by the tape drive when writing variable length records. Some SCSI tape drives require that a nonzero block size be specified in their Mode Select data even when writing variable length records. The Block Size attribute is set to 0 to indicate variable length records. Refer to the specific tape drive SCSI specification to determine whether this is required.

Data Compression: Setting the Data Compression attribute (the **compress** attribute for the **chdev** command) to Yes causes the tape drive to be in compress mode, if the drive is capable of compressing data. If so, then the drive writes data to the tape in compressed format so that more data fits on a single tape. Setting this attribute to No forces the tape drive to write in native mode (noncompressed). Read operations are not affected by the setting of this attribute. The default setting is Yes.

Autoloader: Setting the Autoloader attribute (the **autoload** attribute for the **chdev** command) to Yes causes Autoloader to be active, if the drive is so equipped. If so, and another tape is available in the loader, any read or write operation that advances the tape to the end is automatically continued on the next tape. Tape drive commands that are restricted to a single tape cartridge are unaffected. The default setting is Yes.

Retry Delay: The Retry Delay attribute sets the number of seconds that the system waits after a command has failed before reissuing the command. The system may reissue a failed command up to four times. This attribute applies only to type ost tape drives. The default setting is 45.

Read/Write Timeout: The Read/Write Timeout or Maximum Delay for a READ/WRITE attribute sets the maximum number of seconds that the system allows for a read or write command to complete. This attribute applies only to type ost tape drives. The default setting is 144.

Return Error on Tape Change: The Return Error on Tape Change or Reset attribute, when set, causes an error to be returned on open when the tape drive has been reset or the tape has been changed. A previous operation to the tape drive must have taken place that left the tape positioned beyond beginning of tape upon closing. The error returned is a -1 and **errno** global value is set to **EIO**. After being presented to the application, the error condition is cleared. Also, reconfiguring the tape drive itself clears the error condition.

Attributes for 2.0 GB 4 mm Tape Drives (Type 4mm2gb)

Block Size: The default value is 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values: If a tape drive is configured as a 2.0 GB 4 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Density Setting #1, and Density Setting #2 attributes have predefined values that cannot be changed. The density settings are predefined because the tape drive always writes in 2.0 GB mode.

Attributes for 4.0 GB 4 mm Tape Drives (Type 4mm4gb)

Block Size: The default value is 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The user cannot change the density setting of this drive; the device reconfigures itself automatically depending on the Digital Data Storage (DDS) media type installed, as follows:

Media Type	Device Configuration
DDS	Read-only.
DDS |||	Read/write in 2.0 GB mode only.
DDS2	Read in either density; write in 4.0 GB 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 4.0 GB 4 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Density Setting #1, and Density Setting #2 attributes have predefined values that cannot be changed.

Attributes for 2.3 GB 8 mm Tape Drives (Type 8mm)

Block Size: The default value is 1024. A smaller value reduces the amount of data stored on a tape.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values: If a tape drive is configured as a 2.3 GB 8 mm tape drive, the Retension, Reserve Support, Variable Length Block Size, Data Compression, Density Setting #1, and Density Setting #2 attributes have predefined values which cannot be changed. The density settings are predefined because the tape drive always writes in 2.3 GB mode.

Attributes for 5.0 GB 8 mm Tape Drives (Type 8mm5gb)

Block Size: The default value is 1024. If a tape is being written in 2.3 GB mode, a smaller value reduces the amount of data stored on a tape.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
140	5 GB mode (compression capable)
21	5 GB mode noncompressed tape
20	2.3 GB mode
0	Default (5.0 GB mode)

The default values are 140 for Density Setting #1, and 20 for Density Setting #2. A value of 21 for Density Setting #1 or #2 permits the user to read or write a noncompressed tape in 5 GB mode.

Data Compression: The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values: If a tape drive is configured as a 5.0 GB 8 mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 20000 MB 8mm Tape Drives (Self-Configuring)

Block Size: The default value is 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The drive can read and write data cartridges in 20.0 GB format. During a Read command, the drive automatically determines which format is written on tape. During a Write, the Density Setting determines which data format is written to tape.

The following settings apply:

Setting	Meaning
39	20 GB mode (compression capable)
0	Default (20.0 GB mode)

The default value is **39** for Density Setting #1 and Density Setting #2.

Data Compression: The general information for this attribute applies to this tape drive type.

Attributes with Fixed Values: If a tape drive is configured as a 20.0 GB 8 mm tape drive, the Retension, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 35 GB Tape Drives (Type 35gb)

Block Size: The IBM 7205 Model 311 throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32 K Bytes. Any block size less than 32 K Bytes restricts the data rate (backup and restore time). The following table lists recommended block sizes by command:

Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32 K or 51.2 K (default)	Uses either 32 K or 51.2 K depending on if ″Backup″ is by name or not. No change is required.
TAR	10 K	There is an error in the manual that states a 512 K byte block size. Set the Blocking Parameter to *-N64*.
MKSYSB	See BACKUP	MKSYSB uses the BACKUP Command. No change is required.
DD	n/a	Set the Blocking Parameter to *bs=32K*.
CPIO	n/a	Set the Blocking Parameter to *-C64*.

Note: Be aware of the capacity and throughput when you select a blocksize. Small blocksizes have a significant impact on performance and a minimal impact on capacity. The capacities of the 2.6 GB format (density) and 6.0 GB format (density) are significantly impacted when you use smaller than the recommended blocksizes. As an example: using a blocksize of 1024 bytes to backup 32 GB of data takes approximately 22 hours. Backing up the same 32 GB of data using a blocksize of 32 K Bytes takes approximately 2 hours.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following chart shows the Supported Data Cartridge type and Density Settings (in decimal and hex) for the IBM 7205-311 Tape Drive. When you perform a Restore (Read) Operation, the tape drive automatically sets the density to match the written density. When you perform a Backup Operation (Write), you must set the Density Setting to match the Data Cartridge that you are using.

Supported Data Cartridges	Native Capacity	Compressed Data Capacity	Web-based System Manager or SMIT Density Setting	HEX Density Setting
DLTtape III	2.6 GB	2.6 GB (No Compression)	23	17h
	6.0 GB	6.0 GB (No Compression)	24	18h
	10.0 GB	20.0 GB (Default for drive)	25	19h
DLTtapeIIIxt	15.0 GB	30.6 GB (Default for drive)	25	19h
DLTtapeIV	20.0 GB	40.0 GB	26	1Ah
	35.0 GB	70.0 GB (Default for drive)	27	1Bh

Note: If you request an unsupported Native Capacity for the Data Cartridge, the drive defaults to the highest supported capacity for the Data Cartridge that is loaded into the drive.

Data Compression: The actual compression depends on the type of data being that is being written (see previous table). A Compression Ratio of 2:1 is assumed for this Compressed Data Capacity.

Attributes with Fixed Values: The general information for this attribute applies to this tape drive type.

Attributes for 150 MB 1/4-Inch Tape Drives (Type 150mb)

Block Size: The default block size is 512. The only other valid block size is 0 for variable length blocks.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
16	QIC-150
15	QIC-120
0	Default (QIC-150), or whatever was the last density setting by a using system.

The default values are 16 for Density Setting #1, and 15 for Density Setting #2.

Attributes with Fixed Values: If a tape drive is configured as a 150 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 525 MB 1/4-Inch Tape Drives (Type 525mb)

Block Size: The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you want to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
17	QIC-525*
16	QIC-150
15	QIC-120
0	Default (QIC-525), or whatever was the last density setting by a using system.

* QIC-525 is the only mode that supports the 1024 block size.

The default values are 17 for Density Setting #1, and 16 for Density Setting #2.

Attributes with Fixed Values: If a tape drive is configured as a 525 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 1200 MB 1/4-Inch Tape Drives (Type 1200mb-c)

Block Size: The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
21	QIC-1000*
17	QIC-525*
16	QIC-150
15	QIC-120
0	Default (QIC-1000), or whatever was the last density setting by a using system.

Notes:

1. QIC-525 and QIC-1000 are the only modes that support the 1024 block size.
2. The default values are 21 for Density Setting #1, and 17 for Density Setting #2.

Attributes with Fixed Values: If a tape drive is configured as a 1200 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 12000 MB 4 mm Tape Drives (Self-Configuring)

Block Size: The IBM 12000 MB 4 mm Tape Drive's throughput is sensitive to blocksize. The minimum recommended blocksize for this drive is 32 K Bytes. Any block size less than 32 K Bytes restricts the data rate (backup/restore time). The following table lists recommended block sizes by command:

Command Supported	Default Block Size (Bytes)	RECOMMENDATION
BACKUP	32 K or 51.2 K (default)	Will use either 32 K or 51.2 K depending on if ″Backup″ is by name or not. No change is required.
TAR	10 K	There is an error in the manual that states a 512 K byte block size. Set the Blocking Parameter to **-N64**.
MKSYSB	See BACKUP	MKSYSB uses the BACKUP Command. No change is required.
DD	n/a	Set the Blocking Parameter to **bs=32K**.
CPIO	n/a	Set the Blocking Parameter to **-C64**.

Note: You should be aware of the capacity and throughput when you select a blocksize. Small blocksizes have a significant impact on performance and a minimal impact on capacity.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following chart shows the Supported Data Cartridge type and Density Settings (in decimal and hex) for the IBM 12000 MB 4 mm Tape Drive. When you perform a Restore (Read) Operation, the tape drive automatically sets the density to match the written density. When you perform a Backup Operation (Write), you must set the Density Setting to match the Data Cartridge you are using.

Supported Data Cartridges	Native Capacity	Compressed Data Capacity	Web-based System Manager or SMIT Density Setting	HEX Density Setting
DDS III	2.0 GB	4.0 GB	19	13h
DDS2	4.0 GB	8.0 GB	36	24h
DDS3	12.0 GB	24.0 GB	37	25h

Note: If you request an unsupported Native Capacity for the Data Cartridge, the drive defaults to the highest supported capacity for the Data Cartridge that is loaded into the drive.

Data Compression: The actual compression depends on the type of data being that is being written (see the previous table). A Compression Ratio of 2:1 is assumed for this Compressed Data Capacity.

Attributes with Fixed Values: The general information for this attribute applies to this tape drive type.

Attributes for 13000 MB 1/4-Inch Tape Drives (Self-Configuring)

Block Size: The default block size is 512. The other valid block sizes are 0 for variable length blocks, and 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: Writing to a 1/4-inch tape can only occur at the beginning of tape (BOT) or after blank tape is detected. If data exists on the tape, you cannot overwrite the data except at BOT. If you wish to add data to a tape that has been written and then rewound, you must space forward until the next file mark is detected, which causes the system to return an error. Only then can you start writing again.

Retension: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
33	QIC-5010-DC*
34	QIC-2GB*
21	QIC-1000*
17	QIC-525*
16	QIC-150
15	QIC-120
0	Default (QIC-5010-DC)*

Notes:

1. QIC-525, QIC-1000, QIC-5010-DC, and QIC-2GB are the only modes that support the 1024 block size.
2. The default values are 33 for Density Setting #1, and 34 for Density Setting #2.

Attributes with Fixed Values: If a tape drive is configured as a 13000 MB 1/4-inch tape drive, the Extended File Marks, Reserve Support, and Variable Length Block Size attributes have predefined values which cannot be changed.

Attributes for 1/2-Inch 9-Track Tape Drives (Type 9trk)

Block Size: The default block size is 1024.

Device Buffers: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The following settings apply:

Setting	Meaning
3	6250 bits per inch (bpi)
2	1600 bpi
0	Whichever writing density was used previously.

The default values are 3 for Density Setting #1, and 2 for Density Setting #2.

Attributes with Fixed Values: If a tape drive is configured as a 1/2-inch 9-track tape drive, the Extended File Marks, Retension, Reserve Support, Variable Length Block Size, and Data Compression attributes have predefined values which cannot be changed.

Attributes for 3490e 1/2-Inch Cartridge (Type 3490e)

Block Size: The default block size is 1024. This drive features a high data transfer rate, and block size can be critical to efficient operation. Larger block sizes can greatly improve operational speeds, and in general, the largest possible block size should be used.

Note: Increasing the block value can cause incompatibilities with other programs on your system. If this occurs, you receive the following error message while running those programs:

```
A system call received a parameter that is not valid.
```

Device Buffers: The general information for this attribute applies to this tape drive type.

Compression: The general information for this attribute applies to this tape drive type.

Autoloader: This drive features a tape sequencer, an autoloader that sequentially loads and ejects a series of tape cartridges from the cartridge loader. For this function to operate correctly, the front panel switch must be in the AUTO position and the Autoloader attribute must be set to Yes.

Attributes for Other SCSI Tapes (Type ost)

Block Size: The system default is 512, but this should be adjusted to the default block size for your tape drive. Typical values are 512 and 1024. 8 mm and 4 mm tape drives usually use 1024 and waste space on the tape if the block size attribute is left at 51. 0 indicates variable block size on some drives.

Device Buffers: The general information for this attribute applies to this tape drive type.

Extended File Marks: The general information for this attribute applies to this tape drive type.

Density Setting #1 and Density Setting #2: The default value is 0 for both of these settings. Other values and their meanings vary for different tape drives.

Reserve Support: The default value is No. This may be set to Yes, if the drive supports reserve/release commands. If you are unsure, No is a safer value.

Variable Length Block Size: 0 is the default value. Nonzero values are used primarily on quarter inch cartridge (QIC) drives. Refer to the SCSI specification for the particular tape drive for advice.

Retry Delay: This attribute applies exclusively to type ost tape drives

Read/Write Timeout: This attribute applies exclusively to type ost tape drives

Attributes with Fixed Values: If a tape drive is configured as an Other SCSI tape drive, the Extended File Marks, Retension, and Data Compression attributes have predefined values which cannot be changed.

Special Files for Tape Drives

Writing to and reading from files on tapes is done by using **rmt** special files. There are several special files associated with each tape drive known to the operating system. These special files are **/dev/rmt***, **/dev/rmt*.1**, **/dev/rmt*.2**, ... **/dev/rmt*.7**. The **rmt*** is the logical name of a tape drive, such as **rmt0**, **rmt1**, and so on.

By selecting one of the special files associated with a tape drive, you make choices about how the I/O operations related to the tape drive will be performed.

Density — You can select whether to write with the tape drive Density Setting #1 or with the tape drive Density Setting #2. The values for these density settings are part of the attributes of the tape drive. Because it is customary to set Density Setting #1 to the highest possible density for the tape drive and Density Setting #2 to the next highest possible density for the tape drive, special files that use Density Setting #1 are sometimes referred to as high density and special files that use Density Setting #2 sometimes are referred to as low density, but this view is not always correct. When reading from a tape, the density setting is ignored.

Rewind-on-Close — You can select whether the tape is rewound when the special file referring to the tape drive is closed. If rewind-on-close is selected, the tape is positioned at the beginning of the tape when the file is closed.

Retension-on-Open — You can select whether the tape is retensioned when the file is opened. Retensioning means winding to the end of the tape and then rewinding to the beginning of the tape to reduce errors. If retension-on-open is selected, the tape is positioned at the beginning of the tape as part of the open process.

The following table shows the names of the **rmt** special files and their characteristics. For more information about tape drive special files, see *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

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

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. The following sections provide instructions for managing devices:

Preparing to Install a Device

Installing devices on your system consists of identifying where the device is to be attached, connecting the device physically, and configuring the device with Web-based System Manager, the Configuration Manager, or SMIT.

This section documents installation tasks that are common to all devices. Because of the wide variety of devices that you can install on your system, only a general procedure is provided. For more specific information, see the installation instructions shipped with the specific device.

Note: The following procedure requires a shutdown of your system to install the device. Not all device installations require a shutdown of your system. Refer to the documentation shipped with the specific device.

1. Stop all applications running on the system unit and shut down the system unit using the **shutdown** command.
2. Turn off the system unit and all attached devices.
3. Unplug the system unit and all attached devices.
4. Connect the new device to the system using the procedure described in the setup and operator guide for the device.
5. Plug in the system unit and all attached devices.
6. Turn on all the attached devices leaving the system unit turned off.
7. Turn on the system unit when all the devices complete power-on self-tests (POST).

The Configuration Manager automatically scans the attached devices and configures any new devices it detects. The new devices are configured with default attributes and recorded in the customized configuration database placing the device in **Available** state.

You can manually configure a device using Web-based System Manager (`wsm`, then select `Devices`), or the SMIT fast path, **smit dev**. If you need to customize the device attributes or if the device cannot be configured automatically, see the device documentation that shipped with the device for specific configuration requirements.

Installing an IDE Device

This section outlines the procedure used to install an IDE device on your system. The procedure has been divided into several tasks that must be performed in order.

Prerequisites

- You must have access to the operator's guide for your system unit and the installation guide for the device to be installed. The documentation must identify how to set the IDE device jumper to configure the device to either the master or slave setting.
- There must be at least one unused IDE device ID on an IDE adapter on the system.
- If you are updating the product topology diskettes, you need the Product Topology System diskette which is kept with important records for the system, and the Product Topology Update diskette which is shipped with the device.
- Verify that the interface of the device is compatible with the interface of the IDE controllers on the system unit.
- There are two classifications for IDE devices, ATA and ATAPI. ATA are disk devices and ATAPI are CD-ROM or tape devices. Up to two devices are allowed to be connected to each IDE controller, one master and one slave. Typically an IDE adapter has two controllers, which allows up to four IDE devices to be attached.

  With appropriate cabling, you can attach any of the following device combinations to a single controller:

  – 1 ATA device as master

– 1 ATAPI device as master
– 2 ATA devices as master and slave
– 1 ATA device as master and 1 ATAPI device as slave
– 2 ATAPI devices as master and slave

You cannot attach the following:

– 1 ATA device as slave only
– 1 ATAPI device as slave only
– 1 ATAPI device as master and 1 ATA device as slave

Task 1 - Determine the Number and Location of the IDE Controllers

Determine how many IDE controllers are attached to your system unit and where the IDE controllers are located. An IDE adapter may be in an adapter slot or built into the system planar. Remember that IDE adapters have two IDE controllers (IDE buses). Thus, two IDE controllers are found in an adapter slot or built into the system planar.

You can obtain this information two different ways:

- Using a software configuration command. This method is available only when the operating system has been installed on the system unit.
- Using the *About Your Machine* document shipped with your system unit. This method is valid only for initial setup and installation of a new system unit.

Using a Software Configuration Command: This method applies to a system that already has the operating system installed.

To list the IDE I/O controllers on the system, type the following commands:

```
lscfg -l ide*
```

Examine the list of IDE controllers that are displayed. The following sample display from the **lscfg -l ide** command shows two IDE I/O controllers. Controller `ide0` and `ide1` are located on the system planar. The planar indicator is the second digit in the location value with a value of 1.

```
DEVICE    LOCATION      DESCRIPTION

ide0      01-00-00      ATA/IDE Controller Device
ide1      01-00-01      ATA/IDE Controller Device

           |     |
2nd digit is     6th digit indicates the controller number.
the adapter
slot number
```

Initial Setup: Use the *About Your Machine* document to determine the IDE I/O controllers on the system if the device is being installed during initial setup.

Note: Incorrect results are produced if controllers have been added after the system was shipped from the factory.

Determine whether the system unit has an IDE controller built into the planar board. A built-in IDE I/O controller is standard on some system units. Your system unit has a built-in IDE controller if *About Your Machine* document shows an internal media IDE device with a blank slot number.

Task 2 - Select an IDE Controller and an IDE Address on the Controller

After identifying the IDE controllers attached to the system unit, select the IDE I/O controller to which you want to connect a device. This IDE I/O controller must have at least one IDE setting that is not already assigned to another device.

Determine whether IDE device setting must be jumpered as master or slave. If no device is currently attached to the controller, the IDE device jumper must be set to master (some devices require no device ID setting in this situation). If an IDE device is already attached, the type of device must be determined. Disks are ATA devices. CD-ROM and tape are ATAPI devices. If ATA and ATAPI devices are both attached to the same IDE controller, the ATA device must be set to master ID and the ATAPI device must be set to slave ID.

Determine what IDE devices are attached to a controller by viewing information about the devices already connected to the IDE controllers.

You can use two methods to select an IDE I/O controller and an IDE address on the controller that is not already assigned to another device:

- Using a software configuration command if the operating system is already installed on the system unit.
- Using the *About Your Machine* document for initial setup and installation of a new system unit.

Using a Software Configuration Command: This method applies to a system that already has the operating system installed.

1. Type the following command to list all the currently defined IDE devices:

   ```
   lsdev -C -s ide -H
   ```

2. Examine the list of devices already assigned to each IDE controller. Each row in this display shows the logical name, status, location, and description of an IDE device. The location for each device begins with the location of the controller that the device is connected. In the sample below, the IDE I/O controller with address 01-00-00 has two IDE devices attached. The IDE I/O controller with location 01-00-01 has one IDE device attached.

   ```
   name     status       location       description
   hdisk0   Available    01-00-00-00    720 MB IDE Disk Drive
   hdisk1   Available    01-00-00-01    540 MB IDE Disk Drive
   cd0      Available    01-00-01-00    IDE CD-ROM Drive
                              |
                         IDE controller address (6th digit)
   ```

3. Select a controller that does not have two IDE devices already connected.
4. If one device is already attached to the controller, determine the type of the device. Also determine the type of device to be installed. Disk devices are classified as ATA devices. CD-ROM and tape devices are classified as ATAPI devices.
5. Determine the IDE jumper setting for the new device depending upon the combination of devices to be connected to the IDE controller. If the new device is the only device connected to the controller, the device jumper setting must be set to the master position (some devices require no setting in this case). If both devices are the same type, the new device jumper setting can be set to the slave position. If there is a mix of devices (ATA and ATAPI), the ATA device jumper must be set to the master position and the ATAPI device jumper must be set to the slave position. If there is a mix of devices and the new device is an ATA device (disk), the device jumper for the currently existing ATAPI device must be changed to the slave position and the new ATA device jumper must be set to master. If there is a mix of devices and the new device is an ATAPI device (CD-ROM or tape), the device jumper for the new ATAPI device must be set to slave and if the ATA device does not currently have a jumper setting, it must be set to master.

Initial Setup: Use the *About Your Machine* document to determine the devices assigned to the IDE I/O controllers on the system if the device is being installed during initial setup.

Note: Incorrect results are produced if controllers have been added after the system was shipped from the factory.

1. To determine the IDE devices assigned to addresses on the IDE controllers, see ″Internal Media Devices″ in *About Your Machine*.
2. Select a controller that does not have two IDE devices already connected.

3. If one device is already attached to the controller, determine the type of the device. Also determine the type of device to be installed. Disk devices are classified as ATA devices. CD-ROM and tape devices are classified as ATAPI devices.
4. Determine the IDE jumper setting for the new device depending upon the combination of devices to be connected to the IDE controller. If the new device will be the only device connected to the controller, the device jumper setting must be set to the master position (some devices require no setting in this case). If both devices are the same type, the new device jumper setting can be set to the slave position. If there is a mix of devices (ATA and ATAPI), the ATA device jumper must be set to the master position and the ATAPI device jumper must be set to the slave position. If there is a mix of devices and the new device is an ATA device (disk), the device jumper for the currently existing ATAPI device must be changed to the slave position and the new ATA device jumper must be set to master. If there is a mix of devices and the new device is an ATAPI device (CD-ROM or tape), the device jumper for the new ATAPI device must be set to slave and if the ATA device does not currently have a jumper setting, it must be set to master.

Task 3 - Setting Up the Hardware

Prerequisites:

- Do not begin this task until you have selected and recorded the following:
  - Position of the IDE I/O controller where the device will be connected (either built-in or identified by an adapter slot number).
  - IDE address for the device.
- Determine the physical position on the system unit to connect the selected IDE controller. For example, locate the position of the built-in IDE controller. Refer to the operator's guide for help.

Procedure:

1. Shut down the system unit using the **shutdown** command after stopping all applications that are currently running. Type `shutdown -F` to stop the system immediately without notifying other users.
2. Wait for the message `Halt Completed` or a similar message to be displayed.
3. Turn off the system unit and all attached devices.
4. Unplug the system unit and all attached devices.
5. Make the physical connections following the procedure described in the setup and operator guide.

   Note: Do not power on the system unit; proceed to the next task.

Task 4 - Add the Device to the Customized Configuration Database

This task makes the device known to the system. During system unit startup, the operating system reads the current configuration and detects new devices. A record of each new device is added to the customized configuration database and are given default attributes.

If the device is being installed on a new system unit, the operating system must be installed. Instructions for installing the operating system are included in the installation guide for the operating system.

Follow this procedure to add a device to the customized configuration database:

1. Plug in the system unit and all attached devices.
2. Turn on all the devices, but leave the system unit turned off.
3. Turn on the system unit when all the attached devices have completed power-on self-tests (POSTs).

   Note: The startup process automatically detects and records the device in the customized configuration database.

4. Confirm that the device was added to the customized configuration database using the Web-based System Manager (type **wsm**), or the SMIT fast path, **smit lsdidea**. A list of all defined devices is displayed. Look at the location field for the IDE adapter and IDE address values of the device you just installed.

Task 5 - Customize the Attributes for the Device (Optional)

Default attributes are assigned to a supported device when it is added to the customized configuration database. These attributes are appropriate for typical use of the device. Change the device attributes when the device you are installing is not supported or when you need to customize some part of the device's operation. For example, you might need to change your tape drive to write tapes in a lower-density format.

To customize the attributes for a device use the SMIT fast path, **smit dev**.

Configuring a Read/Write Optical Drive

There are two methods for configuring a read/write optical drive.

Prerequisite

The read/write optical drive must be connected to the system and powered on.

Method 1: Method one is the faster of the two methods. It only configures the read/write optical drive specified. To use this method, you must provide the following information:

Subclass	Defines how the drive is attached.
Type	Specifies the type of read/write optical drive.
Parent Name	Specifies the system attachment the drive is connected to.
Where Connected	Specifies the logical address of the drive.

Enter the following command to configure the read/write optical drive:

```
mkdev -c rwoptical -s Subclass -t Type -p ParentName -w WhereConnected
```

The following is an example of a read/write optical drive that has a SCSI ID of 6, a logical unit number of zero, and is connected to the third (scsi3) SCSI bus:

```
mkdev -c rwoptical -s scsi -t osomd -p scsi3 -w 6,0 -a pv=yes
```

Method 2: Method two uses the Configuration Manager, searching the current configuration, detecting any new devices, and automatically configuring the devices. This method is used when little information is known about the read/write optical drive.

1. Use the configuration manager to configure all newly detected devices on the system (including the read/write optical drive) by typing:

   ```
   cfgmgr
   ```

2. Type the following command to list the names, location codes, and types of all currently configured read/write optical drives:

   ```
   lsdev -C -c rwoptical
   ```

3. Determine the name of the newly configured read/write optical drive using the location code that matches the location of the drive being added.

Managing Hot Plug Connectors

This section includes the following procedures for managing hot plug connectors and slots and for preparing PCI hot plug adapters to be added, removed, or replaced:

• "Displaying PCI Hot-Plug Slot Information" on page 151

For additional information about hot plug management, see PCI Hot Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Displaying PCI Hot-Plug Slot Information

Before you add, remove, or replace a hot-plug adapter, you can display the following information about the PCI hot-plug slots in a machine:

- A list of all the PCI hot-plug slots in the machine
- Whether a slot is available or empty
- Slots that are currently in use
- The characteristics of a specific slot such as slot name, description, connector type, and the attached device name

You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

For additional information, see PCI Hot-Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about hot-plug slots and connected devices:

- The **lsslot** command displays a list of all the PCI hot-plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.

Managing MPIO-Capable Devices

Beginning with AIX 5.2, you can use the Multiple Path I/O (MPIO) feature to define alternate paths to a device for failover purposes. *Failover* is a path-management algorithm that improves the reliability and availability of a device because the system automatically detects when one I/O path fails and re-routes I/O through an alternate path. All SCSI SCSD disk drives are automatically configured as MPIO devices. Other devices can be supported, providing the device driver is compatible with the MPIO implementation in AIX. For more information about MPIO concepts, see Multi-path I/O in *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

MPIO is installed and configured as part of BOS installation. No further configuration is required, but you can add, remove, reconfigure, enable, and disable devices (or device paths) using SMIT, Web-based System Manager, or the command-line interface. The following commands help manage MPIO paths:

mkpath
Adds a path to a target device.

rmpath
Removes a path to a target device.

chpath
Changes an attribute or the operational status of a path to a target device.

lspath Displays information about paths to a target device.

Cabling a SCSI Device as an MPIO Device

A SCSI device can be supported by a maximum of two adapters when configured as a MPIO-capable device. To cable a parallel SCSI device as an MPIO device, use the following simple configuration as an example. The following is the minimum configuration that must be done; your device might require additional configuration.

1. With the power off, install two SCSI adapters.
2. Cable the device to both SCSI adapters.
3. Power on the system.
4. Change the settings on one of the adapters to a unique SCSI ID. By default, SCSI adapters have a SCSI ID of 7. Because each ID must be unique, change one adapter to another number, for example, 6.
5. Run the **cfgmgr** command.
6. To verify the configuration, type the following on the command line:

   ```
   lspath -l hdiskX
   ```

   where *X* is the logical number of the newly configured device. The command output should display two paths and their status.

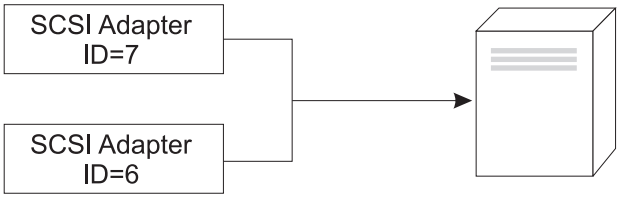


Figure 1. Cable Configuration for MPIO SCSI Device. This illustration shows cabling two SCSI adapters to the same device.

Cabling a Fibre Channel Device as an MPIO Device

A Fibre Channel device can be cabled to multiple adapters. There is no limit within the software. To cable a Fibre Channel device as an MPIO device, use the following simple configuration as an example. The following is the minimum configuration that must be done; your device might require additional configuration.

1. With the power off, install two Fibre Channel adapters.
2. Cable the adapters to a switch or hub.
3. Cable the device to the switch or hub.
4. Power on the system.
5. To verify the configuration, type the following on the command line:

   ```
   lspath -l hdiskX
   ```

   where *X* is the logical number of the newly configured device. The command output should display one path for each adapter you installed and the status of each.

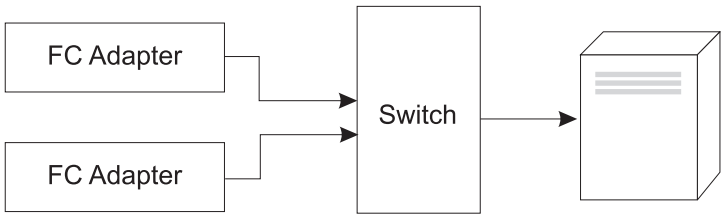


Figure 2. Cable Configuration for MPIO Fibre Channel Device. This illustration shows a simple configuration of two Fibre Channel adapters to a switch, which is cabled to a device.

Unconfiguring Communications Adapters

Before you can remove or replace a hot-plug adapter, you must unconfigure that adapter. This section provides the following procedures for unconfiguring communications adapters:

- "Unconfiguring Ethernet, Token-ring, FDDI, and ATM Adapters"
- "Unconfiguring WAN Adapters" on page 155
- "Unconfiguring Other Adapters" on page 156

Unconfiguring a communications adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing or replacing
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter's slot location
- Displaying and removing interface information from the network interface list
- Making the adapter unavailable

To perform these tasks, you must log in as **root**.

For additional information about unconfiguring communications adapters, see PCI Hot-Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

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

To unconfigure an Ethernet, Token-ring, FDDI, or ATM Adapter:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type the appropriate SMIT command, shown in the following examples, to list installed adapters and show the current state (see "Devices" on page 145) 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. To continue with this procedure, network dump locations must be disabled on the system. To look for and disable network dump locations, do the following:
   a. Type the following from a command line:

```
smit dump
```

b. Select **Show Current Dump Devices**.

c. Check whether any configured dump device shows a network location. If not, exit SMIT and you are ready for step 4. To change a dump device to a local location, select **Cancel** or press F3 and continue with the following step.

d. If the primary dump device shows a network location, change to a local location by selecting **Change the Primary Dump Device** and then enter the local location in the **Primary dump device** field.

e. If the secondary dump device shows a network location, change to a local location by selecting**Change the Secondary Dump Device** and then enter the local location in the **Secondary dump device** field.

f. When finished, click OK or press Enter.

4. Type `netstat -i` to display a list of all configured interfaces and determine whether your adapter is configured for TCP/IP. Output similar to the following displays:

```
Name  Mtu    Network   Address         Ipkts  Ierrs  Opkts Oerrs Coll
lo0   16896  link#1                      076      0    118     0    0
lo0   16896  127       127.0.0.1         076      0    118     0    0
lo0   16896  ::1                         076      0    118     0    0
tr0    1492  link#2    8.0.5a.b8.b.ec    151      0    405    11    0
tr0    1492  19.13.97  19.13.97.106      151      0    405    11    0
at0    9180  link#3    0.4.ac.ad.e0.ad     0      0      0     0    0
at0    9180  6.6.6     6.6.6.5             0      0      0     0    0
en0    1500  link#5    0.11.0.66.11.1    212      0      1     0    0
en0    1500  8.8.8     8.8.8.106         212      0      1     0    0
```

Token-ring adapters can have only one interface. Ethernet adapters can have two interfaces. ATM adapters can have multiple interfaces. For additional information, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

5. Type the appropriate ifconfig command, shown in the following examples, to remove the interface from the network interface list.

`ifconfig` *`en0`* `detach` `ifconfig` *`et0`* `detach`	To remove the standard Ethernet interface To remove the IEEE 802.3 Ethernet interface
`ifconfig` *`tr0`* `detach`	To remove a token-ring interface
`ifconfig` *`at0`* `detach`	To remove an ATM interface

For an explanation of the association between these adapters and their interfaces, see Unconfiguring Communications adapters in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

6. Type the appropriate rmdev command, shown in the following examples, to unconfigure the adapter and *keep* its device definition in the Customized Devices Object Class:

`rmdev -l ent0`	To unconfigure an Ethernet adapter
`rmdev -l tok1`	To unconfigure a token-ring adapter
`rmdev -l atm1`	To unconfigure an ATM adapter
`rmdev -p pci1`	To unconfigure the children of a PCI bus and all other devices under them while retaining their device definitions in the Customized Devices object class.

Note: To unconfigure the adapter and *remove* the device definition in the Customized Devices object class, you can use the rmdev command with the **-d** flag. *Do not* use the **-d** flag with the **rmdev** command for a hot-plug operation unless your intent is to remove the adapter and not replace it.

Unconfiguring WAN Adapters

To unconfigure a WAN Adapter:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type the appropriate SMIT command, shown in the following examples, to list installed adapters and show the current state of all the devices in the system unit:

`smit 331121b9_ls`	To list 2-Port Multiprotocol WAN adapters
`smit riciophx_ls`	To list ARTIC WAN adapters

The following naming convention is used for the different type of adapters:

Name	Adapter Type
dpmpa	2-Port Multiprotocol Adapter
riciop	ARTIC960 Adapter

3. Type `lsdev -C -c port` to list X.25 ports on your host. A message similar to the following displays:

```
sx25a0  Available 00-05-01-00     X.25 Port
x25s0   Available 00-05-01-00-00  V.3 X.25 Emulator
```

4. Close all applications that are using the adapter you are unconfiguring. To continue with this procedure, network dump locations must be disabled on the system. To look for and disable network dump locations, do the following:
   a. Type the following from a command line:
      `smit dump`
   b. Select **Show Current Dump Devices**.
   c. Check whether any configured dump device shows a network location. If not, exit SMIT and you are ready for step 4 on page 154. To change a dump device to a local location, select **Cancel** or press F3 and continue with the following step.
   d. If the primary dump device shows a network location, change to a local location by selecting **Change the Primary Dump Device** and then enter the local location in the **Primary dump device** field.
   e. If the secondary dump device shows a network location, change to a local location by selecting**Change the Secondary Dump Device** and then enter the local location in the **Secondary dump device** field.
   f. When finished, click OK or press Enter.
5. Remove an X.25 driver and port, following the steps in Configuration Commands in *AIXlink/X.25 Version 1.1 for AIX: Guide and Reference*.
6. Use the commands in the following table to unconfigure and remove the device drivers and emulator ports for these adapters:

2-Port Multiprotocol adapter	
`smit rmhdlcdpmpdd`	To unconfigure the device
`smit rmsdlcscied`	To unconfigure the SDLC COMIO emulator

For additional information, see 2-Port Multiprotocol Adapter HDLC Network Device Driver Overview in the *AIX 5L Version 5.2 System Management Guide: Communications and Networks*.

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

For additional information, see ARTIC960HX PCI Adapter Overview in the *AIX 5L Version 5.2 System Management Guide: Communications and Networks*.

Unconfiguring Other Adapters

This section includes procedures for unconfiguring adapters that require special handling.

IBM 4-Port 10/100 Base-TX Ethernet PCI Adapters: The 4-Port 10/100 Base-TX Ethernet PCI adapter has four ethernet ports and each port must be unconfigured before you can remove the adapter.

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type `smit lsdenet` to list all the devices in the PCI subclass. A message similiar to the following displays:

   ```
   ent1  Available 1N-00 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 1)
   ent2  Available 1N-08 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 2)
   ent3  Available 1N-10 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 3)
   ent4  Available 1N-18 IBM 4-Port 10/100 Base-TX Ethernet PCI Adapter (23100020) (Port 4)
   ```

3. Close all applications that are using the adapter you are unconfiguring. To continue with this procedure, network dump locations must be disabled on the system. To look for and disable network dump locations, do the following:
   a. Type the following from a command line:

      ```
      smit dump
      ```

   b. Select **Show Current Dump Devices**.
   c. Check whether any configured dump device shows a network location. If not, exit SMIT and you are ready for step 4 on page 154. To change a dump device to a local location, select **Cancel** or press F3 and continue with the following step.
   d. If the primary dump device shows a network location, change to a local location by selecting **Change the Primary Dump Device** and then enter the local location in the **Primary dump device** field.
   e. If the secondary dump device shows a network location, change to a local location by selecting**Change the Secondary Dump Device** and then enter the local location in the **Secondary dump device** field.
   f. When finished, click OK or press Enter.
4. Type `netstat -i` to display a list of all configured interfaces and determine whether your adapter is configured for TCP/IP. Output similar to the following displays:

   ```
   Name  Mtu    Network   Address         Ipkts  Ierrs  Opkts Oerrs Coll
   lo0   16896  link#1                      076      0    118     0    0
   lo0   16896  127       127.0.0.1         076      0    118     0    0
   lo0   16896  ::1                         076      0    118     0    0
   tr0    1492  link#2    8.0.5a.b8.b.ec    151      0    405    11    0
   tr0    1492  19.13.97  19.13.97.106      151      0    405    11    0
   at0    9180  link#3    0.4.ac.ad.e0.ad     0      0      0     0    0
   at0    9180  6.6.6     6.6.6.5             0      0      0     0    0
   en0    1500  link#5    0.11.0.66.11.1    212      0      1     0    0
   en0    1500  8.8.8     8.8.8.106         212      0      1     0    0
   ```

   Ethernet adapters can have two interfaces, for example, **et0** and **en0**. For additional information, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.
5. Use the ifconfig command to remove each interface from the network interface list. For example, type `iconfig en0 detach` to remove the standard Ethernet interface, and type `iconfig et0` to remove the IEEE 802.3 interface. For an explanation of the association between these adapters and their interfaces, see Unconfiguring Communications Adapters in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.
6. Use the rmdev command to unconfigure the adapter amd retain its device definition in the Customized Devices Object Class. For example, `rmdev -l ent0`.

Note: To unconfigure the adapter and *remove* the device definition in the Customized Devices object class, you can use the rmdev command with the **-d** flag. *Do not* use the **-d** flag with the **rmdev** command for a hot-plug operation unless your intent is to remove the adapter and not replace it.

ATM Adapters: Classic IP and LAN emulation protocols can run over ATM adapters. LAN emulation protocol enables the implementation of emulated LANs over an ATM network. Emulated LANs can be Ethernet/IEEE 802.3, Token-ring/IEEE 802.5, and MPOA (MultiProtocol Over ATM). You must unconfigure each LAN-emulated device before you can remove the adapter.

For instructions for removing a classical interface, see "Unconfiguring Ethernet, Token-ring, FDDI, and ATM Adapters" on page 153. To remove a LAN interface, do the following:

1. Type `lsslot -c pci` to list all the hot-plug slots in the system unit and display their characteristics.
2. Type `smit ls_atm` to list all the ATM adapters. A message similiar to the following displays:

   ```
   .
   .
   atm0 Available 04-04 IBM PCI 155 Mbps ATM Adapter (14107c00)
   atm1 Available 04-06 IBM PCI 155 Mbps ATM Adapter (14104e00)
   ```

3. Type `smit listall_atmle` to list all the LAN-emulated clients on the adapters. A message similiar to the following displays:

   ```
   ent1 Available  ATM LAN Emulation Client (Ethernet)
   ent2 Available  ATM LAN Emulation Client (Ethernet)
   ent3 Available  ATM LAN Emulation Client (Ethernet)
   tok1 Available  ATM LAN Emulation Client (Token Ring)
   tok2 Available  ATM LAN Emulation Client (Token Ring)
   ```

   All ATM adapters can have multiple emulated clients running on them.
4. Type `smit listall_mpoa` to list all the LAN-emulated clients on the adapters. A message similar to the following displays:

   ```
   mpc0 Available     ATM LAN Emulation MPOA Client
   ```

   atm0 and *atm1* are the physical ATM adapters. *mpc0* is an MPOA-emulated client. *ent1, ent2, ent3, tok1,* and *tok2* are LAN-emulated clients.
5. Type entstat to determine on which adapter the client is running. A message similiar to the following displays:

   ```
   -------------------------------------------------------------
   ETHERNET STATISTICS (ent1) :
   Device Type: ATM LAN EmulationATM Hardware Address: 00:04:ac:ad:e0:ad
   .
   .
   .
   ATM LAN Emulation Specific Statistics:
   --------------------------------------
   Emulated LAN Name: ETHelan3
   Local ATM Device Name: atm0
   Local LAN MAC Address:
   .
   .
   ```

6. Close all applications that are using the adapter you are unconfiguring. To continue with this procedure, network dump locations must be disabled on the system. To look for and disable network dump locations, do the following:
   a. Type the following from a command line:

      ```
      smit dump
      ```

   b. Select **Show Current Dump Devices**.
   c. Check whether any configured dump device shows a network location. If not, exit SMIT and you are ready for step 4 on page 154. To change a dump device to a local location, select **Cancel** or press F3 and continue with the following step.

d. If the primary dump device shows a network location, change to a local location by selecting **Change the Primary Dump Device** and then enter the local location in the **Primary dump device** field.

e. If the secondary dump device shows a network location, change to a local location by selecting**Change the Secondary Dump Device** and then enter the local location in the **Secondary dump device** field.

f. When finished, click OK or press Enter.

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
8. To unconfigure the SCSI adapter `scsi1` and all of its children while retaining their device definitions in the Customized Devices object class, type:

   ```
   rmdev  -R scsi1
   ```

   The system displays a message similar to the following:

   ```
   rmt0 Defined
   hdisk1 Defined
   scsi1 Defined
   ```
9. To unconfigure just the children of the SCSI adapter `scsi1`, but not the adapter itself, while retaining their device definitions in the Customized Devices object class, type:

   ```
   rmdev  -p scsi1
   ```

   The system displays a message similar to the following:

   ```
   rmt0 Defined
   hdisk1 Defined
   ```
10. To unconfigure the children of PCI bus `pci1` and all other devices under them while retaining their device definitions in the Customized Devices object class, type:

    ```
    rmdev  -p pci1
    ```

    The system displays a message similar to the following:

    ```
    rmt0 Defined
    hdisk1 Defined
    scsi1 Defined
    ent0 Defined
    ```

Resolving Adapter-Removal Problems

If the following type of message displays when the **rmdev** command is to unconfigure an adapter, this indicates that the device is open, possibly because applications are still trying to access the adapter you are trying to remove or replace.

```
#rmdev -l ent0
Method error (/usr/lib/methods/ucfgent):
        0514-062
 Cannot perform the requested function because the
 specified device is busy.
```

To resolve the problem, you must identify any applications that are still using the adapter and close them. These applications can include the following:

- TCP/IP
- SNA
- OSI

- IPX/SPX
- Novell NetWare
- Streams
- The generic data link control (GDLC)
  - IEEE Ethernet DLC
  - Token-ring DLC
  - FDDI DLC

Systems Network Architecture (SNA) Applications

Some SNA applications that may be using your adapter include:

- DB2
- TXSeries (CICS & Encina)
- DirectTalk
- MQSeries
- HCON
- ADSM

Streams Applications

Some of the streams-based applications that may be using your adapter include:

- IPX/SPX
- Novell NetWare V4 and Novell NetWare Services 4.1
- Connections and NetBios for this operating system

Applications Running on WAN Adapters

Applications that may be using your WAN adapter include:

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

TCP/IP Applications

All TCP/IP applications using the interface layer can be detached with the ifconfig command. This causes the applications using TCP/IP to time out and warn users that the interface is down. After you add or replace the adapter and run the **ifconfig** command to attach the interface, the applications resume.

Unconfiguring Storage Adapters

This section provides steps for unconfiguring SCSI, SSA, and Fibre Channel storage adapters.

Before you can remove or replace a storage adapter, you must unconfigure that adapter. Unconfiguring a storage adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing, replacing, or moving
- Unmounting file systems
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter's slot location
- Making parent and child devices unavailable
- Making the adapter unavailable

To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Unconfiguring SCSI, SSA, and Fibre Channel Adapters

Storage adapters are generally parent devices to media devices, such as disk or tape drives. Removing the parent requires that all attached child devices either be removed or placed in the define state.

To unconfigure SCSI, SSA, and Fibre Channel Adapters:

1. Close all applications that are using the adapter you are unconfiguring.
2. Type `lsslot-c pci` to list all the hot plug slots in the system unit and display their characteristics.
3. Type `lsdev -C` to list the current state of all the devices in the system unit.
4. Type `umount` to unmount previously mounted file systems, directories, or files using this adapter. For additional information, see “Mount a JFS or JFS2” on page 86 in the *AIX 5L Version 5.2 System Management Guide: Operating System and Devices*.
5. Type `rmdev -l adapter -R` to make the adapter unavailable.

   Attention: Do *not* use the `-d` flag with the **rmdev** command for hot plug operations because this will cause your configuration to be removed.

Unconfiguring Async Adapters

This section provides steps for unconfiguring async adapters.

Before you can remove or replace an async adapter, you must unconfigure that adapter. Unconfiguring an async adapter involves the following tasks:

- Closing all applications that are using the adapter you are removing, replacing, or moving
- Ensuring that all devices connected to the adapter are identified and stopped
- Listing all slots that are currently in use or a slot that is occupied by a specific adapter
- Identifying the adapter’s slot location
- Making parent and child devices unavailable
- Making the adapter unavailable

To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Unconfiguring Async Adapters

Before you can replace or remove an async adapter, you must unconfigure the adapter and all the devices controlled by that adapter. To unconfigure the devices, you must terminate all the processes using those devices. Use the following steps:

1. Close all applications that are using the adapter you are unconfiguring.
2. Type `lsslot-c pci` to list all the hot plug slots in the system unit and display their characteristics.
3. Type `lsdev -C -c tty` to list all available tty devices and the current state of all the devices in the system unit. For additional information, see Removing a TTY in the *AIX 5L Version 5.2 Asynchronous Communications Guide*.
4. Type `lsdev -C -c printer` to list all printer and plotter devices connected to the adapter. For additional information, see Printers, Print Jobs, and Queues for System Administrators in the *AIX 5L Version 5.2 Guide to Printers and Printing*.
5. Use the rmdev command to make the adapter unavailable.

Attention: Do *not* use the `-d` flag with the **rmdev** command for hot plug operations because this will cause your configuration to be removed.

Removing or Replacing a PCI Hot Plug Adapter

This section provides procedures for removing a PCI hot plug adapter. You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

You can remove or replace a PCI hot plug adapter from the system unit without shutting down the operating system or turning off the system power. Removing an adapter makes the resources provided by that adapter unavailable to the operating system and applications.

Replacing an adapter with another adapter of the same type retains the replaced adapter's configuration information and compares the information to the card that replaces it. The existing device driver of the replaced adapter must be able to support the replacement adapter.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Prerequisites

Before you can remove an adapter, you must unconfigure it. See Unconfiguring Communications Adapters, Unconfiguring Storage Adapters, or Unconfiguring Async Adapters for instructions for unconfiguring adapters.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about hot plug slots and connected devices and to remove a PCI hot plug adapter:

- The **lsslot** command displays a list of all the PCI hot plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.
- The **drslot** command prepares a hot plug slot for removal of a hot plug adapter. For information about using this command, see drslot in the *AIX 5L Version 5.2 Commands Reference, Volume 2*.

For information about the physical handling of a PCI hot plug adapter, refer to your system unit documentation.

Adding a PCI Hot Plug Adapter

This section provides procedures for adding a new PCI hot plug adapter.

Attention: Before you attempt to add PCI hot plug adapters, refer to the *PCI Adapter Placement Reference*, shipped with system units that support hot plug, to determine whether your adapter can be hot plugged. Refer to your system unit documentation for instructions for installing or removing adapters.

You can add a PCI hot plug adapter into an available slot in the system unit and make new resources available to the operating system and applications without having to reboot the operating system. The adapter can be another adapter type that is currently installed or it can be a different adapter type.

Adding a new PCI hot plug adapter involves the following tasks:

- Finding and identifying an available slot in the machine
- Preparing the slot for configuring the adapter
- Installing the device driver, if necessary
- Configuring the new adapter

You can complete these tasks with Web-based System Manager. You can also use SMIT or system commands. To perform these tasks, you must log in as root user.

For additional information, see PCI Hot Plug Management in the *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*.

Note: When you add a hot plug adapter to the system, that adapter and its child devices might not be available for specification as a boot device using the **bootlist** command. You might be required to reboot your system to make all potential boot devices known to the operating system.

SMIT Fastpath Procedure

1. Type `smit devdrpci` at the system prompt, then press Enter.
2. Use the SMIT dialogs to complete the task.

To obtain additional information for completing the task, you can select the F1 Help key in the SMIT dialogs.

Commands Procedure

You can use the following commands to display information about PCI hot plug slots and connected devices and to add a PCI hot plug adapter:

- The **lsslot** command displays a list of all the hot plug slots and their characteristics. For information about using this command, see lsslot in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.
- The **lsdev** command displays the current state of all the devices installed in your system. For information about using this command, see lsdev in the *AIX 5L Version 5.2 Commands Reference, Volume 3*.
- The **drslot** command prepares a hot plug slot for adding or removing a hot plug adapter. For information about using this command, see drslot in the *AIX 5L Version 5.2 Commands Reference, Volume 2*.

For information about installing or removing adapters, refer to your system unit documentation.

Determining the Cause of Device Problems

Use the following procedures to determine the cause of device problems.

Check the Device Software

Correct a device software problem by:

- “Checking the Error Log” on page 163
- “Listing All Devices” on page 163
- “Checking the State of a Device” on page 163
- “Checking the Attributes of a Device” on page 163
- “Changing the Attributes of a Device” on page 163

- “Using a Device with Another Application”
- “Defining a New Device” on page 164

Checking the Error Log:

Check the error log to see whether any errors are recorded for either the device, its adapter, or the application using the device. Go to Error Logging Facility for information about performing this check. Return to this step after completing the procedures.

Did you correct the problem with the device?

If you were not able to correct the correct the problem using the previous method, go to the next step, “Listing All Devices.”

Listing All Devices:

Use the **lsdev -C** command to list all defined or available devices. This command shows the characteristics of all the devices in your system.

If the device is in the list of devices, go to the next step, “Checking the State of a Device.”

If the device is not in the list of devices, go to “Defining a New Device” on page 164.

Checking the State of a Device:

Find the device in the list generated from the **lsdev -C** command. Check whether the device is in the Available state.

If the device is in the Available state, go to the next step, “Checking the Attributes of a Device.”

If the device is not in the Available state, go to “Defining a New Device” on page 164.

Checking the Attributes of a Device:

Use the **lsattr -E -l** *DeviceName* command to list the attributes of your device.

The **lsattr** command shows attribute characteristics and possible values of attributes for devices in the system. Refer to the documentation for the specific device for the correct settings.

If the device attributes are set correctly, go to “Using a Device with Another Application.”

If the device attributes are not set correctly, go to the next step, “Changing the Attributes of a Device.”

Changing the Attributes of a Device:

Use the **chdev -l** *Name* **-a** *Attribute*=*Value* command to change device attributes. Before you run this command, refer to *AIX 5L Version 5.2 Commands Reference*.

The **chdev** command changes the characteristics of the device you specify with the **-l** *Name* flag.

If changing the attributes did not correct the problem with the device, go to the next step, “Using a Device with Another Application.”

Using a Device with Another Application: Try using the device with another application. If the device works correctly with another application, there might be a problem with the first application.

If the device worked correctly with another application, you might have a problem with the first application. Report the problem to your software service representative.

If the device did not work correctly with another application, go to the next step, “Defining a New Device.”

Defining a New Device:

Note: You must either have root user authority or be a member of the security group to use the **mkdev** command.

Use the **mkdev** command to add a device to the system.

The **mkdev** command can either define and make available a new device or make available a device that is already defined. You can uniquely identify the predefined device by using any combination of the **-c**, **-s**, and **-t** flags. Before you run this command, refer to the *AIX 5L Version 5.2 Commands Reference*.

If defining the device did not correct the problem, You can either stop and report the problem to your service representative or use a diagnostics program to test your device.

Check the Device Hardware

Correct a device hardware problem by using the following procedures:

- “Checking the Device Connections”
- “Checking the Ready State of a Device”
- “Running Diagnostics on a Device” on page 165

Checking the Device Connections:

Follow these steps to check your device connections:

1. Check that power is available at the electrical outlet.
2. Check that the device power cable is correctly attached to the device and to the electrical outlet.
3. Check that the device signal cable is attached correctly to the device and to the correct connection on the system unit.
4. For SCSI devices, check that the SCSI terminator is correctly attached and the SCSI address setting is correct.
5. For communications devices, check that the device is correctly attached to the communications line.
6. Check that the device is turned on.

Refer to the documentation for the specific device for cabling and configuring procedures and for further troubleshooting information.

If your check of the device connections have not corrected the problem. Go to the next step, “Checking the Ready State of a Device.”

Checking the Ready State of a Device:

To determine whether the device is in a ready state, do the following:

1. Check that the device’s Ready indicator is on.
2. Check that removable media, such as tape, diskette, and optical devices, are inserted correctly.
3. Check the ribbon, the paper supply, and the toner supply for printers and plotters.
4. Check that the write medium is write-enabled if you are trying to write to the device.

Did your checks correct the problem with the device?

If your check of the device's ready state did not correct the problem, go to the next step, "Running Diagnostics on a Device."

Running Diagnostics on a Device:

You might have a defective device. Run your hardware diagnostics.

If running hardware diagnostics fails to find a problem with your device, go to "Check the Device Software" on page 162 If your device passes the diagnostic tests, you might have a problem with the way your device works with your system software. If it is possible that the preceding problem exists, report the problem to your software service organization.

Appendix. Notices

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

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

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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

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

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

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

Trademarks

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

AIX
AIX 5L
IBM
RS/6000

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

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

Index

Special characters

A

B

C

D

E

F

G

H

I

J

K

L

M

O

P

Q

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

AIX 5L Version 5.2
System Management Guide:
Operating System and Devices

Publication No. SC23-4126-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

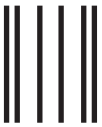
Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC23-4126-07

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department H6DS-905-6C006
11501 Burnet Road
Austin, TX 78758-3493

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

SC23-4126-07