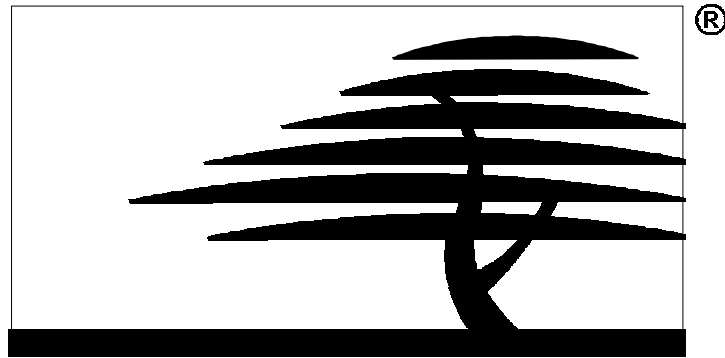




SCO

**UnixWare® 7
Administration I:
User Services**

Instructor Guide

Course Release: 2.0

For Software: UnixWare® 7

© 1987–1999 The Santa Cruz Operation, Inc. All rights reserved.

This publication is protected under copyright laws and international treaties.

Information in this document is subject to change without notice and does not represent a commitment on the part of The Santa Cruz Operation, Inc.

SCO, The Santa Cruz Operation, the SCO logos, VP/ix, SCO OpenServer, UnixWare, dbXtra, Panner, SCO Global Access, SCO MPX, SCO Doctor, SCO Doctor for Networks, SCO Doctor Lite, SCO Premier Motif, SCO Visual Tcl, SCO VisionFS, SCO ToolWare, SCO TermLite, SCO Vision 97, SCO CIFS Bridge, SCO WebTop, The Internet Way of Computing, and IWoC are trademarks or registered trademarks of The Santa Cruz Operation, Inc. in the USA and other countries. IXI, X.desktop, Deskworks, Wintif, IXI Panorama, Deskterm, and IXI Desktop are trademarks or registered trademarks of IXI Limited, a subsidiary of The Santa Cruz Operation, Inc. Visionware, Devkit.Vision, Esprit, Kodon, Super.Vision, Visionware Super.Vision, Term.Vision, Visionware Direction, the Visionware logo, Visionware SQL-Retriever, and XVision are registered trademarks of Visionware Limited, a subsidiary of The Santa Cruz Operation, Inc. SuperVision, TermVision, X-Visionware, SQL-Retriever, and Vision Builder are trademarks of Visionware Limited. UNIX is a registered trademark of The Open Group in the United States and other countries. Cheyenne and ARCServe are registered trademarks of Cheyenne Software, Inc. Netscape, Netscape Navigator, Netscape Communications Server, Netscape Commerce Server, Netscape Proxy Server, Netscape FastTrack Server, Netscape Enterprise Server, Netscape SuiteSpot, Netscape Catalog Server, Netscape News Server, Netscape Mail Server, and Netscape Navigator Gold are trademarks of Netscape Communications Corporation. NFS was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V NFS. LACHMAN is a trademark of Legent Corporation. NFS is a trademark of Sun Microsystems, Inc. TCP/IP was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V STREAMS TCP, a joint development of Lachman Associates and Convergent Technologies. MPX was developed by Corollary, Inc. VP/ix is a product developed and licensed by Phoenix Technologies, Ltd/INTERACTIVE Systems Corporation. XRemote is a registered trademark of Network Computing Devices, Inc. Oracle is a registered trademark of Oracle Corporation, Redwood City, California. Java is a trademark of Sun Microsystems, Inc. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

The SCO software that accompanies this publication is commercial computer software and, together with any related documentation, is subject to the restrictions on US Government use as set forth below. If this procurement is for a DOD agency, the following DFAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the US Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

If this procurement is for a civilian government agency, this FAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: This computer software is submitted with restricted rights under Government Contract No. _____ (and Subcontract No. _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (g)(3)(i) of FAR Clause 52.227-14 alt III or as otherwise expressly stated in the contract. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

The copyrighted software that accompanies this publication is licensed to the End User only for use in strict accordance with the End User License Agreement, which should be read carefully before commencing use of the software.



The SCO® Authorized Education class you are about to take may form part of the recommended preparation for those seeking the SCO ACE™ certification.

The SCO ACE certification program uses a series of exams to measure your ability to support and administer SCO installations with the SCO recommended skills that maximize system performance. As a certified SCO ACE graduate, you earn all of the respect that the industry accords to each certified member of the extended SCO support team. When professionals in the computer industry see your SCO ACE certification, they know that you have passed demanding SCO testing requirements. This certification is the foundation for mastering real-world UNIX® systems, including those from other vendors.

Important!

When registering for any SCO ACE exam at a Sylvan Prometric™ testing center, please quote the course release number on the front of the ***Student Guide*** that the exam covers. This number corresponds to the version number of the SCO ACE exam for that course.

Ask your SCO Authorized Instructor, or call SCO for more information about SCO Certification.

Table of Contents

Lesson 1: Course Introduction	1-1
Introduction.....	1-3
Course goal and purpose.....	1-3
Target audience	1-3
Student Materials	1-6
The Student Guide	1-6
Job aids	1-6
SCO documentation.....	1-6
Typographical Conventions	1-8
Using scoadmin (1M)	1-10
Sample exam items	1-12
 Lesson 2: Using SCO Administration Tools	 2-1
Using SCOadmin	2-7
Accessing SCOadmin	2-7
Starting individual managers	2-9
Using the Character Motif (CHARM).....	2-11
Describing the Screen Areas of SCOadmin	2-13
Menus.....	2-13
Control buttons	2-13
Display area	2-13
Status line.....	2-13
Graphical mode.....	2-13
Character mode	2-15
Locating Topics in SCO Documentation	2-17
Overview of printed documentation	2-17
Overview of online documentation.....	2-17
Using SCOhelp	2-18
Searching in SCOhelp.....	2-19
Using the manual pages	2-21
Using the SCO support library.....	2-21
Using SCO's Online Support (SOS) System	2-22
Newsgroups	2-22
Other resource sites.....	2-23
Technical support	2-23
Using the root and System Owner Account.....	2-24
Maintaining a System Log.....	2-25
Lesson Summary.....	2-26
Relevant Commands and Files	2-28
Answers to Exercise and Review Questions.....	2-29

Lesson 3: Administering User Accounts	3-1
Analyzing User Account Requirements	3-6
User ID.....	3-6
Login	3-7
Security profiles and password settings.....	3-9
Login Shell.....	3-11
Home directory	3-13
Groups.....	3-13
Creating a group.....	3-15
Changing the default login group	3-17
Changing the login locale	3-17
Reviewing permissions	3-19
Default Discretionary Access Control (DAC)	3-21
Login environment.....	3-23
System environment files.....	3-24
Creating User Accounts	3-25
Creating a default account	3-27
Creating an account using modified defaults.....	3-28
Creating user accounts with useradd(1M)	3-31
Deleting Users.....	3-33
Managing user files.....	3-33
Deleting users	3-34
Modifying Accounts	3-36
Modifying individual account information.....	3-36
Using usermod(1M).....	3-37
Deactivating a Login.....	3-38
Modifying an individual account environment.....	3-38
Modifying the umask of a single account	3-38
Modifying user passwords	3-39
Controlling password expiration.....	3-39
Controlling password options with default files	3-40
Managing User Groups	3-42
Modifying group membership	3-42
Deleting a group.....	3-42
Setting Login Attempt Restrictions	3-43
Login restriction parameters for user accounts.....	3-45
Locking and unlocking a user account	3-46
Using Account Activity Reports.....	3-48
Reporting password status	3-48
Reporting login activity	3-49
Troubleshooting User Accounts.....	3-50
Fixing forgotten or compromised passwords.....	3-50
Fixing an incorrect terminal type.....	3-50
Lesson Summary.....	3-51
Lab: Creating Groups.....	3-53

Overview	3-53
Procedure	3-55
Lab: Creating New Users.....	3-56
Overview	3-56
Procedure	3-57
Relevant Commands and Files	3-58
Answers to Exercises and Review Questions	3-60
 Lesson 4: Managing Processes	 4-1
Describing a Process	4-6
Definitions	4-6
The process table	4-6
Viewing current processes	4-7
Process genealogy	4-9
Foreground and background processes	4-9
Daemon processes.....	4-9
Defunct processes	4-10
Terminating Processes	4-11
The kill (1) command	4-11
Using the kill (1) command	4-11
Managing Processes with the Process Manager	4-13
Viewing processes on a system.....	4-13
Deleting processes	4-16
Scheduling Tasks	4-17
Setting the system date and time.....	4-17
Using the Task Scheduler.....	4-18
Deleting scheduled tasks.....	4-20
Modifying System Tasks.....	4-21
Lesson Summary.....	4-22
Lab: Scheduling Processes.....	4-23
Overview	4-23
Relevant Commands and Files	4-25
Answers to Exercises and Review Questions	4-26
 Lesson 5: Working with Filesystems	 5-1
Describing Filesystem Basics	5-7
Using Different Filesystem Types.....	5-8
Default <i>vxfs</i> features.....	5-9
Mounting and Unmounting a Filesystem.....	5-11
Describing filesystem information.....	5-11
Adding the mount configuration.....	5-12
Mounting a filesystem	5-14
Why mounting can fail	5-14
Unmounting a filesystem	5-15
Repairing a Non-root Filesystem	5-16

Causes of filesystem corruption.....	5-16
The <i>lost+found</i> directory	5-16
Repairing a non-root filesystem manually	5-16
Monitoring Filesystems	5-19
Determining filesystem free space.....	5-19
Determining the size of a directory.....	5-21
Determining disk usage by user	5-23
Locating and Managing User Files	5-24
Finding large files	5-24
Finding files by owner	5-24
Finding and removing <i>core</i> files	5-24
Managing System Log Files and Temporary Directories	5-26
Clearing key system logs	5-26
Using the System Logs Manager	5-27
Clearing key temporary directories.....	5-27
Lesson Summary	5-28
Lab: Working with a Floppy Disk Filesystem	5-30
Overview.....	5-30
Procedure	5-31
Relevant Commands and Files	5-33
Answers to Exercises and Review Questions	5-34

Lesson 6: Working with Disks and Tapes
6-1

Working with Floppy Disks	6-7
Identifying floppy device names.....	6-7
Formatting a floppy disk.....	6-9
Working with Tape Drives	6-10
Identifying tape device names	6-10
Working with tapes	6-11
Transferring Data to Tape or Disk	6-12
Absolute versus relative pathnames.....	6-12
Transferring symbolically linked files	6-13
The tar (1) command.....	6-15
The cpio (1) command.....	6-21
Copying Data to DOS filesystems	6-23
Lesson Summary	6-24
Lab: Creating an Archive and Extracting Selected Files	6-25
Overview.....	6-25
Procedure	6-26
Relevant Commands and Files	6-28
Answers to Exercises and Review Questions	6-29

Lesson 7: Backup Administration	7-1
Organizing and Maintaining Filesystem Backups	7-6
Deciding when to back up filesystems	7-6
Storing backup media	7-6
Maintaining backup logs	7-7
Describing ARCserveIT Products	7-8
System requirements	7-9
Licensing ARCserveIT	7-9
Installing ARCserveIT	7-9
Configuring ARCserveIT	7-10
Starting ARCserveIT	7-10
Stopping ARCserveIT services	7-11
Accessing ARCserveIT	7-13
Exiting ARCserveIT	7-14
Setting up user profiles	7-14
Creating a user	7-15
Accessing Tape Device(s)	7-17
Selecting devices and device views	7-17
Maintaining Media	7-19
Ejecting a tape	7-21
Using compression	7-21
Backing up files and filesystems	7-23
Expanding and object	7-23
Viewing filesystems and files	7-24
Performing a system backup	7-27
Backing up filesystems	7-28
Backing up selected files	7-29
Monitoring the status of a backup	7-31
Backup filter options	7-31
Backup method	7-32
Backup schedule	7-32
Placing backup jobs on hold	7-33
Saving backup jobs as scripts	7-33
Verifying the backup and checking logs	7-37
Scanning media	7-37
Viewing Reports and Logs	7-37
Restoring files and filesystems from backups	7-41
Browsing media	7-41
Performing a Basic Restore Job	7-42
Restore filter options	7-43
Lesson Summary	7-44
Relevant Commands and Files	7-45
Answers to Review Questions	7-46

Lesson 8: Managing Printers	8-1
Managing the Print Service.....	8-6
Describing the print service	8-6
Stopping the print service	8-7
Starting the print service	8-9
Accepting and Rejecting Print Jobs	8-11
Rejecting print jobs	8-11
Accepting print jobs	8-12
Disabling and Enabling Printers	8-14
Disabling a printer	8-14
Enabling a printer.....	8-14
Managing Print Jobs	8-17
Viewing print jobs.....	8-17
Deleting print jobs	8-19
Holding print jobs	8-20
Moving print jobs.....	8-21
Viewing and Changing Printer Settings.....	8-25
Setting the default printer	8-25
Setting a default printer for a user	8-25
Controlling access to a printer	8-27
Preventing banner pages	8-29
Troubleshooting Printer Problems	8-30
Lesson Summary	8-31
Lab: Managing Printers	8-33
Overview	8-33
Procedure	8-34
Relevant Commands and Files	8-35
Answers to Exercises and Review Questions	8-36
 Lesson 9: Stopping and Starting the System	 9-1
Stopping a UnixWare 7 System	9-7
Normal shut down.....	9-8
Other shut down circumstances	9-10
Starting a UnixWare 7 System.....	9-11
Autoboot to network state.....	9-11
Other boot options	9-11
Switching Between System States.....	9-14
Lesson Summary.....	9-15
Relevant Commands and Files	9-16
Answers to Exercises and Review Questions	9-17

1

Course Introduction

Instructor Guide

Lesson 1

Course Introduction

1.1 Introduction

The *UnixWare 7 Administration I: User Services* course is designed for individuals who need to perform routine system administration tasks on a daily basis. The target audience includes support technicians, developers, engineers, system administrators, and other technical users who require the ability to perform standard system administration tasks.

1.1.1 Course goal and purpose

At the conclusion of this course, you should be able to perform the tasks and duties associated with the routine operation of a UnixWare 7 system. These tasks include technical procedures such as supporting user accounts and user processes, maintaining filesystems and backing up their data, managing printers, and performing system startups and shutdowns.

1.1.2 Target audience

This class is aimed at system operators, developers, engineers, support technicians, system administrators and other technical users who require an understanding of front line system administration. Students are likely to have a wide variety of backgrounds in XENIX® or UNIX®, but must have prerequisite skills equal to or exceeding those provided in the *Introduction to SCO UNIX Systems* course.

Course schedule

This course takes three days to complete. A suggested lesson duration is specified at the beginning of each lesson in this Instructor Guide.

The labs included in this course must be completed in order to meet course objectives.

Suggestions for practice exercises are also included throughout the course. Ample time is allotted to each lesson to allow for the completion of these exercises.

Equipment

The following equipment should be installed in a classroom to support 14 students:

- 14 (7 if shared) Intel Pentium PC microprocessors containing:
 - A UNIX partition of at least 500MB.
 - An additional 500 MB hard disk (minimum) for each system for user files and applications
 - A minimum of 64MB of RAM in each system. This is required for ARCserveIT.
 - A 1GB (or larger) primary disk
 - A 3.5 inch diskette drive
 - A CD-ROM drive
 - A Super VGA monitor capable of least 800x600 resolution
 - A serial, bus, or PS/2-compatible mouse
 - A Quarter-Inch Cartridge (QIC), Digital Linear Tape (DLT), or 4mm tape device. If you cannot supply a tape drive on all classroom machines, have at least one machine with a SCSI tape device. The exercises on ARCserveIT require one SCSI device.
- One liquid crystal display (LCD) unit, VGA projector, or large-screen display monitor
- White board with markers
- Overhead projector

Training materials

The following training materials are used in this course:

Instructor Guide, Transparencies, and Student Guide

The IG also contains notes which are instructional aids and a course GIF transparency disk.

You can present graphics to the students with the GIF files rather than by projecting slides made with the transparency masters. Benefits of the GIF files include:

- They can be projected in full color rather than greyscale, as they appear in the workbook.

- There is no added cost of creating acetate transparencies.
- The GIF files do not deteriorate over time as acetate slides can.

You can display the GIF files with a variety of UNIX or Microsoft® Windows utilities, including, but not limited to, the following:

- xv—UNIX-based public domain graphics viewer
- Microsoft PowerPoint®—Windows-based presentation product

You can copy and rename the files for sequential viewing.

Software

The UnixWare 7.1 Enterprise System is used in this course.

The *Instructor Guide*

The *Instructor Guide* (*IG*) is organized to include:

- Instructor notes are intermingled with text in the *Student Guide* (*SG*) allowing the instructor to easily refer to section content.
- Page numbers in the *IG* do not correspond to those in the *SG*, however the heading numbers do.
- Cross references to other sections within the course materials are included within the text. These cross references generally include the section number or AV number, the section name, and page number. The page number is almost always different in the *SG* than the *IG*; however, the other components are the same.

The *IG* also contains notes which are instructional aids, including:

AV 1-1: Slide Title

These notes explain the instructional objective of every transparency. The AV number cross references to the number that appears above every slide in the workbook.

IG Notes provide extra information not presented in the *Student Guide*.

1.2 Student Materials

The contents of the box containing your student materials are yours to keep and write notes in. Your instructor may have other reference materials in the classroom for your use while attending this class. Please do not take or write in these materials as they will be needed again for later classes.

1.2.1 The *Student Guide*

The instructor notes contain all of the material that is presented in the Student Guide. The SG contains references to other materials, including SCO documentation.

The *Student Guide* contains:

- Outline of presentation
- Copies of all transparencies

1.2.2 Job aids

Job aids are designed to assist you in performing on-the-job administration and as references to other helpful materials. This course includes the *vi Quick Reference Guide*, a card that provides a list of the most commonly used **vi**(1) commands and their functions.

1.2.3 SCO documentation

This course references the online and printed documentation included with UnixWare 7.

Lesson plan

Each lesson follows a similar approach, or methodology, in the delivery of instruction:

- The suggested lesson duration and instructor preparation notes are provided at the beginning of each lesson when applicable.
- The lesson begins with an overview transparency of the major topics and a list of the lesson objectives.
- The lesson continues with the presentation of lesson topics and the demonstration of lesson tasks.
- Exercises, which allow the students to practice discrete tasks, appear throughout the presentation.

- References appear where appropriate.
- The lesson content concludes with a summary. Use this to reinforce the topics and tasks covered. You should also refer to the objectives that were presented at the beginning of the lesson.
- Following the content of most lessons are summary exercises, which consist of review questions and labs. The review questions help you determine how well the students understood the content, and the labs allow students to apply the material that they learned.

1.3 Typographical Conventions

This publication presents commands, filenames, keystrokes, and other special elements as shown here:

lp or lp(1)	Commands, device drivers, programs, and utilities (names, icons, or windows); the letter in parentheses indicates the reference manual section in which the command, driver, program, or utility is documented
<i>/new/client.list</i>	Files, directories, and desktops (names, icons, or windows)
root	System, network, or user names
<i>arg</i> or <i>arg</i>	Placeholders (replace with appropriate name or value)
[<i>arg</i>]	Surrounds an <i>option</i> or <i>cmdarg</i> that is not mandatory
<i>arg</i> ...	Indicates multiple occurrences of the <i>option</i> or <i>cmdarg</i>
\$	Command line prompt for commands executable from the Bourne shell by any user
#	Command line prompt for commands only executable by the super user from the root account
	Keyboard keys
 	Press  and  keys simultaneously
  	Press all three keys,  ,  , and  , simultaneously
 d	Press  key. With  still depressed, also press  .
 0240	Press  key. With  still depressed, also press and release in sequence  ,  ,  , and  .
 Q + i	Press  key. With  still depressed, also press  . Release both keys and press  .
 Q + I	Press  key. With  still depressed, also press  . Release both keys and press   .
Exit program?	System output (prompts, messages)

tar tv	User input, such as on a command line
“Description”	Field names or column headings (on screen or in database)
Cancel	Button names
Edit	Menu names
Copy	Menu items
File ⇨ Find ⇨ Text	Sequences of menus and menu items
open or open(2)	Library routines, system calls, kernel functions, C keywords; the letter in parentheses indicates the reference manual section in which the file is documented
\$HOME	Environment or shell variables
SIGHUP	Named constants, signals, and kernel parameters
“adm3a”	Data values
<i>employees</i>	Database names and tables
buf	C program structures
b_b.errno	Structure members

1.4 Using **scoadmin(1M)**

Many procedures in this course indicate to “start the **Account Manager**” or “run **scoadmin(1M)**” when invoking administration utilities.

UnixWare 7 includes both graphical and character-based versions of most administration utilities. When started from the Desktop, the graphical versions automatically run. When started from a character device (such as a terminal), the character versions run.

In this course, the Desktop is used to start the graphical versions of administration utilities. There are several ways to run **scoadmin(1M)** utilities.

Demonstrate the different ways to access the **SCOadmin** managers. Show students that “selecting” a manager, requires a “double click.”

For example, to run the **Account Manager**, a tool that allows you to create and manage users:

- From the **SCOadmin** icon, select ⇨ **Account Manager**.
- From a terminal window, enter **scoadmin Account Manager**.
- From the command line, enter **scoadmin Account Manager**.

When you are directed to “run the **Account Manager**” (or “start the **Account Manager**” later in this guide, you can use any of these methods.

Be sure you are logged in as **root**.

Classroom setup

When setting up the classroom:

- Install the necessary software, including the operating system and the class software on all systems.
- Configure classroom equipment, your own display, and the LCD.

Lesson preparation

When preparing for each lesson:

- Read the pre-lesson preparation prior to each lesson. Complete any tasks listed in the preparation.
- Read the lesson thoroughly before teaching. Add any additional notes or exercises.
- Read through the appropriate sections of the SCO documentation in support of the lesson topics.
- Review the system files in each lesson to which students need access, and change the file permissions to make the files readable if necessary.

1.5 Sample exam items

The following questions are representative exam items on the SCO ACE certification exam for this course. Being able to correctly answer these questions does not guarantee that you will be able to pass the actual exam.

1. When creating a user account, what login shell is assigned by default?
 - A. The Bourne shell
 - B. The C shell
 - C. The Korn shell
 - D. The SCO shell
2. What types of processes perform system tasks on a periodic basis and sleep between those tasks?
 - A. Child processes
 - B. Daemon processes
 - C. Foreground processes
 - D. Zombie processes
3. What filesystem feature can reduce the system downtime incurred when cleaning a large filesystem?
 - A. Access control lists
 - B. Data compression
 - C. Intent logging
 - D. Extent based allocation

4. Which system log file contains account records?
- A. `/etc/wtmp`
 - B. `/etc/syslogd`
 - C. `/etc/motd`
 - D. `/usr/adm/syslog`
5. Which device file represents a floppy device?
- A. `/dev/xct0`
 - B. `/dev/vt02`
 - C. `/dev/dsk/f03ht`
 - D. `/dev/c1s0`
6. Which command can you use to send a job to a printer?
- A. **accept(1)**
 - B. **enable(1)**
 - C. **lp(1)**
 - D. **lpsched(1M)**

Answers to sample exam items

1. C
2. B
3. C
4. A
5. C
6. C

2

Using SCO Administration Tools

Instructor Guide

Instructor Guide

Lesson 2

Using SCO Administration Tools

Suggested lesson duration

This lesson should take approximately 1 hour to complete. This lesson has no lab.

Pre-lesson classroom preparation

Have a sample set of the hard copy documentation that ships with UnixWare 7 available for students to review. Verify that the Verity documentation indexing process has been run on each of the student systems. Refer to the **config_search(1M)** manual page for details on documentation indexing.

Instructor preparation

When preparing for this lesson:

- Review the **scoadmin(1M)** manual page.
- Practice accessing the graphical and character versions of the **scoadmin(1M)** managers.
- Practice using the **scohelp(X1)** browser interface.
- Visit the SCO World Wide Web Page technical support area at <http://www.sco.com/support/>.

AV 2-1

Using SCO Administration Tools

- Use **scoadmin**(1M)
- Locate topics in SCO documentation
- Identify other sources of information
- Describe the importance of the superuser and owner accounts
- Maintain a system log

sa1g-0201

© The Santa Cruz Operation, Inc.

Introduction

A system administrator is responsible for performing a wide variety of tasks. This course focuses on the most common tasks involved in the routine administration of a UnixWare 7 system.

Objectives

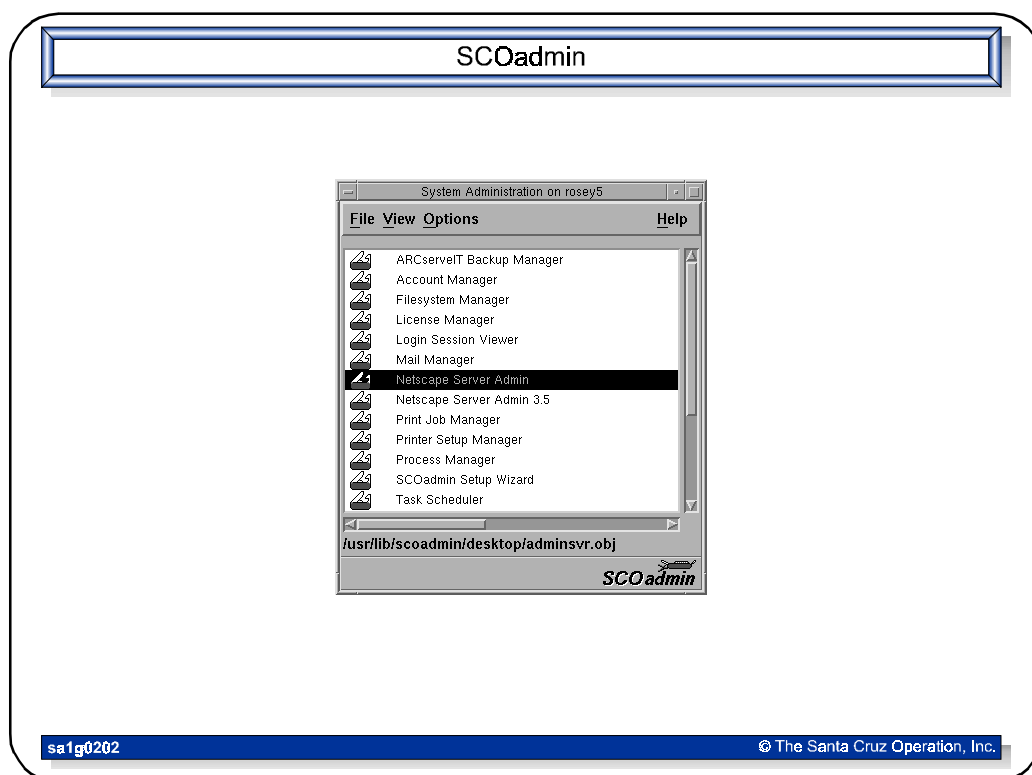
This lesson introduces a system administrator's responsibilities and the available tools and resources. By the end of this lesson you will be able to:

- Use **scoadmin(1M)**
- Locate topics in SCO documentation
- Identify other sources of information
- Describe the importance of the **root** and system owner accounts
- Maintain a system log

AV 2-1: Using SCO Administration Tools

This slide describes the overall topics covered in this lesson.

AV 2-2



2.1 Using SCOadmin

AV 2-2: SCOadmin

The Graphical Scoadmin Manager Interface.

Most of the system administration tasks described in this course can be accomplished using **scoadmin**(1M), SCO's system administration and configuration tool. This tool consists of a series of managers that support a graphical interface. Many of the **SCOadmin** managers are available in a character interface, but the methods of navigation differ.

2.1.1 Accessing SCOadmin

Show students how to select a manager. Double-click on the manager.

You can use either one of these methods to access the **SCOadmin** managers from your CDE desktop:

- Step 1. Log in as **root** using the graphical login.
- Step 2. Click on the arrow above the **SCO logo** icon from the **Main Panel** of your desktop.
- Step 3. Click on **SCOadmin**.
- Step 4. Select a manager. Double-click on the manager name.
- Step 5. Exit the manager. Select **Host** ⇨ **Exit**.
- Step 6. Exit **SCOadmin**. Select **File** ⇨ **Exit**.

Exercise: Accessing a SCOadmin manager.

Access the **SCOadmin Account Manager** by following the steps under Section 2.1.1, "Accessing SCOadmin," on page 2-7.

From the command line while in the desktop, use the second method:

- Step 1. Open a graphical terminal window. From the **Main Panel**, click on the arrow above the **Personal Applications** icon. Click on **Terminal**.

- Step 2. Enter **scoadmin&**. The **&** allows you to continue to use your terminal window for other commands. More details on this capability are discussed in Lesson 4, “Managing Processes.”
- Step 3. Select a manager.

2.1.2 Starting individual managers

You can also start individual managers by using the **scoadmin(1M)** command with the application name. For example, to start the **Account Manager** from a desktop **Terminal** window, enter:

```
scoadmin account manager&
```

List the available managers, enter:

```
scoadmin -t
```

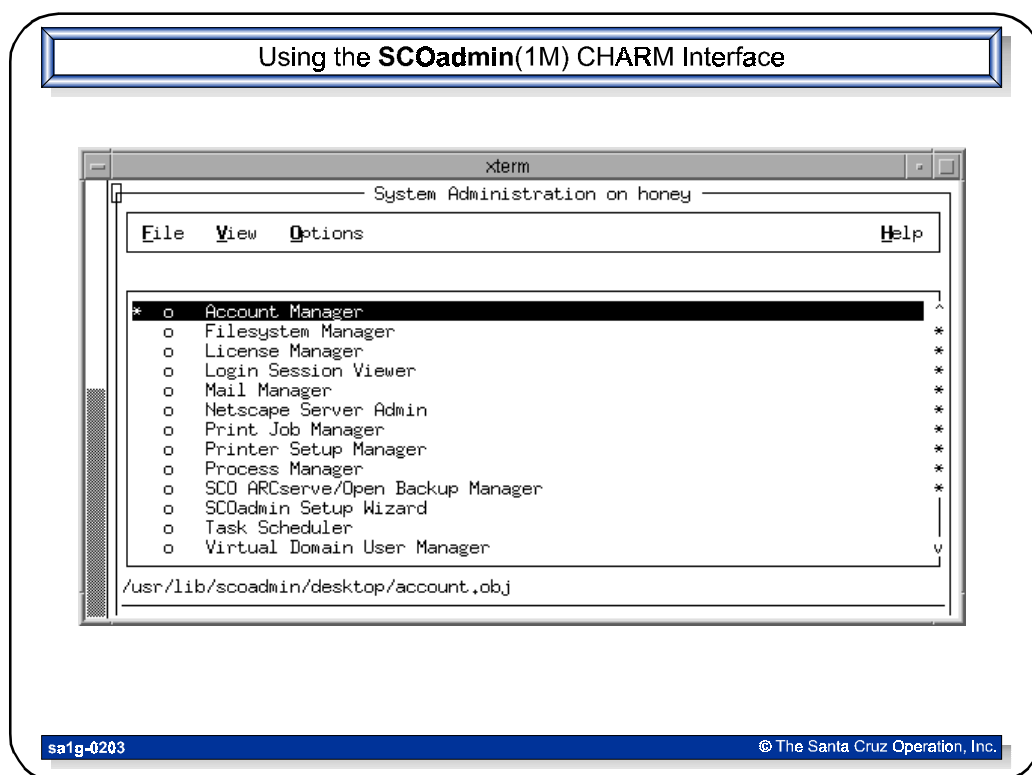
Note that you do not have to enter the full manager name. A minimum number of characters is accepted. For example, to run the **Account Manager**, enter:

```
scoadmin A&
```

Exercise: Starting an individual manager

Start the **SCOadmin Process Manager** from a **Terminal** window. Refer to the second method under Section 2.1.2, “Starting individual managers,” on page 2-9.

AV 2-3



2.1.3 Using the Character Motif (CHARM)

AV 2-3: CHARM SCOadmin Managers.

This is a view of the **scoadmin(1M)** CHARM interface. This screen shot was taken by first running `rlogin -u root machine_name` to create an Xterm window that will run a CHARM session. By default a graphical session of **scoadmin(1M)** is invoked from an Xterm window.

You can also access **SCOadmin** using the Character Motif (CHARM) interface by switching from your desktop to a console screen. This is also useful if you are accessing **SCOadmin** from a terminal. Follow these steps to access the **SCOadmin** managers using the CHARM interface:

Step 1. Switch from the desktop to a console screen. Press:



Step 2. Log in as **root**. Enter the password.

Step 3. Enter **scoadmin**. Select the manager.

Step 4. Press  ⇒ **Host** ⇒ **Exit** to exit the manager.

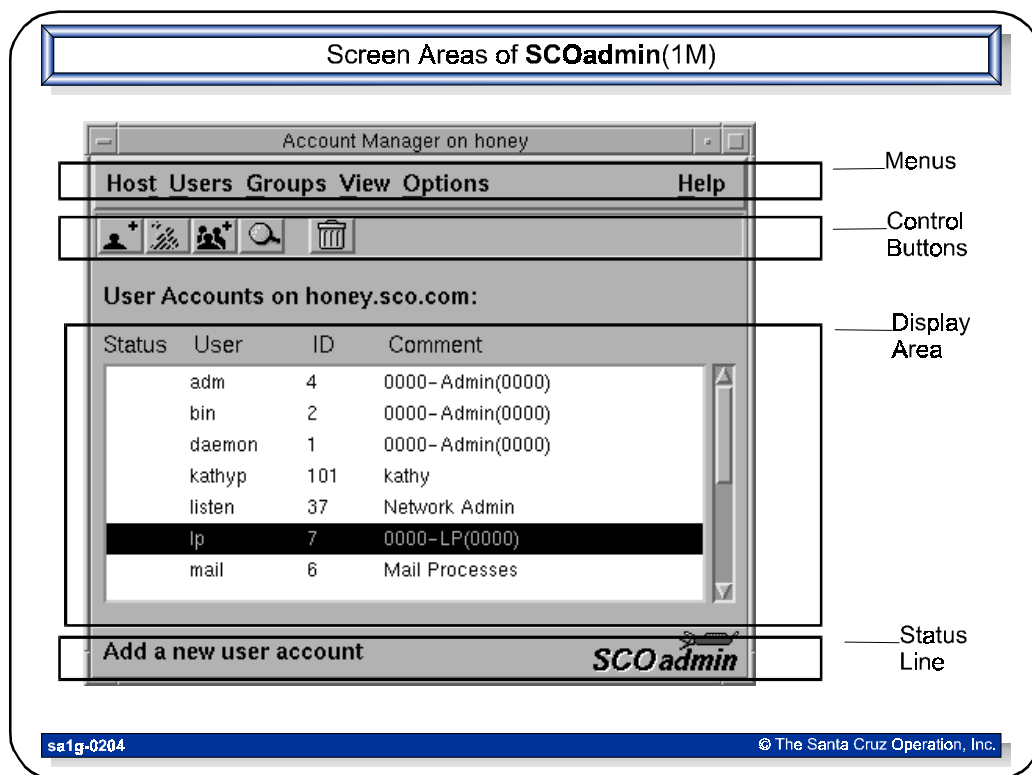
Step 5. Press  ⇒ **File** ⇒ **Exit** to exit the **SCOadmin** manager.

Step 6. Press    to return to the desktop.

Exercise: Starting the SCOadmin character interface

Start and stop the **SCOadmin** character interface. Follow the steps under Section 2.1.3, “Using the Character Motif (CHARM),” on page 2-11.

AV 2-4



2.2 Describing the Screen Areas of SCAdmin

AV 2-4: Graphical SCAdmin Manager

The graphical **SCAdmin** manager. Point out the menus, the toolbar, the data area, and the quick help.

In each **SCAdmin** manager, there are four distinct areas of the window.

2.2.1 Menus

Located at the top of the window, the menu provides access to the various administration tasks supported by that manager. For example, the **Host** menu lets you select a remote system to control and the **Help** menu allows you to access context-sensitive online help.

2.2.2 Control buttons

Control buttons appear in the data area, typically at the top. They provide shortcuts to the menu options or allow you to configure additional options for a particular manager.

2.2.3 Display area

This section contains the system elements that each manager supports. For example, the display area of the **Account Manager** lists user accounts, and the display area of the **Filesystem Manager** lists mounted filesystems.

2.2.4 Status line

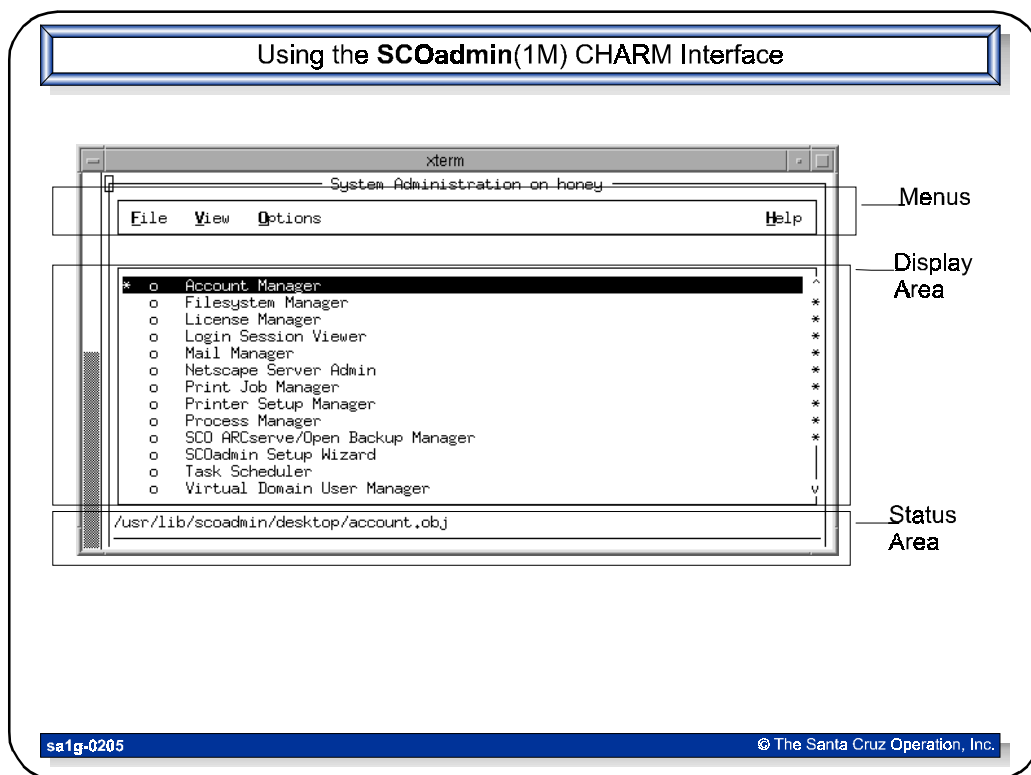
At the bottom of the screen is a status line. The default behavior of the manager is to list a brief explanation of the currently selected menu option or button. If you find the default behavior distracting, select **Options** ⇨ **Point Help** to disable the display.

2.2.5 Graphical mode

These are general guidelines for using the administration managers in graphical mode:

- Use the mouse to switch between the various screen areas.
- Select a menu by clicking on it. A drop down menu appears. Execute an option by clicking on it.

AV 2-5



- Switch between options within a particular screen area by using the arrow keys.
- Activate buttons by clicking on them.
- Select a particular element in the display area by clicking on it.

2.2.6 Character mode

AV 2-5: CHARM SCOadmin Manager

Screen shot of a CHARM **SCOadmin** manager. Show that both the graphical and CHARM versions have identical options and layout. The Character Motif (CHARM) version of **SCOadmin** follows the Motif style guide.

The character mode version of **scoadmin(1M)** is based upon the Character Motif (CHARM) interface. It executes some of the same managers as the graphical version, so the layout of the data and menu options are similar. Instead of using a mouse, you can use these keys to navigate through the interface:

- Use  to switch between the various screen areas. You can also press  to go to the menu.
- Use  on a menu to open the drop-down menu. Use  and  to select a menu option. Press  to execute a menu option.
- Activate a button by selecting it, then pressing  or .
- Select a particular element in the display area by using the arrow keys to highlight it, then press  or .
- Use the  key to cancel a drop down menu.

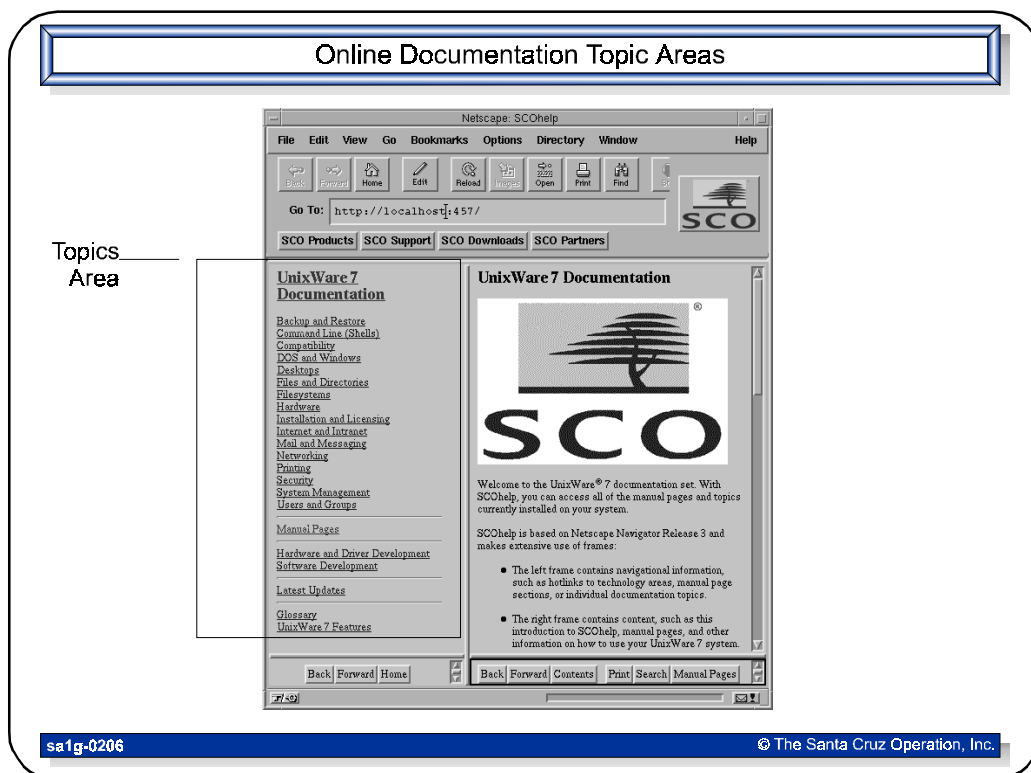
While in any character based **SCOadmin** manager, use the  to list the “Charm Navigation and Select Keys.” help screen.

Exercise: Using SCOadmin to change the system time.

Follow the steps under Section 2.1.1, “Accessing SCOadmin,” on page 2-7 and access the **System** ⇨ **System Time Manager**. If necessary, change the time.

AV 2-6

Instructor Guide



2.3 Locating Topics in SCO Documentation

SCO provides comprehensive documentation covering the use of its systems. This documentation is packaged online as part of the product. Some of the documentation is available in printed form. This section provides an overview of this documentation so that you can easily locate topics to find the answers to your questions.

2.3.1 Overview of printed documentation

The printed documentation includes:

- ***UnixWare 7 Installation Guide***
- ***UnixWare 7 Runtime Release Notes***
- ***UnixWare 7 System Handbook***

The topics in the ***UnixWare 7 System Handbook*** are also included with the online documentation.

2.3.2 Overview of online documentation

AV 2-6: Topic Areas

Use this slide to demonstrate what topics are available.

The online documentation is organized differently than in previous releases of the SCO operating system.

SCOhelp(X1) is divided into four frames.

Top left	Table of contents
Top right	Topic area
Bottom left	Buttons for controlling the content of the frame
Bottom right	Buttons for controlling the topic frame, search, and manual pages

Rather than accessing information through books or guides, you can access it by *topics* or subject areas.

2.3.3 Using SCOhelp

■ The SCOhelp browser is now Netscape Communicator 4.08.

Use **SCOhelp(X1)** to access the online documentation set. The **SCOhelp(X1)** browser is Netscape Communicator[™]. For more information on the browser, refer to **SCOhelp** ⇒ **UnixWare 7** ⇒ **New Features** ⇒ **Release 7.1 new features**.

From the desktop, you can start **SCOhelp** in one of three ways:

1. Click on the arrow above the **SCOhelp** icon. This icon is available from the CDE front panel. It is the icon with a question mark in the middle. Select **SCOhelp**.
2. Open a terminal window from the Desktop. Enter:

scohelp&

scohelp cannot be accessed from a character terminal. Use the online **man(1)** pages.

3. Click on **Help** in any SCO application window.

The enhanced features of **SCOhelp** for UnixWare 7 include:

- A new frames interface
- New organization of topics (or subject areas)
- Enhanced print functionality
- Ability to open a specific manual page
- Buttons for navigation
- The ability to search for both words and phrases using the Verity Search Engine

2.3.4 Searching in SCOhelp

■ Remind students, this command has been run on their classroom systems.

SCOhelp uses a powerful search engine powered by Verity. After the installation of all software and documentation, you can create a search index using the **config_search(1M)** command. This process can be run in the background and takes up to an hour.

To create a search index from the command line, enter:

```
/usr/man/bin/config_search -f&
```

Exercise: Using SCOhelp(X1)

From the desktop, run **SCOhelp**.

Under which topic would you find *user administration* documentation?

Search for the word *printer*. Which topic provides the information to install a printer?

AV 2-7

Manual Page Section Mapping

UnixWare 7 manual pages have a main section name, an optional prefix, and an optional suffix. The main names are:

- 1 Unrestricted commands, which can be run by any user.
- 1M Administrative commands, whose options may be fully or partially restricted to the root or owner accounts.
- 2 System calls.
- 3 Library routines.
- 4 System files.
- 5 Miscellaneous.
- 7 Device drivers and driver interfaces.

Prefixes are X (for X windows system commands) and D (for driver development commands). For example, section X1M contains X windows administrative commands, and section D3 contains kernel utility functions.

A variety of suffixes subdivide the sections further, to allow for logical groupings of manual pages by technology and to enable easy scanning. Examples include section 1nfs (Unrestricted NFS commands) and 3M (Library math routines).

sa1g-0207

© The Santa Cruz Operation, Inc.

2.3.5 Using the manual pages

You can access the manual pages in **SCOhelp**:

- From the Verity Search Engine, click on the **Manual Pages** button at the bottom of the right frame. Enter the command name.
- From the left frame of the “home” topic view (if you are not in the home view, click on the **Home** button at the bottom of the frame):
 - Click on **Manual Pages**.
 - Select a section (for example, **Unrestricted commands**, **Administrative commands**, or **TCP/IP administrative commands**).
 - Click on the command name.

AV 2-7: Manual Page Section Mapping

This table shows the UnixWare 7 manual page sections.

Exercise: Locating the shutdown(1M) manual page

Use the **Manual Pages** button to locate the manual page for the **shutdown(1M)** command.

For additional information on **SCOhelp(X1)**, refer to **scohelp** ⇒ **Desktops** ⇒ **Using SCOhelp**.

2.3.6 Using the SCO support library

SCO’s Technical Support group keeps technical bulletins describing how to fix various problems the group has encountered. You can purchase this collection of bulletins for your own reference. These bulletins are grouped by major product functions, and you can conduct a key word search to locate help on specific problems.

This library also includes a hardware compatibility handbook, various supplemental software patches (SLS), and extended feature supplements (EFS) that you can install to enhance the functionality of an SCO system.

2.3.7 Using SCO's Online Support (SOS) System

SOS is a menu driven BBS program that provides a character-based, front-end for ease of use for those who do not have a Web browser or Internet access.

SCO's Online Support (SOS) system contains similar information to that available on WWW.

The required software or hardware to access SOS, include:

- Terminal and modem
- Computer, modem, and third-party communications package
- **cu**(1bnu) command (for SCO XENIX® and SCO UNIX® systems)

Note: To download supplemental patches, your third-party communications package must support XMODEM, YMODEM, ZMODEM, or kermit transfer protocols.

2.3.8 Newsgroups

If you have access to the Internet, you can find many technical newsgroups where users share tips and information. Communicate with a wide range of users and find someone who has encountered, or solved, a problem similar to yours.

SCO-specific newsgroups include:

- comp.unix.sco.announce
- comp.unix.sco.misc
- comp.unix.sco.programmer
- comp.unix.unixware.announce
- comp.unix.sco.announce
- comp.unix.unixware.misc

For information about these newsgroups check the technical support area on the SCO WWW Page:

<http://www.sco.com/company/netnews.html>

2.3.9 Other resource sites

Mention that students must have an Internet connection to be able to access either SCO's World Wide Web or FTP sites. Similarly, students must have an account on CompuServe to be able to access SCOFORUM.

In addition to newsgroups, SCO also sponsors:

Home page on the World Wide Web

Provides a graphical interface to browse SCO's technical scripts and download patches. Access <http://www.sco.com/>.

FTP sites

Download patches using File Transfer Protocol (FTP). If you do not have a Web browser, you can download patches from these sites. Access <ftp.sco.com> and <sosco.sco.com>.

CompuServe

SCOFORUM

2.3.10 Technical support

You can also receive one-on-one help through the Technical Support services offered by SCO or its authorized partners. These professionals can help you solve problems you might encounter while administering the system.

2.4 Using the root and System Owner Account

Every UNIX system has an account for system administration. It is known as the **root** account and:

- Can read any file
- Can write or delete any file
- Can execute and terminate any user program

Because there are no restrictions to this account, you can potentially delete major portions of the system. Use the **root** account only when necessary and be careful when you are using it. Use your regular login account when you are not performing system duties.

For those of you who are administering your systems using **SCOadmin** from the desktop, some administration tasks can be performed by using the *system owner* account. A user is designated as the system owner during system installation and is given the authority to perform day-to-day system administration tasks available through **SCOadmin**. These tasks include:

- Shutting down the system
- Administering users, printers, filesystems, and networking
- Changing system tunables and monitoring system resources

2.5 Maintaining a System Log

When troubleshooting a system, one of the most valuable tools available is a current system log. This book should be kept next to the system and should contain the following types of information:

- All system modifications, including hardware and software configuration information
- All system problems encountered, including detailed summaries of the causes and solutions
- Statistics describing system use, performance, and growth

2.6 Lesson Summary

There are many resources available to you as an administrator. Administration tools and documentation come with the system to support your job. For the most current information and more extensive support, you can turn to technical libraries, other users, or SCO Technical Support.

Review questions

1. List the steps to start the **SCOadmin Process Manager** from a **Terminal** window.

The steps to start the SCOadmin Process Manager from a terminal window are: Log into the CDE desktop as root. Click on the Personal Applications icon. Select Terminal. Enter: scoadmin pro.

2. Which option to the **scoadmin(1M)** command would you use to display the available **SCOadmin** managers?

The option to list the available SCOadmin managers is scoadmin -t.

3. Which menu selection in each of the **scoadmin(1M)** managers allows you to turn off the Status Line?

The menu selection in each of the scoadmin(1M) managers that allows you to turn off the Status Line is the Options § Point Help menu selection.

4. List three methods to access SCOhelp.

Three methods to access SCOhelp are: click on the arrow above the SCOhelp Manager icon, enter scohelp(X1) from a Terminal window, or select Help from any SCO application window.

5. What is the major difference between the **root** and system owner account when performing system administration?

The major difference between the root and owner account when performing system administration is that the owner account cannot perform system administration from the command line.

6. Should the system log be kept online? Why or why not?

The system log should not be kept online. If the system crashes to the point where you cannot boot, you need to be able to access a hard copy log.

2.7 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

man(1)	Displays manual pages
scoadmin(1M)	Invokes SCOadmin managers
scohelp(X1)	Displays documents, manual pages, and context sensitive help

Relevant files

<i>/etc/default/man</i>	Default configuration file for the use of man(1)
-------------------------	---

2.8 Answers to Exercise and Review Questions

This section provides the answers to exercises and review questions presented in this lesson.

Exercise: Using scoadmin(1M) to change the system time

- Step 1. Log in as **root** using the graphical login.
- Step 2. Start **SCOadmin**. Select **System** ⇒ **System Time Manager**.
- Step 3. Change the time. Select **Host** ⇒ **Set Time**.
- Step 4. Accept the time. Click on **OK** twice.
- Step 5. Exit the **System Time Manager**. Click on **Host** ⇒ **Exit**.
- Step 6. Exit **SCOadmin**. Click on **File** ⇒ **Exit**.

Exercise: Using SCOhelp

User administration is found under the User and Group topic.

The topic entitled “Adding, modifying, or copying a local printer “ is found when you click on 2 in more results.

Exercise: Locating the shutdown(1M) manual page

- Step 1. Click on **Manual Pages**.
- Step 2. Type shutdown in the top box.
- Step 3. Click on **Search**.

Review questions

1. The steps to start the **SCOadmin Process Manager** from a terminal window are: Log into the CDE desktop as **root**. Click on the **Personal Applications** icon. Select **Terminal**. Enter: **scoadmin pro**.

2. The option to list the available **SCOadmin** managers is `scoadmin -t`.
3. The menu selection in each of the **scoadmin(1M)** managers that allows you to turn off the Status Line is the **Options** ⇨ **Point Help** menu selection.
4. Three methods to access **SCOhelp** are: click on the arrow above the **SCOhelp Manager** icon, enter `scohelp(X1)` from a **Terminal** window, or select Help from any SCO application window.
5. The major difference between the **root** and owner account when performing system administration is that the owner account cannot perform system administration from the command line.
6. The system log should not be kept online. If the system crashes to the point where you cannot boot, you need to be able to access a hard copy log.

3

Administering User Accounts

Instructor Guide

Instructor Guide

Lesson 3

Administering User Accounts

Suggested lesson duration

This lesson should take approximately 2 hours to complete, including the lab exercises.

Pre-lesson classroom preparation

Install the classroom system using Traditional security so that students are able to activate and deactivate user accounts. Unless otherwise noted, the students should be logged into the system as **root**.

Create three (3) user accounts using the defaults. Name these accounts **user1**, **user 2** and **user3**. Students are instructed to create a new group in Section 3.1.7, "Creating a group," on page 3-15. They will add two users to the new group. The third user is deleted in Section 3.3.2.3, "Using the `userdel(1M)` command," on page 3-35.

Instructor preparation

For background information on this lesson, review **scohelp** ⇒ **Users and Groups**. For **Account Manager** enhancements, refer to **scohelp** ⇒ **UnixWare 7 Features** ⇒ **Release 7.1 New features** ⇒ **System administration** ⇒ **Users and groups**.

AV 3-1

Instructor Guide

Administering User Accounts

- Analyze user account requirements
- Create, modify, and delete user accounts
- Manage user groups
- Set, change, and remove login and password restrictions
- Create and use account activity reports
- Troubleshoot user accounts

sa1g-0301© The Santa Cruz Operation, Inc.

Introduction

The main task of any system administrator is to support the use of computer resources by users. Before a user can use a UnixWare 7 system, the user must have an account on the system. The system administrator's job includes creating accounts for users and maintaining these accounts by changing user environments, passwords, and group membership, as necessary.

Objectives

This lesson demonstrates the creation and management of user accounts and groups. By the end of this lesson, you will be able to:

- Analyze user account requirements
- Create, modify, and delete user accounts
- Manage user groups
- Set, change, and remove login and password restrictions
- Create and use account activity reports
- Troubleshoot user accounts

AV 3-1: Administering User Accounts

This slide describes the overall topics covered in this lesson.

3.1 Analyzing User Account Requirements

Before a user can log into and use the system, you must create an account for that user. A user account is more than a login ID; it sets up the user's basic working environment and access privileges for the system.

A little planning can simplify account management. Most users probably share similar requirements with regards to access privileges. Others might have special needs. Setting up system-wide account defaults saves time when creating and maintaining accounts. This section addresses issues to consider before creating user accounts.

3.1.1 User ID

■ Instruct students to run the **id(1)** command.

The User ID, or UID, is a unique number that identifies each user. It can be assigned by the system or by the administrator. The suggested minimum UID for individual accounts is 100. The suggested maximum UID is 60000.

Use the same UID to identify a specific person on all systems to which the person has access.

The **id(1)** command displays the user name and user ID and the group name and group ID for a user. It also displays any other group names and IDs to which a user belongs.

3.1.2 Login

The login is the account name entered at the `login:` prompt. It must be unique for each user on the system. The maximum length is 254 characters. For compatibility with all system utilities and other UNIX platforms, the suggested length is between 3-8 characters.

The login name:

An account using the maximum characters can cause problems with NIS. In addition, the `ftp(1tcp)` command supports accounts up to a maximum of only 50 characters.

- Should not contain upper case letters
- Cannot contain a colon character (:)
- Cannot start with a number

As with the User ID, use the same login to identify a specific person on all systems.

AV 3-2

Password Settings and Security Profiles

Low	Passwords are not required.
Traditional	Passwords are required. The minimum length is three (3) characters.
Improved	Passwords are required. The minimum length is six (6) characters.
High	Passwords are required. The minimum length is eight (8) characters.

sa1g-0302

© The Santa Cruz Operation, Inc.

3.1.3 Security profiles and password settings

AV 3-2: Password Settings and Security Profiles

This graphic shows the default password settings as determined by the security profiles.

Before a user can log into the system, the user account should have an assigned password. Password restrictions are based upon the security profile of the system, but you can also modify password expiration parameters for an individual user.

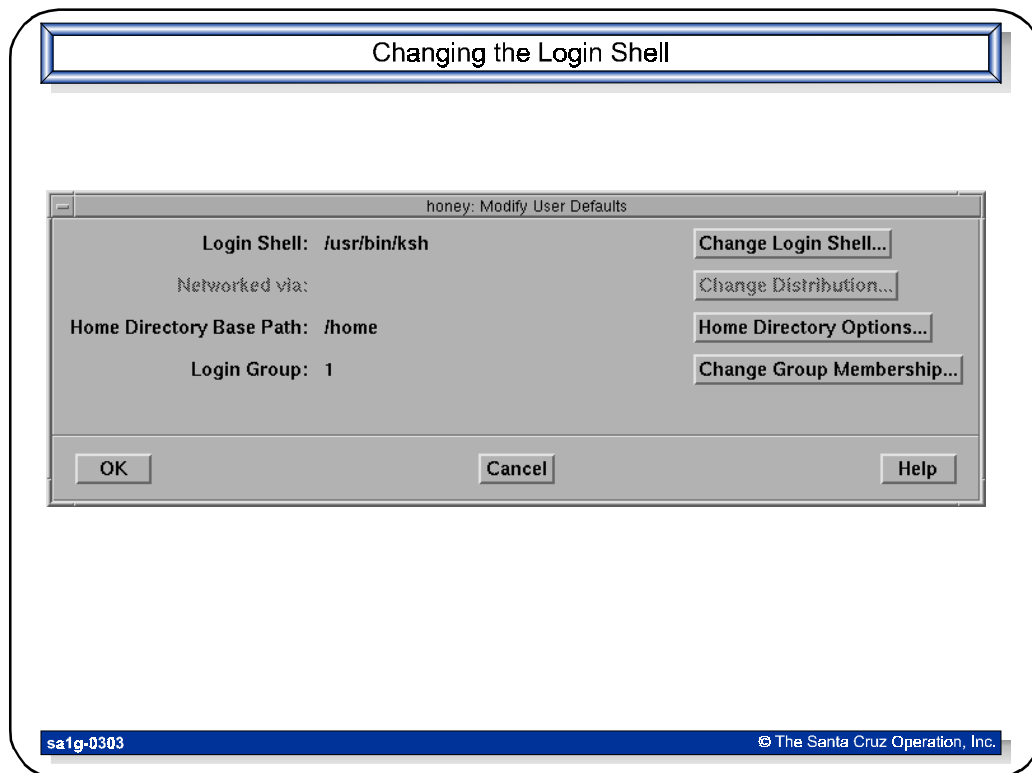
The security profile determines password length. Security profiles are found in the `/etc/security/seclevel/*/etc_def` files. Explain to students that the security profile can be changed after installation, however it is not covered in this class. Try to keep your discussions of the security profile related to password and login restrictions.

The security profile is chosen during the installation of your system. The four security profiles are:

Low	Passwords are not required.
Traditional	Passwords are required. The minimum length is three (3) characters.
Improved	Passwords are required. The minimum length is six (6) characters.
High	Passwords are required. The minimum length is eight (8) characters.

Unless your system is set to Low security, no one can access the system without a valid account name and password.

AV 3-3



3.1.4 Login Shell

AV 3-3: Changing the Login Shell

In addition to changing the login shell, remind students that the user ID ranges can be changed.

The *login shell* is the command shell the user sees immediately after login. The default shell is the Korn shell (ksh), but the default also can be set to any of these shells:

- Restricted Bourne Shell or Bourne Shell with Job Control
- Korn, Restricted Korn Shell, or the Windowing Korn Shell
- C Shell

Use these steps to change the login shell for account creation:

Step 1. Start **SCOadmin** ⇒ **Account Manager**.

Step 2. Select **Options** ⇒ **User Defaults**.

Note the login shell, home directory, and login group.

Step 3. Select **Change Login Shell**, select the new login shell, then click on **OK** to return to the main defaults window.

Step 4. Click on **OK** twice to exit the **User Defaults** window and proceed with the change.

Step 5. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

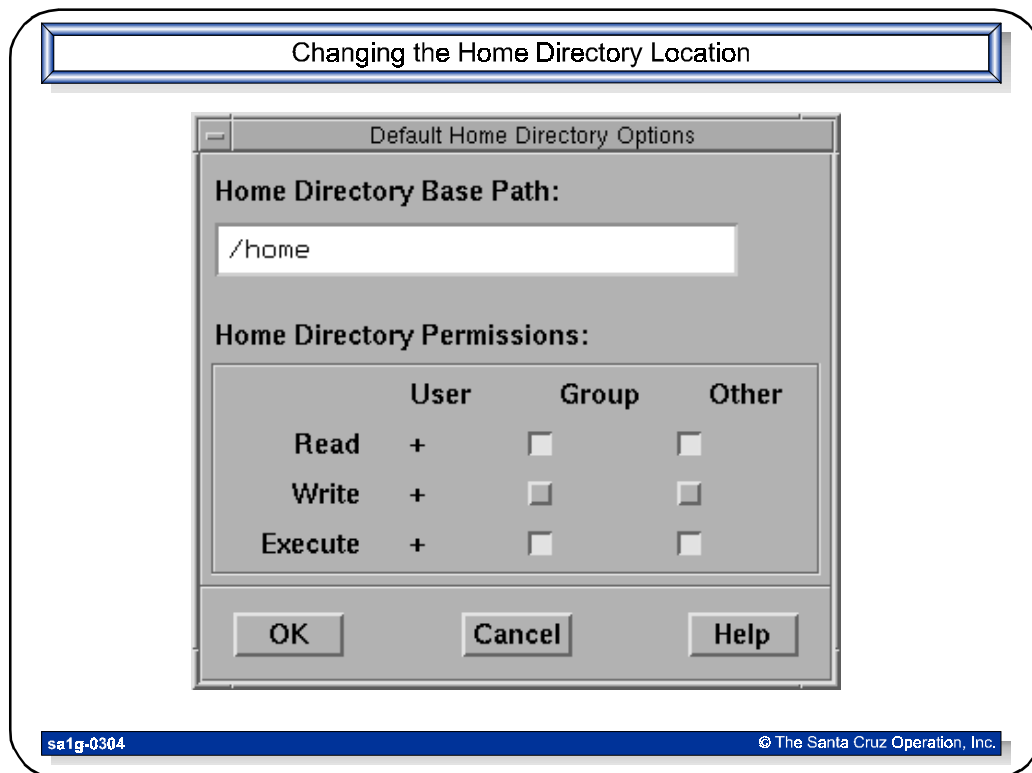
Any defaults changed affect only the creation of new user accounts. Existing accounts are not affected.

This exercise lets students begin using the **SCOadmin Account Manager**.

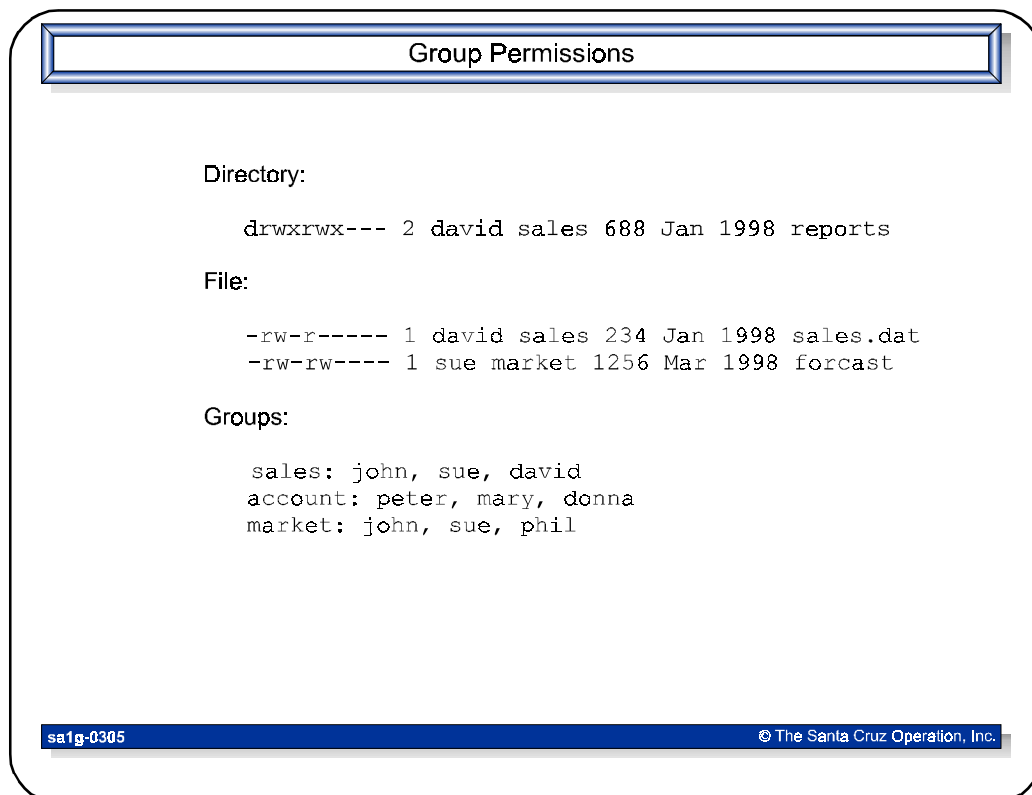
Exercise: Setting the default login shell

On your classroom system, change the default login shell to the Bourne shell. If necessary, refer to the steps under Section 3.1.4, “Login Shell,” on page 3-11.

AV 3-4



AV 3-5



3.1.5 Home directory

AV 3-4: Changing the Home Directory Location

Explain to students that the default permissions on the home directory are determined by the security profile. Show students that you can provide additional security by changing the defaults.

Because the concept of filesystems has not yet been introduced, using separate filesystems for user home directories is not covered in this section.

The *home directory* is the user's "work space" on the system and the directory where most of the user's files are stored. By default, this directory is */home/login_name*.

In some environments, groups of users share a single home directory. In that case, the directory name should reflect the group, not an individual user.

From the **SCOadmin Account Manager**, change the default home directory location by selecting **Options** ⇒ **Users Defaults** ⇒ **Home Directory Options**.

3.1.6 Groups

Groups allow sets of users to share files. The group permissions on a file or directory determine whether members of a group can access them. This allows work groups to share files and still restrict access to sensitive data.

The maximum number of groups that a user can be in at one time is 16. This limit is controlled by the Process Limit Parameter, `NGROUPS_MAX` tuneable kernel parameter.

A user can be a member of several groups simultaneously, and can access any file or directory that is within that user's group set, if group permissions allow. By default, files created by a user have the group ID of that user's login group.

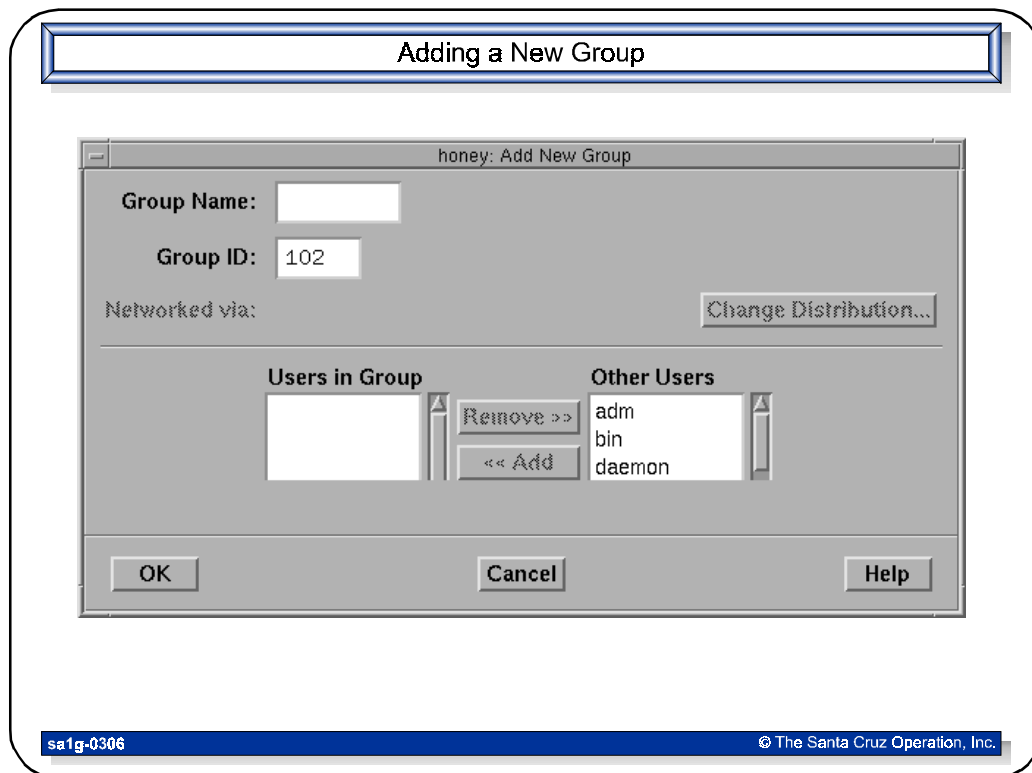
AV 3-5: Group Permissions

Use this graphic with the "Reviewing group permissions" exercise to demonstrate how group membership affects access to files and directories.

Exercise: Reviewing group permissions

Refer to the lower graphic on the adjoining page. Who can read and write to the file *sales.dat*? Who can read and write to the file *forecast*?

AV 3-6



Instructor Guide

As with User ID, and login names, each group should have the same group name and group ID on all systems in the organization.

3.1.7 Creating a group

AV 3-6: Adding a New Group

Show students how a new group is created and how users can be added to the group.

These steps describe how to create a new group:

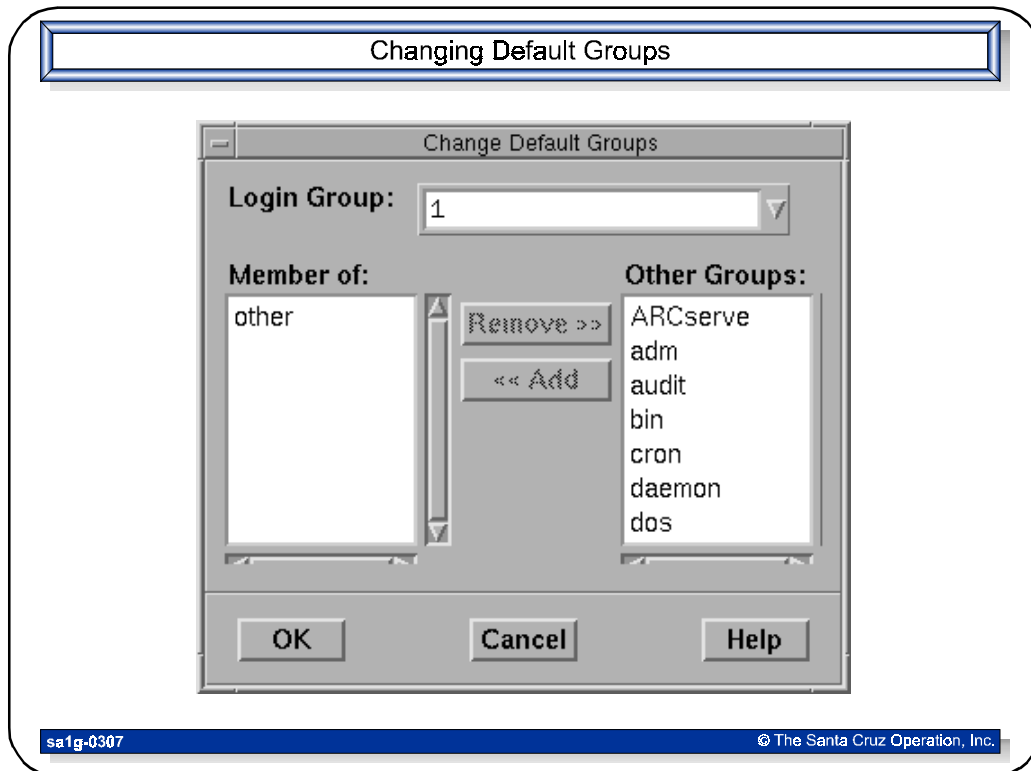
- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select **Groups** ⇒ **Add New Group**.
- Step 3. Enter a group name of 3-8 characters.
- Step 4. Accept the default Group ID or enter a new one.
- Step 5. Add users to the group. Select them from the **Other Users** list and select **Add**. Remove users from the group. Select them from the **Users in Group** list and select **Remove**.
- Step 6. Click on **OK** to create the group.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

This exercise gives students practice creating groups and adding users to them.

Exercise: Creating a group

Using the steps under Section 3.1.6, “Groups,” on page 3-13, create a new group called *class*. Add **user1** and **user2** to the *class* group.

AV 3-7



Instructor Guide

3.1.8 Changing the default login group

AV 3-7: Default Login Group

Screen shot of the **Account Manager** "Modify User Defaults" screen, emphasizing the default login group.

If the majority of users belong to a specific group, you might want to set that group to be the default login group. On a newly installed system, *other* is the default login group.

These steps describe how to change the default login group for new users:

- Step 1. Start SCOadmin. Select **Account Manager**.
- Step 2. Select **Options** ⇒ **User Defaults**.
- Step 3. Click on **Change Group Membership**.
- Step 4. Enter or Select the login group. When entering a new group, you are prompted to create the new group.
- Step 5. Click on **OK** to accept changes.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

This exercise asks the students to set the default login group. Emphasize that changing this setting does not affect existing user accounts.

Exercise: Modifying the default login group

Change the default login group to *class*. Will this change an existing account's login group?

3.1.9 Changing the login locale

Locales define the system's language and country environment. The default (C locale) refers to an United States English environment. The system-wide locale is chosen during installation. If multiple language supplements are installed, you can select a different locale. Changing the locale determines how some prompts display.

AV 3-8

Changing Permissions

Each permission is assigned a number:

read = 4 write = 2 execute = 1

Add these numbers for each user category:

	OWNER	GROUP	OTHER
-	r w -	r - -	r - -
	4 2	4	4
	6	4	4

Use with chmod(1):

\$ chmod 644 filename

sa1g-0308

© The Santa Cruz Operation, Inc.

3.1.10 Reviewing permissions

AV 3-8: Changing Permissions

This graphic reviews the use of absolute values with **chmod(1)**. This sets up the review for **umask(1)**.

Each file and directory has permissions for three categories of users:

User	The owner of the file
Group	Members of a designated group
Other	Other users

Users can change the permissions of files and directories that they own. Permissions are set with the **chmod(1)** command. This command includes numeric options for setting permissions:

Read	4
Write	2
Execute	1

Add these numbers to determine the permission for the owner, group, or others. This number sequence is known as the file's *mode*.

For example, to set the permissions for the */etc/motd* file, enter:

```
chmod 664 /etc/motd
```

The resulting file permissions are:

```
-rw-rw-r--
```

In this example:

- Owner permissions = read (4) + write (2) = 6
- Group permissions = read (4) + write (2) = 6
- Other permissions = read (4) = 4

AV 3-9

Instructor Guide

Default Discretionary Access Control		
Directories:	(7) (7) (7)	
Unrestricted permissions:	drwxrwxrwx	
— umask 022	0 2 2	
Permissions of new directories	drwxr-xr-x	
	(7) (5) (5)	
Ordinary files:	(7) (7) (7)	
Unrestricted permissions:	-rwxrwxrwx	
— umask 022	0 2 2	
— No execute permission	---x---x---x	
Permissions of new files	-rw-r--r--	
	(6) (4) (4)	

sa1g-0309 © The Santa Cruz Operation, Inc.

3.1.11 Default Discretionary Access Control (DAC)

When a file or directory is created, it is set with default permissions defined by the system. Typical permissions are:

For files `-rw-r--r--`

For directories `drwxr-xr-x`

If a group of users shares a common set of directories and files, you can change the default permissions for users within that group. For example, you might want the default permissions to grant write permissions to all members within the group.

3.1.11.1 Review of umask(1)

AV 3-9: Default Discretionary Access Control

This graphic shows how **umask(1)** works on both files and directories.

Default DAC is set with the **umask(1)** command. This command specifies which permissions to *withhold*.

Point out that for ordinary files, you will not get execute permission, regardless of the **umask** value. If the umask value is 023, permissions for a new directory will be 754 (`drwxr-xr--`), whereas for an ordinary file, they will be 644 (`-rw-r--r--`). Some instructors suggest that you can easily determine the permissions for an ordinary file by subtracting the umask from 666. *This does not work reliably!* It would imply that the umask 023 would yield 643 (`-rw-r--wx`), which is *not* correct. You must first subtract from 777 and then also remove any execute permission that might result.

For example, to set the default permissions:

Owner All permissions (none excluded)

Group All permissions (none excluded)

Others Read (r) and search (x) permissions (write excluded)

Use this command:

umask 002

Given these defaults, new files are set to the mode 664 (`-rw-rw-r--`), and new directories are set to mode 775 (`drwxrwxr-x`).

3.1.11.2 Modifying system-wide umask(1) defaults

Without any **umask** setting, permissions are completely open on both new files (-rw-rw-rw-) and new directories (drwxrwxrwx). An initial **umask** is defined in */etc/profile* and */etc/cshrc*. These files are discussed in Section 3.1.13, “System environment files,” on page 3-24.

The default **umask** in these files is determined by the security profile of the system:

Low and Traditional	022
Improved and High	077

To modify this setting, edit the appropriate environment file.

This exercise reviews how **umasks** are set. You can illustrate these situations by setting a **umask**, creating a new file and directory, then listing the permissions for them.

Exercise: Setting umasks

Situation 1: Set up the Bourne and Korn shell system-wide **umask** so that only the owner has permissions to view or modify a file, or change into a directory. What are the permissions for any new file created? For any new directory?

Situation 2: Set up the C shell system-wide **umask** so that only the owner can modify a file or directory, but everyone can read or execute. What are the permissions for any new file created? For any new directory?

Note that many third-party applications set their own **umask**, so the permissions on files created with those applications may not reflect the system or user's **umask**.

3.1.12 Login environment

When the system creates a user's home directory, it populates the directory with the appropriate startup files for the login shell. These files set the user's working environment, including the system prompt, the command search path, and other environment variables.

You can modify the system-wide default startup files to match the needs of your users. Listed below are some of the changes commonly made:

- Adding a variable identifying a default printer for the user
- Modifying the user's search path
- Modifying the user's default terminal settings

3.1.12.1 Default account startup files

When creating users with the **Account Manager**, regardless of the shell type, all files are copied from */usr/lib/scoadmin/account/skel* to the user's home directory.

When creating users with the **useradd(1M)** command, files are copied from the */etc/default/usradd* directory. If additional files are placed into the */etc/skel* directory, they are also copied to the user's home directory.

When you create an account using the **SCOadmin Account Manager**, default account startup files are copied from */etc/profile* file and the */usr/lib/scoadmin/account/skel* directory.

These files can contain default environment settings for the:

- Terminal type
- Search path
- Mail folder

3.1.13 System environment files

In addition to the default account files, these system environment files are executed before executing the user startup file:

/etc/profile Executed for both the Bourne and Korn shells

/etc/cshrc Executed for C shells

These files are configured by default to:

- Create the user's umask value
- Inform the user if there is unread mail waiting in the mailbox

3.2 Creating User Accounts

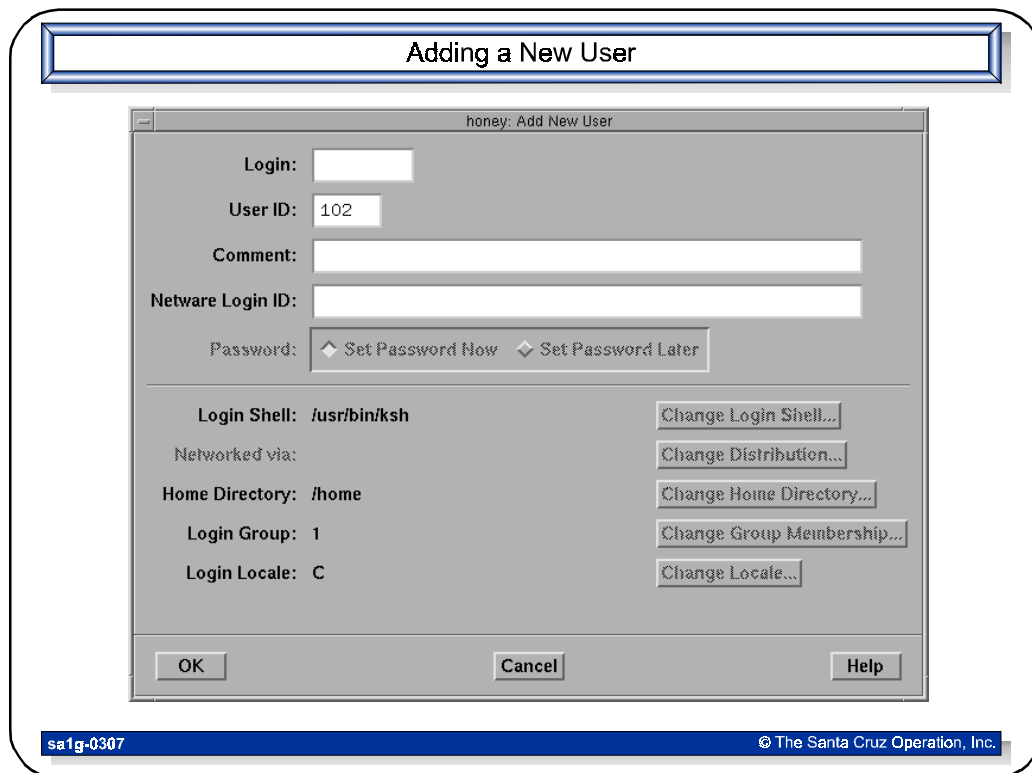
If students are sharing a system, remind them that they cannot create the same account. Have each of them create different account names.

When a new person requires access to the system, you must create a user account. You can either accept the default account, or modify some of the account parameters. You can also set the password for the new account to avoid unauthorized access.

After using the system for a while, a user might want to use a different login shell or belong to different groups. Some users might forget their account passwords. In those cases, you can modify the current account settings.

User accounts can be managed from either the **SCOadmin Account Manager** or the command-line interfaces.

AV 3-10



3.2.1 Creating a default account

AV 3-10: Adding a New User

Using this slide, briefly discuss the purpose of the NetWare login ID and Networked Via fields.

These steps describe how to create a user account using system defaults:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select **Users** ⇨ **Add New User**.
- Step 3. Enter a login name. Accept the UID.
- Step 4. Enter information about the user into the **Comment** field. You can enter information about this user, such as full name, department, and extension.
- Step 5. Accept the defaults for the remaining fields.
- Step 6. Select **Set password now**.

Note that, if you select **Set password later**, the user cannot log in until you set the initial password.

- Step 7. Click on **OK** to continue.

The system prompts you to set the initial password for the account.

- Step 8. Do one of the following:
 - Set the password; the system prompts you to enter the password twice.
 - Remove a password if the security profile allows. This lets a user login without a password. It is not recommended.
- Step 9. Select whether or not you want to force the user to change the password at the first login.
- Step 10. Click on **OK**. The system creates the user account.
- Step 11. Select **Host** ⇨ **Exit** to exit the **Account Manager**.

3.2.2 Creating an account using modified defaults

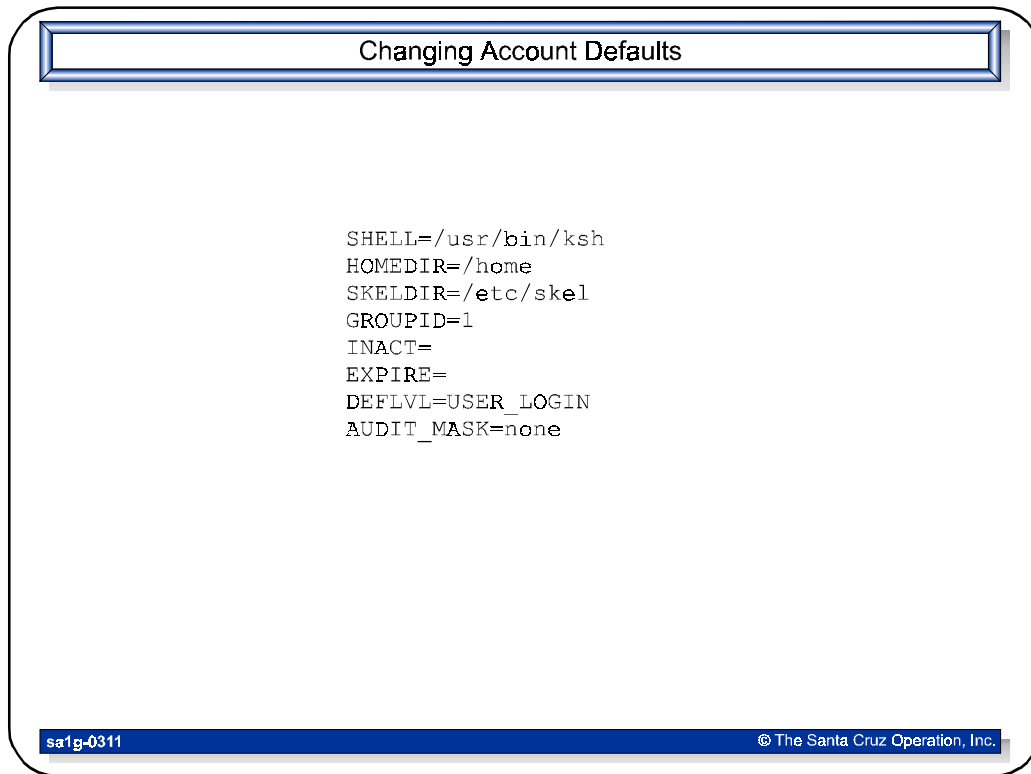
These steps describe how to create a user account using modified defaults:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select **Users** ⇒ **Add New User**.
- Step 3. Enter the login name.
- Step 4. Enter a different **User ID**.
- Step 5. Enter information about the user into the **Comment** field.
- Step 6. Select **Set password now**.

Note that, if you select **Set password later**, the user cannot log in until you set the initial password.

- Step 7. Click on **Change Login Shell** and select the appropriate shell.
- Click on **Add Shell Environment Files to Home Directory** and set up the default user environment for that shell. Click on **OK** to continue.
- Step 8. Click on **Change Distribution** and select one of the following: local, Advanced Server, or NIS network.
- Step 9. Click on **Change Home Directory**, enter the new directory location, and set the permissions for the home directory. Click on **OK** to continue.
- Step 10. Click on **Change Group Membership** and set the login group. A list of groups and a list of groups to which the account belongs displays. **Add** and **Remove** groups between those two lists. Click on **OK** to continue.
- Step 11. Click on **Change Locale** and select a new locale. Click on **OK** to continue. Click on **OK** to create the account.
- Step 12. Set the password for this account.
- Step 13. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

AV 3-11



Instructor Guide

This exercise lets students practice creating a user account. Some modifications to the default values are suggested so that students gain experience with the interface.

Exercise: Creating a user account

In an earlier exercise, the default login shell was changed to the Bourne shell. Change the default login shell to the Korn shell before creating this user. Refer to the steps under Section 3.1.4, “Login Shell,” on page 3-11.

Create an additional user account for yourself. Select your login name. Add *adm* to your group membership.

3.2.3 Creating user accounts with `useradd(1M)`

Because the **Account Manager** and the `useradd(1M)` command use different default files, highly recommend to the students that they use one or the other.

The `useradd(1M)` command lets you create a user's audit event mask. You cannot do this with the **SCOadmin Account Manager**. All other usage is equivalent.

You can also use the `useradd(1M)` command to create user accounts. Some administrators find it faster using command-line options as opposed to a graphical interface.

3.2.3.1 Changing account defaults

AV 3-11: Changing Account Defaults

Relate the contents of `/etc/default/useradd` to the **SCOadmin Account Manager**.

Recall when creating accounts with the **Account Manager**, defaults are established by accessing **Options** ⇒ **User Defaults**. When you create accounts using the `useradd(1M)` command, the defaults are stored in `/etc/default/useradd`.

There are several ways that you can change these defaults:

- Use the **SCOadmin System** ⇒ **System Defaults Manager**
- Edit the `/etc/default/useradd` file
- Use the `defadm(1M)` command

For example, to change the default shell to the Korn shell, enter:

```
defadm useradd SHELL=/bin/ksh
```

3.2.3.2 Creating user accounts

Unless the **-m** option is used, the home directory specified in */etc/default/useradd* is not created. You can also use the **-d** option to specify a home directory other than the default. However, the directory is not created.

To create an account using the defaults from */etc/default/useradd* and a user ID of 250, enter:

```
useradd -m -u 250 login_name
```

The user is not able to log in until a password is assigned.

Exercise: Creating a user account with useradd(1M)

Create a user account with a UID of 150, a home directory in */home*, and a comment about the user. Refer to **useradd(1M)** for the option that is used to add the comment. Enclose the comment with quotes.

3.3 Deleting Users

When a user leaves the company, you should disable that user's account to prevent any unauthorized access. To disable a user account:

- Deactivate the account. No one is able to log into the system using the login name, and the login name is unavailable for reuse.
- Delete the account so that the login name and user ID can be reused

3.3.1 Managing user files

If you deactivate or delete a user account, you must decide what to do with the user's files and directories. Leaving the files unchanged can mean that disk space is used unnecessarily. Also, any files that belong to that user might be restricted to access by the **root** account.

You have two options:

- Back up the files and directories, then delete any files or directories owned by the user. This frees up disk space, but can remove files that other users require. If at a later date, you need a file, you can restore it from the backup.
- Assign ownership of the files to another user. That user can then decide which files to keep and which to remove.

Use the **find(1)** command to locate any files owned by a particular user.

Exercise: Locating user files

Use **find(1)** to locate any files owned by your new user account. For example, if the new user login is **user1**, enter:

```
find / -user user1 -print | pg
```

3.3.2 Deleting users

Remind students that this same rule applies when adding users. Use one or the other. Do not interchange.

If you add users using the **Account Manager**, use the **Account Manager** to delete your users. If you add your users using the **useradd(1M)** command, use the **userdel(1M)** command to delete your users.

3.3.2.1 Re-using UIDs

This information applies to both the **Account Manager** and the **userdel(1M)** command.

When a user is deleted from the system, the UID of the user is stored in the */etc/security/ia/ageduid* file.

You do not see the */etc/security/ia/ageduid* file on the system until a user is deleted.

By default, the UID is kept in this file for twelve (12) months. You can change this parameter by changing the UIDAGE parameter in the */etc/default/userdel* file.

If the UID is:

- Never to be reused, enter UIDAGE=-1
- Reused immediately, enter UIDAGE=0
- Reused in six (6) months, enter UIDAGE=6

3.3.2.2 Using the SCOadmin Account Manager

If a user's files are outside of their home directory hierarchy, they are not deleted. Stress to students that they **MUST** back up the user's files or they are removed when the user's account is deleted.

WARNING: Any instance of the user is removed including the user's home directory and its contents!

These steps describe how to delete a user account:

- Step 1. Back up the user's files.
- Step 2. Start **SCOadmin**. Select **Account Manager**.
- Step 3. Select the user account.

Step 4. Select **Users** ⇒ **Delete**. Click on **OK**.

Step 5. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

3.3.2.3 Using the `userdel(1M)` command

The **userdel(1M)** command offers flexibility when deleting user accounts. You can specify whether the:

- Home directory and its' contents are to be removed
- UID should be reused in a number of months, reused immediately, or never reused. The `UIDAGE` parameter in the `/etc/default/userdel` file is overridden.

This command describes how to delete a user account, save the home directory and its contents, and immediately reuse the UID:

userdel -n 0 login_name

The **-n** option specifies a value for the number of months to age the UID. Specify **-1** to indicate the UID should never be reused. Specify **0** to indicate the UID can be reused immediately. If the **-n** option is not specified, the UID is aged for a default number of months before it is reused. Defaults are stored in `/etc/default/userdel`.

Exercise: Researching the `userdel(1M)` command

Which option to the **userdel(1M)** command is used to remove the user's home directory and its contents?

Remove the **user3** account.

3.4 Modifying Accounts

You can make changes to individual accounts and change system-wide defaults that determine the settings for new accounts. Modifications for individual accounts or system-wide can include:

- Environment variables and location of home directories
- **umask** value
- Passwords or password expiration

Changes on individual accounts take place upon the next user log in.

Changing system-wide defaults affect the default settings when creating new accounts.

3.4.1 Modifying individual account information

When modifying a user account using the **SCOadmin Account Manager**, you can change any of the values except the login name and user ID.

Follow these steps to modify an existing account:

Step 1. Start **SCOadmin**. Select **Account Manager**.

Step 2. Select an account to modify.

Step 3. Select **Users** ⇒ **Modify**.

The screen is the same as the screen used to create a new user.

Step 4. Select a **Change** option(s) and make the necessary changes. For example, to change the login shell, select **Change Login Shell**.

Step 5. Click on **OK** after each change.

Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

Exercise: Modifying a user account

Modify your student account (created in an earlier exercise) so that the **Comment** field states the date and name of this course.

3.4.2 Using usermod(1M)

The **usermod** command offers more flexibility than the **SCOadmin Account Manager** when modifying user accounts. You can change the:

- UID number
- Login name

To change the UID number, enter:

```
usermod -u uid login_name
```

After changing the UID number, files and directories owned by the user still reflect the old UID. Use the **chown**(1) and **chgrp**(1) commands to change ownership of all files and directories owned by the user. Don't forget the user's home directory.

You can also set login expiration dates, activate, and deactivate user accounts.

3.4.2.1 Setting a login expiration date

It might be necessary to set up a temporary user account. So that the login expires when the account is no longer in use, use **usermod** to set an expiration date, enter:

```
usermod -e mm/dd/yy login_name
```

To remove the expiration date, enter:

```
usermod -e "" login_name
```

If the user account was created using the **SCOadmin Account Manager**, you can also set or remove the login expiration date. Select **Account Manager** ⇒ **User name** ⇒ **Users** ⇒ **Expiration**.

3.4.3 Deactivating a Login

Should a user not log in to the system for a period of time, you can deactivate the user's login by setting the "inactive" field of the login.

usermod -f *n* login_name

Where *n* is considered the number of inactive number of days after the last time the user logged in.

You can reactivate the user's login, enter:

usermod -f 0 login_name

The amount of warning time, the number of days before deactivation, and the expiration date is displayed using **logins(1M)** with the **-x** option.

3.4.4 Modifying an individual account environment

When the home directory (*\$HOME*) is created for the user, copies of the default startup files are placed there. Listed below are the shells and the names of their respective startup files:

Bourne shell	<i>\$HOME/.profile</i>
C shell	<i>\$HOME/.cshrc</i> and <i>\$HOME/.login</i>
Korn shell	<i>\$HOME/.kshrc</i> and <i>\$HOME/.profile</i>

3.4.5 Modifying the umask of a single account

You can set up a user's environment to use a specific default by including a **umask(1)** statement in the shell's startup file, such as *\$HOME/.profile* or *\$HOME/.login*. This overrides the system-wide default. Note that this **umask** could create a potential security breach because the permissions on all new files will differ from the system defaults.

If you change an individual's **umask**, you might have to use the **chmod(1)** command to set the permissions on existing files to match the new environment.

3.4.6 Modifying user passwords

These steps describe how to modify a user's password:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select the user.
- Step 3. Select **Users** ⇒ **Change Password**.
- Step 4. Set the password.
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

To modify a user's password from the command line, use **passwd(1)**.

If students change the permissions to 444 on a user's *.profile* and change the ownership to **root**, the user is not able to edit the *.profile* file.

Exercise: Changing the password

Change the password for your newly created student account.

3.4.7 Controlling password expiration

You can control password expiration for an individual user. These steps describe how to change the password expiration values:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select the user.
- Step 3. Select **Users** ⇒ **Expiration**.
- Step 4. Select the default or enter the values for:
 - **Days required between changes**. This is the number of days until the password can be changed.

- **Days before password expires.** This is the maximum number of days a password is valid. This number must be larger than the number of days required between changes.
- **Days until account is warned.** This is the number of days before the password expires that a warning is issued to change your password. This number should be less than the number of days until the password expires.

Step 5. Click on **OK**.

Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

Password values can also be changed using **passwd(1)**.

3.4.8 Controlling password options with default files

By assigning values to a set of parameters in the */etc/default/passwd* file, an administrator can control the aging and length of passwords. The following parameters are available.

MINWEEKS	Minimum number of weeks before a password can be changed.
MAXWEEKS	Maximum number of weeks a password can be unchanged.
WARNWEEKS	Number of weeks before a password expires that the user is warned.
PASSLENGTH	Minimum number of characters in a password.

Two parameters located in */etc/default/login* control the existence of passwords.

PASSREQ	If set to YES, all users must have a password. Users who do not have a password are requested for one at the next opportunity permitted by password aging.
MANDPASS	If set to YES, all users must have a password. The PASSREQ parameter is overwritten and users who have a NULL password are denied access.

Exercise: Changing the password length

Edit the `/etc/default/passwd` file and change the minimum password length to five (5).

3.5 Managing User Groups

You can add and remove users from groups, as well as remove groups.

3.5.1 Modifying group membership

These steps describe how to modify a group's membership:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select **View** ⇒ **By Groups**. Select the appropriate group.
- Step 3. Select **Groups** ⇒ **Modify**. Add and remove users. Click on **OK**.
- Step 4. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

Use the **chgrp(1)** command to change group ownership on the files.

3.5.2 Deleting a group

These steps describe how to delete a group:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select **View** ⇒ **By Groups**. Select the appropriate group.
- Step 3. Select **Groups** ⇒ **Delete**. Click on **OK**.
- Step 4. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

After you remove a group, you should also:

- Set the default login group to a different group if this group was the default login group.
- Use the **chgrp(1)** command to change group ownership of the files still assigned to the deleted group.

3.6 Setting Login Attempt Restrictions

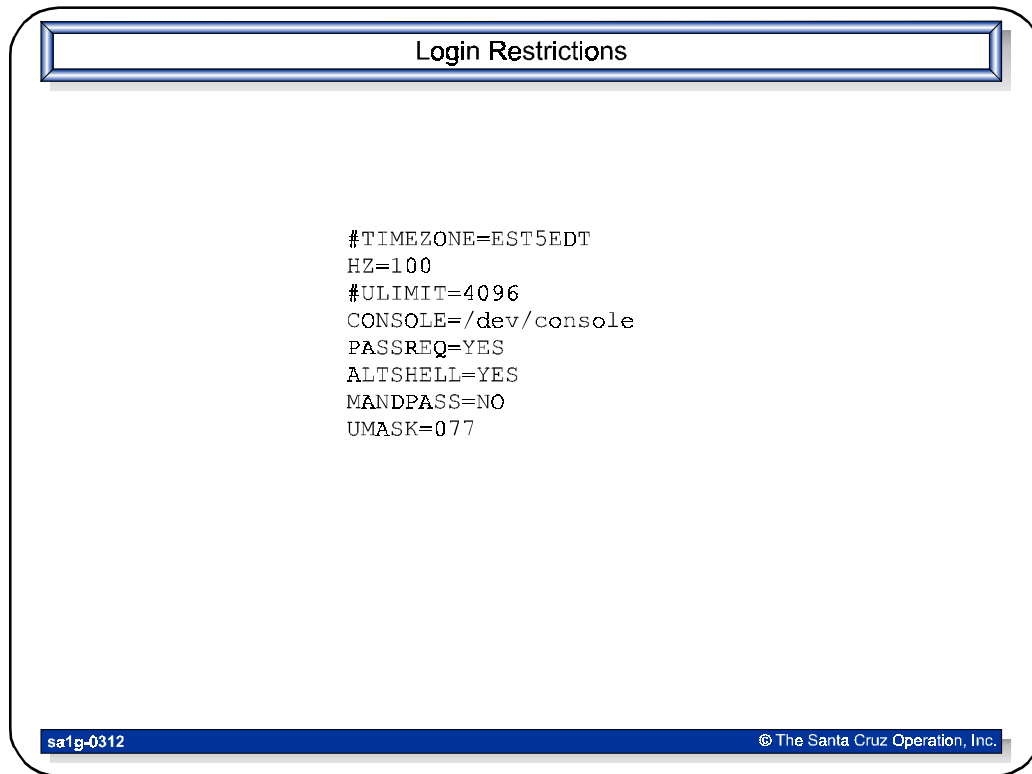
The **Account Manager** shows an icon to indicate a locked account. To view the icons, select **Options** ⇨ **Show Status**. If this option is selected, the **Account Manager** takes longer to run initially.

The **Account Manager** does not reflect changes made from the command line until the students restart the **Account Manager**.

One way that a person can try to break into a system is to repeatedly attempt to log into a terminal by guessing the password for specific accounts. You can protect both terminals and user accounts by limiting the number of consecutive unsuccessful login attempts. The system locks the account or terminal if the unsuccessful attempts exceed the specified limit.

Of course, if legitimate users forget their passwords, their accounts or terminals can be locked. In that case, unlock accounts and terminals so that those users can access the system again.

AV 3-12



Instructor Guide

3.6.1 Login restriction parameters for user accounts

AV 3-12: Login Restrictions

The `/etc/default/login` file. Explain to students the following parameters have to be added to this file.

Increase the difficulty of users logging into your system by setting these parameters in the `/etc/default/login` file.

DISABLETIME	Interval between login prompts after an unsuccessful login attempt. The default is ten (10) seconds.
MAXTRYS	Maximum number of login attempts allowed. The default is 99 attempts.
TIMEOUT	Maximum interval for a login attempt. When this period expires, the login is considered unsuccessful and the session is closed. The default is 60 seconds.

3.6.1.1 Editing `/etc/default/login`

These steps describe how to set login restrictions for user accounts:

- Step 1. Start **SCOadmin**. Select **System** ⇨ **System Defaults Manager**.
- Step 2. Select **System login parameters**.
- Step 3. Add the login restriction parameters. For example, to override the default, enter:
 - `DISABLETIME=30`
 - `MAXTRIES=3`
 - `TIMEOUT=30`
- Step 4. Click on **OK**.
- Step 5. Select **Host** ⇨ **Exit** to exit the **System Defaults Manager**.

You can also use **defadm(1M)** to change login restriction parameters:

defadm login parameter=value

3.6.1.2 Recording unsuccessful login attempts

If you suspect that someone is trying to break into your system, you can record unsuccessful login attempts. Record unsuccessful login attempts by adding the **LOGFAILURES** parameter with the number of unsuccessful attempts to the `/etc/default/login` file.

The default number of login attempts is 99.

You must also create a `/var/adm/loginlog` file. The file owner must be **root**, a member of the group **sys**, and the permissions read and write by the owner.

Exercise: Recording unsuccessful login attempts

Using the steps under Section 3.6.1.1, “Editing `/etc/default/login`,” on page 3-45 as a guide, change the **LOGFAILURES** parameter to three (3).

Create the `/var/adm/loginlog` file, enter:

> /var/adm/loginlog

Remember to change ownership to **root** and group ownership to **sys**.

Using your student account, log into your system and enter an incorrect password. Log in as **root** and view the `/var/adm/loginlog` file.

What information is recorded about your login attempt? If the login attempt is not recorded, what is your problem?

3.6.2 Locking and unlocking a user account

If a user is going to be away for an extended period of time, you can lock the account to prevent unauthorized logins.

Follow these steps to lock an account:

Step 1. Start **SCOadmin**. Select **Account Manager**.

Step 2. Select the user account.

Step 3. Select **Users** ⇌ **Lock**.

- Step 4. Click on **OK**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

Follow these steps to unlock an account and force a password change at the next login:

- Step 1. Start **SCOadmin**. Select **Account Manager**.
- Step 2. Select the user account.
- Step 3. Select **Users** ⇒ **Unlock**.
- Step 4. Click on “Enter a New Password.” Enter the new password.
- Step 5. Click on “Force Password Change at Next Login.”
- Step 6. Click on **OK**.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

■ This exercise provides practice in locking and unlocking an account.

Exercise: Locking and unlocking an account

Using the **SCOadmin Account Manager**, lock your student account. Log in as that user. Unlock the account, enter a new password, and force a password change at the next login.

3.7 Using Account Activity Reports

Part of maintaining system security is watching for potential problems. Expired passwords, locked terminals and accounts, and repeated unsuccessful logins can all indicate either a security problem or an education problem for your users.

Because a system often has a large number of users, it is impractical to use the **Account Manager** to examine each individual account for potential problems. UnixWare 7 provides a **Reports Manager** that generates system-wide reports for account, password, and terminal status.

3.7.1 Reporting password status

You can display a system-wide password status report that includes all users or individual users. This report shows the:

- Status of accounts (locked or unlocked)
- Date the password was changed
- Password expiration controls

To display password status:

- Step 1. Start **SCOadmin**. Select **System** ⇒ **Reports Manager** ⇒ **Reports** ⇒ **Password Status**.
- Step 2. Select **By users...** to display the status of an individual user or select **Systemwide** to display a report for all users.
- Step 3. Select **Host** ⇒ **Exit** to exit the **Reports Manager**.

Exercise: Running the password status report

Use the **Reports Manager** and run a password status report for your student account. What is the status of your password expiration controls?

3.7.2 Reporting login activity

The user login status report can address a single user, terminal, all users, or the current user. In a networking environment, you can also display and print a status report by each system. This report provides the:

- User name
- Terminal associated with the login
- Time of login
- Status of the login
- Last logout time
- System logged on

To display login activity:

- Step 1. Start **SCOadmin**. Select **System** ⇨ **Reports Manager**.
- Step 2. Select **Reports** ⇨ **User Logins**.
- Step 3. Select the type of report.
- Step 4. Select **Host** ⇨ **Exit** to exit the **Reports Manager**.

To print the **Password Status** or **User Logins** report while in the **Reports Manager**, select **Host** ⇨ **Print report**.

Exercise: Running the Report Manager

Print the **User Logins** report for all users connected to your system. Save this information to a file in the */tmp* directory.

3.8 Troubleshooting User Accounts

From time to time users may run into problems using their accounts. Listed below are some of the common problems and the steps to correct them.

3.8.1 Fixing forgotten or compromised passwords

■ Stress the importance of not forgetting the **root** password!

These steps describe what you should do if you need to change a user's password:

- Step 1. Confirm the user's identity.
- Step 2. Unlock the user's account, if necessary.
- Step 3. Change the password. Force the password to be changed at the next login.
- Step 4. Remind the user to keep the password private.

3.8.2 Fixing an incorrect terminal type

Sometimes a user incorrectly sets the terminal type during login. As a result, some applications might not display or interpret keystrokes correctly. To reset the terminal type, you must modify the **TERM** variable.

In either the Bourne or Korn shell, at the user prompt, enter:

```
TERM=terminal_type  
export TERM
```

■ It is not necessary to re-export the **TERM** variable if it has already been exported by the current shell.

In the C shell, at the user prompt, enter:

```
setenv TERM terminal_type
```

3.9 Lesson Summary

Before users can access a system, they must have been designated accounts. These accounts set up the users' working environments. In addition to creating and removing accounts, there are a number of elements that you control:

- Which accounts are members of which groups
- How strict are the parameters defining acceptable passwords
- What type of login restrictions are enforced for both accounts and terminals

Review questions

1. Which security profile sets the `PASSLENGTH` field in `/etc/default/passwd` to three(3)?

■ The Traditional security profile sets the `PASSLENGTH` field to three (3) in `/etc/default/passwd`.

2. Which group is the default login group for all users? If you change this group, is the default group automatically changed for existing users?

■ The default login group for all users is `other`. When you change the default group, the group is not automatically changed for existing users.

3. What **umask** value grants the owner and members of the group full access, but denies any access to other users?

■ The `umask` value `007` grants the owner and members of the group full access, and denies any access to others.

4. Which command can you use to change account defaults used by **useradd**(1M) in the `/etc/default/useradd` file?

You can use the `defadm(1M)` command to change account defaults in the `/etc/default/useradd` file.

5. Which two tasks can you perform using the **userdel(1M)** command that you cannot perform using the **SCOadmin Account Manager**?

Using the `userdel(1M)` command, you can specify whether the home directory and its contents are removed and the number of months after which a UID can be reused.

6. Which file sets an individual account environment using the Bourne shell?

The `$HOME/.profile` sets an individual account environment using the Bourne shell.

7. Which parameter in the `/etc/default/login` file do you change so that unsuccessful login attempts are recorded? Which log file must you also create?

So that unsuccessful login attempts are recorded, you must change the `LOGFAILURES` parameter in `/etc/default/login`. You must also create the `/var/adm/loginlog` file.

8. Which report in the **SCOadmin** ⇒ **System** ⇒ **Reports Manager** can you generate that gives you the status of the account, the date the password was changed, and the password expiration controls?

You can generate the Password Status Report in the SCOadmin-> System-> Reports Manager to give you the status of the account, the date the password was changed, and the password expiration controls.

9. List the steps to fix a forgotten or compromised password.

The steps to fix a forgotten or compromised password are: 1. Confirm the user's identity. 2. Unlock the user's account if necessary. 3. Change the password. Force the password to be changed at the next login. 4. Remind the user to keep the password private.

3.10 Lab: Creating Groups

In the next two labs, you are going to create user accounts that will belong to different groups. In this first lab, you will set up groups for the organization.

3.10.1 Overview

Create two new groups called **admin** and **sales**.

3.10.2 Procedure

First, create the **admin** group and assign members.

- Step 1. Start **SCOadmin** ⇒ **Account Manager**.
- Step 2. Select **Groups** ⇒ **Add New Group**.
- Step 3. Enter **admin** as the **Group Name**.
- Step 4. Click on **OK**.
- Step 5. Repeat Steps 3 through 5 to create the **sales** group (enter the appropriate **Group Name** in Step 4).
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

3.11 Lab: Creating New Users

Set up new user accounts and modify them as specified. In addition, assign them to the appropriate groups.

3.11.1 Overview

Create user accounts for two (2) individuals. Assign a password to each account. Modify the default settings according to the individual's requirements:

sales1 Uses the Bourne shell

sysadm Uses the Korn shell; also belongs to the **lp** group.

The **sysadm** account should also belong to the **admin** group. The **sales1** account should belong to the **sales** group.

3.11.2 Procedure

These steps describe how to set up and modify user accounts:

Step 1. Start **SCOadmin** ⇒ **Account Manager**.

Perform these steps for each account.

Step 2. Select **Users** ⇒ **Add New User**.

Step 3. Enter the login name.

Step 4. Enter a comment to describe the account.

Step 5. Select **Set password now**.

Step 6. Select **Change Login Shell**.

Step 7. Select the correct shell for the user.

Step 8. Click on **OK** to set the login shell.

Step 9. Select **Change Group Membership**.

Step 10. Select the group to add from the **Other Groups** list, then select **Add**.

Step 11. Change the login group.

Step 12. Assign other group memberships.

Step 13. Click on **OK** to set the group membership.

Next, you create the account and set the new user password.

Step 14. Click on **OK** from the **Add New User** screen to create the user account. The system sets up the account, including the populated home directory.

Step 15. Enter the initial password when prompted in both the **Enter Password** and **Confirm Password** fields.

Step 16. Select **Force password change at login**, then click on **OK** to set the password.

Step 17. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

3.12 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

defadm (1M)	Displays and modifies account defaults in the <i>/etc/default/useradd</i> file
find (1M)	Finds user files
passwd (1)	Sets a password. Also locks and unlocks user accounts.
scoadmin (1M)	Invokes SCOadmin applications (in this lesson, the Account Manager and the Reports Manager)
setenv (1)	Sets environment for command execution in the C shell
umask (1)	Displays or sets file-creation mode mask
useradd (1M)	Creates user accounts using a command line interface
userdel (1M)	Deletes user accounts using a command line interface
usermod (1M)	Modifies user accounts using a command line interface

Relevant files

<i>/etc/cshrc</i>	Is the system environment file for the C shell
<i>/etc/default/login</i>	Contains system-wide log in parameters
<i>/etc/default/passwd</i>	Contains password aging parameters
<i>/etc/default/useradd</i>	Contains account defaults used by the useradd (1M) command
<i>/etc/default/userdel</i>	Contains the UIDAGE parameter
<i>/etc/profile</i>	Is the system environment file for the Bourne or Korn shell

<i>/etc/default/passwd</i>	Is the file specifying default password information
<i>/usr/lib/scoadmin/account/skel/*</i>	Contains default account startup files used by the SCO Admin Account Manager
<i>/etc/security/ia/ageduid</i>	Contains used UIDs
<i>\$HOME/.chsrc</i>	Is the account environment file for the C shell
<i>\$HOME/.login</i>	Is the account environment file for the C shell
<i>\$HOME/.kshrc</i>	Is the account environment file for the Korn shell
<i>\$HOME/.profile</i>	Is the account environment file for the Bourne or Korn shell

3.13 Answers to Exercises and Review Questions

This section provides the answers to exercises and review questions presented in this lesson.

Exercise: Changing the password length

- Step 1. Run **scoadmin(1M)**.
- Step 2. Double click on **System** ⇨ **System Defaults Manager** ⇨ **Password parameters: passwd(1)**
- Step 3. Change the **PASSLENGTH=3** to **PASSLENGTH=5**
- Step 4. Click **OK**.

Exercise: Reviewing group permissions

The accounts **david**, **john**, and **sue** can read *sales.dat*. Only **david** can write to *sales.dat*.

The accounts **sue**, **john**, and **phil** are the only accounts that can either read or write to the file *forecast*.

Exercise: Modfying the default login group

This change will not affect existing accounts. It will be set to the default group when adding new accounts.

Exercise: Setting umasks

- For Situation 1:
 - umask: 077
 - New file permissions: -rw-----
 - New directory permissions: drwx-----

- For Situation 2:
 - umask: 022
 - New file permissions: -rw-r--r--
 - New directory permissions: drwxr-xr-x

Exercise: Creating a user account with useradd(1M)

`useradd -m -u 150 -c "Secretary - Martha Stinger" login_name`

Exercise: Researching the userdel(1M) command

The `-r` option deletes the users home account.

Exercise: Recording unsuccessful login attempts

The information recorded in the `/var/adm/loginlog` is the username, tty, and date time of the failed attempt. If the information was not recorded correctly the problem could be that you did not successfully edit the `/etc/default/login` file or the `/var/adm/loginlog` was not set with the correct user, group, and permissions.

Review questions

1. The Traditional security profile sets the `PASSLENGTH` field to three (3) in `/etc/default/passwd`.
2. The default login group for all users is *other*. When you change the default group, the group is not automatically changed for existing users.
3. The umask value `007` grants the owner and members of the group full access, and denies any access to others.
4. You can use the **defadm**(1M) command to change account defaults in the `/etc/default/useradd` file.
5. Using the **userdel**(1M) command, you can specify whether the home directory and its contents are removed and the number of months after which a UID can be reused.
6. The `$HOME/.profile` sets an individual account environment using the Bourne shell.

7. So that unsuccessful login attempts are recorded, you must change the LOGFAILURES parameter in */etc/default/login*. You must also create the */var/adm/loginlog* file.
8. You can generate the **Password Status Report** in the **scoadmin(1M) Account Manager** to give you the status of the account, the date the password was changed, and the password expiration controls.
9. The steps to fix a forgotten or compromised password are: 1. Confirm the user's identify. 2. Unlock the user's account if necessary. 3. Change the password. Force the password to be changed at the next login. 4. Remind the user to keep the password private.

4

Managing Processes

Instructor Guide

Instructor Guide

Lesson 4

Managing Processes

Suggested lesson duration

This lesson should take approximately 2 hours to complete, including the lab exercise.

Pre-lesson classroom preparation

None.

Instructor preparation

Review the **ps(1)** and **kill(1)** manual pages. Practice using the **ps(1)** command and the **SCOadmin Process Manager**.

AV 4-1

The slide is titled "Managing Processes" in a blue-bordered box at the top. Below the title, there is a list of four bullet points. At the bottom of the slide, there is a blue footer bar containing the text "sa1g-0401" on the left and "© The Santa Cruz Operation, Inc." on the right.

- Describe a process
- Terminate processes
- Manage processes using the **SCOadmin Process Manager**
- Automate system tasks using the **SCOadmin Task Scheduler**

sa1g-0401 © The Santa Cruz Operation, Inc.

Instructor Guide

Introduction

Every program that runs on a UnixWare 7 system runs as a process. As the system administrator, support your users by ensuring that processes are running efficiently.

You also can automate jobs that clean or monitor the system. You can schedule these maintenance tasks to occur during periods of low system use without administrator or operator intervention.

Objectives

This lesson covers process management and job scheduling. By the end of this lesson, you will be able to:

- Describe a process
- Terminate processes
- Manage processes using the **SCOadmin Process Manager**
- Automate system tasks using the **SCOadmin Task Scheduler**

AV 4-1: Managing Processes

This slide describes the overall topics covered in this lesson.

4.1 Describing a Process

Every event that occurs on a UnixWare 7 system is the result of a process. Both users and the system can generate processes, which can affect the performance of the system. Understanding how processes work can help you identify problems and decide how best to fix them.

4.1.1 Definitions

A process is a single instance of a program in execution. This can be a login shell or an operating system command, but not a built-in shell command. If a command is built into the shell, a separate process is not created on its invocation; the built-in command is issued within the context of the shell process.

Processes differ from programs in that they are actively present in memory, and their state changes with time. A program, on the other hand, does nothing until it is executed and gives rise to a process. Each process is assigned a unique numerical ID. This number is called the process ID or PID.

UnixWare 7 systems support many processes running simultaneously. This is called *multitasking*.

Various system calls enable processes to create other processes, communicate with other processes, and terminate other processes.

4.1.2 The process table

■ Run the `sar(1M)` command with the `-v` option. Show students the current size of the process table.

The kernel maintains a table of all running processes. This table can grow dynamically to a maximum size determined by the kernel and available system resources.

Every time a new process is created, the kernel assigns it a unique process identification number (PID) and adds information describing it to the process table.

4.1.3 Viewing current processes

Use the **ps(1)** command to view processes currently in the table. Common options for the **ps** command include:

- f** Generates a full listing of a process
- u** Generates a list of processes owned by the specified user(s)
- t** Generates a list of processes associated with the specified terminal
- e** Displays the entire list of processes

■ This exercise shows how the various **ps(1)** options affect its output.

Exercise: Viewing user processes

Use **ps(1)** to view all of the processes associated with your current login.

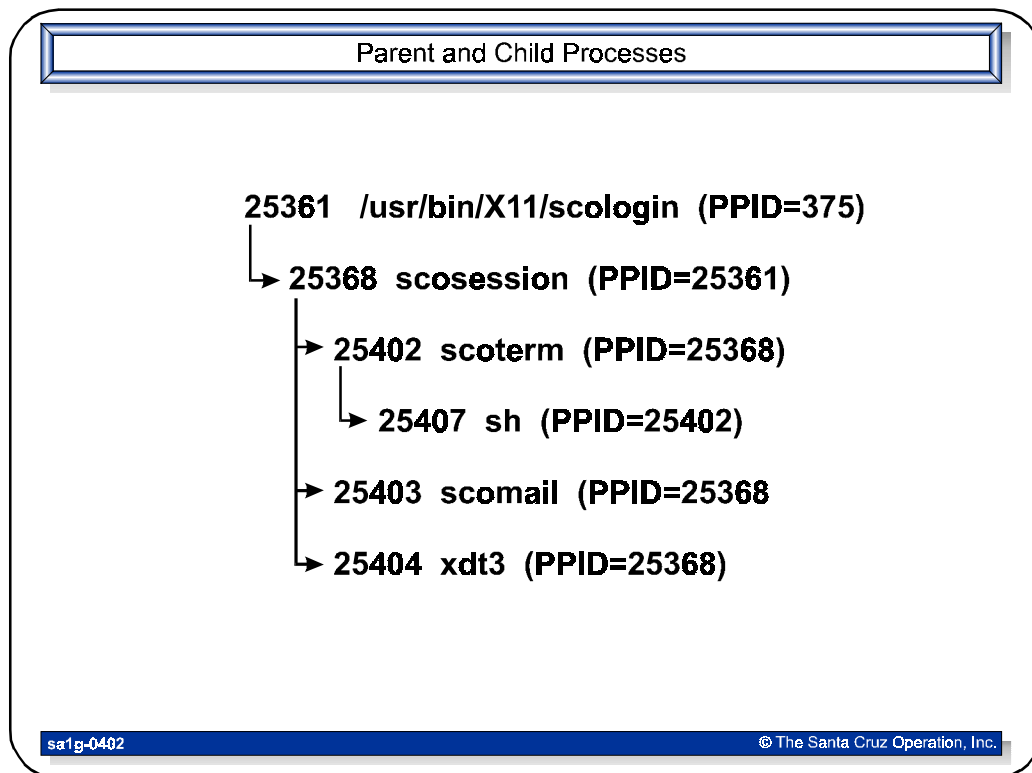
Use **ps -f** to view more information about the processes associated with your current login.

Use **ps -fu root | pg** to view information about all of **root**'s current processes.

Use **ps -ft console** to view information about all processes associated with the console.

Use **ps -ef | pg** to view information about all processes.

AV 4-2



Instructor Guide

4.1.4 Process genealogy

AV 4-2: Parent and Child Processes

This slide shows the relationship between parent and child processes. Point out that unless the child process is a background process, the parent process waits for the child process to terminate before continuing.

A process that creates a new process is called the *parent* process. The new process is called the *child*.

The shell takes most commands and creates a child process to run them. Often, a parent process waits for the child process to complete before continuing.

By starting child processes in the background, one parent process can have many child processes.

A child process can have only one parent process.

4.1.5 Foreground and background processes

When a command is entered at the shell prompt, the shell creates a child process to run the command. The shell waits for the command to exit, then returns the prompt to the user. This command is said to run in the *foreground* because the user cannot execute another command until it completes.

When a command is entered at the shell prompt followed by an ampersand (&), the shell creates a child process to run the command, but does not wait for the command to exit. Instead, it immediately returns the prompt to the user. This command is said to run in the *background*.

Background processes must be non-interactive. Different shells handle foreground and background processes differently.

4.1.6 Daemon processes

A daemon is a background process that performs a regular routine or provides a service without human intervention. A daemon might be started as a response to some event, or it can be executed at regular intervals. One of the most important daemons on the system is **cron**, which regularly runs other programs.

Daemon processes are processes that are not associated with a terminal or an active user session. They perform system tasks on a periodic basis, and sleep between those tasks. The **ps(1)** command indicates daemons with a question mark (?) in the *tty* field.

4.1.7 Defunct processes

A defunct process is a process that has terminated but has not been removed from the process table because its parent did not “wait” for it. While the parent is still alive and not waiting for the child, defunct processes can remain in the process table. The slot in the process table is the only system resource consumed by it.

Large numbers of defunct processes can interfere with the creation of new processes, as the total number of processes that can exist on the system is limited.

Usually, a defunct process is removed when its parent terminates. If it is not removed, **init**(1M) inherits and removes it.

Should a defunct process remain, consider rebooting the system to remove it.

4.2 Terminating Processes

■ Refer to the **kill(1)** manual page.

Sometimes processes stop functioning. For example, a program might encounter an unexpected error and hang. The process is still in the process table, and sometimes a window still displays, but the process is not running. You must manually terminate such a process.

You might also need to terminate runaway processes. These have not stopped working; they are caught in some form of infinite loop. These usually occur as a result of a user script error. Runaway processes continue to use system time and memory until you terminate them.

4.2.1 The **kill(1)** command

You can terminate processes using the **kill(1)** command:

kill [-signal] PID

The **kill** command sends a signal to a process which usually results in the termination of that process. Some processes can ignore signals or respond to them without terminating. This is called *trapping* the signal.

To terminate a process with the **kill** command, you must know the process ID number (PID) of the process to terminate. Non-root users can kill only their own processes.

4.2.2 Using the **kill(1)** command

You send various signals to a process when using the **kill(1)** command. Send them in the following order until the process terminates:

- Press  (**kill -2**) at the terminal with the hung process.
- Press  \ (**kill -3**) at the terminal with the hung process. This is likely to create a file named *core* which contains the program code.
- Run **ps -u account_name** from another terminal or console to get the PID of the hung process.

- Run **kill *PID*** from another terminal or console. This is the same as **kill -15 *PID***. Some programs trap this signal, terminate child processes, and clean up any temporary files before exiting.
- Run **kill *PID*** on the parent process.

If none of these signals work, run **kill -9 *PID***. Processes cannot trap or ignore this signal. Because this signal cannot be trapped, the process cannot clean up temporary files and child processes.

Note that high-priority processes cannot be terminated without rebooting the system.

4.3 Managing Processes with the Process Manager

You can also change a priority of a process and send a signal to a process using the **SCOadmin Process Manager**. Explain to the students that these two topics are not in the scope of this class.

You can use the **SCOadmin Process Manager** to manage processes on a local or remote system. The **Process Manager** lets you:

- View processes
- Delete (kill) processes

4.3.1 Viewing processes on a system

By default, the **Process Manager** uses these attributes to display all processes on a system:

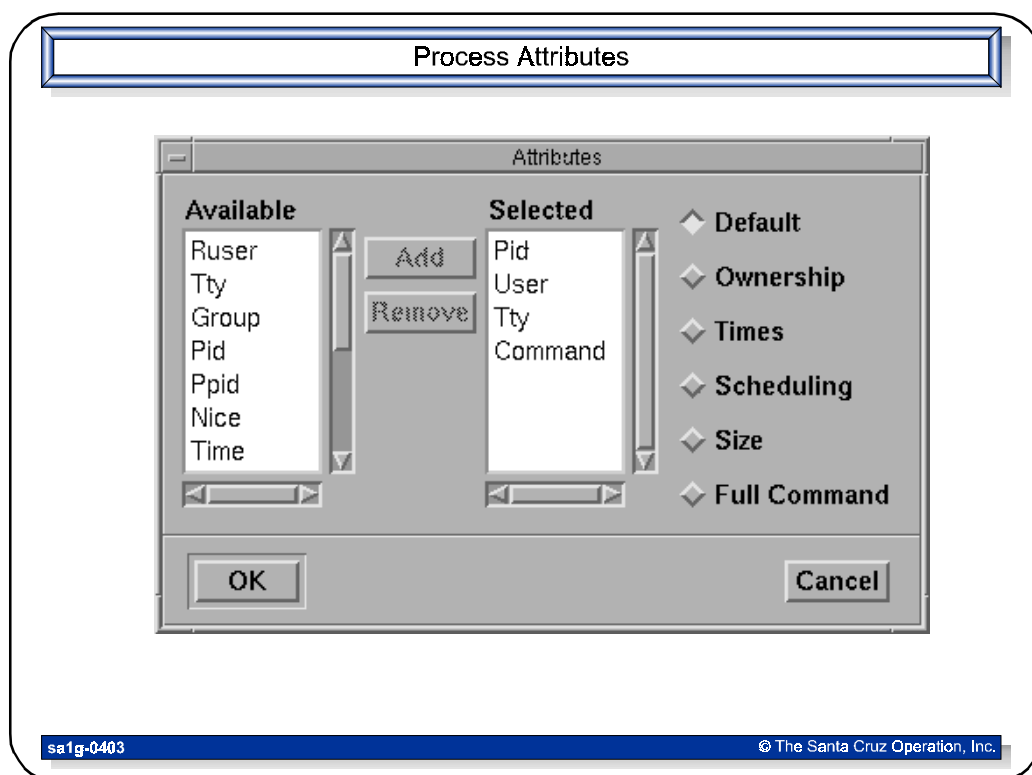
PID	The number that identifies the process.
User	The owner of the process.
Tty	The terminal that is associated with the process.
Command	The command that is executed.

You can also view processes associated with a specific User, Tty, or PID.

These steps describe how to access the **Process Manager** and view processes associated with an individual user:

- Step 1. Start **SCOadmin**. Select **Process Manager**.
- Step 2. Select **View By User**.
- Step 3. Select the user from the **Available** column. Click on **Add**.
- Step 4. Click on **OK**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Process Manager**.

AV 4-3



Instructor Guide

4.3.1.1 Changing displayed process attributes

AV 4-3: Process Attributes

Use this slide to show students the different attributes. They can customize the viewing of processes to meet their needs or select from one of the choices.

You can change the viewing of processes by adding or removing attributes. For example, to add the accumulated time that a process has been running to the default view, perform these steps:

- Step 1. Start **SCOadmin**. Select **Process Manager**.
- Step 2. Select **View** ⇒ **Attributes**.
- Step 3. Select **Time from the Available column**. Click on **Add**.
- Step 4. Click on **OK**.

4.3.1.2 Sorting by attributes

You can change the attributes by which processes are sorted. To determine which processes are using the most CPU (accumulated) time, perform these steps:

- Step 1. Start **SCOadmin**. Select **Process Manager**.
- Step 2. Select **View** ⇒ **Sort**.
- Step 3. Select **Time**. Click on **Decreasing**.
- Step 4. Click on **OK**.

The processes are sorted by the **Time** attribute and display in descending order.

4.3.2 Deleting processes

In Section 4.2.2 on page 4-11 you learned how to use the **kill(1)** command with different signals to terminate processes. You can also use the **Process Manager** to delete (kill) processes.

These terms describe some of the signals used when deleting processes using the **Process Manager**.

INT	Signal 2
QUIT	Signal 3
TERM	Signal 15
KILL	Signal 9

For a complete description of all the signals used by the **Process Manager**, refer to the **signal(5)** manual page.

These steps describe how to send a TERM signal to a process using the **Process Manager**:

- Step 1. Start **SCOadmin**. Select **Process Manager**.
- Step 2. Select a process to delete.
- Step 3. Select **Process** ⇒ **Signal**.
- Step 4. Select **TERM**
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Process Manager**.

4.4 Scheduling Tasks

One way to make your job easier is to automate system tasks such as unattended backups and system clean ups. The **cron**(1) daemon runs these automated tasks at designated hours on designated days. You can schedule non-interactive tasks to run during off-hours when the system load is lighter.

A scheduled task can be either a single command or a shell script containing many commands. Output of a command is mailed to you unless redirected to a file or terminal.

4.4.1 Setting the system date and time

Before you schedule tasks, verify the system date and time are correct.

These steps describe how to set the correct date and time using the **System Time Manager**:

- Step 1. Start **SCOadmin**. Select **System** ⇒ **System Time Manager**.
- Step 2. **Select Host** ⇒ **Set Time**.
- Step 3. Enter the correct date and time. Note that hours are expressed in a 24-hour format. For example, enter **14** to indicate 2:00 p.m.
- Step 4. Click on **OK** to set the system clock to the specified date and time.
- Step 5. Click on **OK** to accept the date and time.
- Step 6. Select **Host** ⇒ **Exit** to exit the **System Time Manager**.

Use the **date**(1) command to set the system date and time from the command line.

Exercise: Setting today's date and time

Use the **System Time Manager** to set the system clock to the correct date and time.

4.4.2 Using the Task Scheduler

Explain to students that the **Task Scheduler** is an X application ported from UnixWare 2.1. It is not a vTcl script, therefore, there is no CHARM (character) interface.

Use the **SCOadmin Task Scheduler** to automate system tasks. With the **Task Scheduler**, you can:

- Authorize users to schedule tasks
- Add or modify tasks
- View scheduled tasks
- Delete scheduled tasks

4.4.2.1 Authorizing users to schedule tasks

Follow these steps to authorize users on your system to schedule tasks:

- Step 1. Start **SCOadmin** ⇒ Select **Task Scheduler**.
- Step 2. Select **Task** ⇒ **Authorization**.
- Step 3. Select a name of the user from the “Denied” column. Click on **Add**.
- Step 4. Click on **OK**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Task Scheduler**.

In Step 3, to remove a user’s authorization, select the name of the user from the “Allowed” column and click on **Deny**.

*When authorizing users, the user name is added to the `/etc/cron.d/cron.allow` file. This file is an explicit list of who can schedule **cron(1)** jobs.*

*When removing a user’s authorization, the user name is removed from the `/etc/cron.d/cron.deny` file, which is an explicit list of who cannot schedule **cron(1)** jobs.*

Note that under Low and Traditional security, the `cron.allow` and the `cron.deny` files are empty. All user’s can submit cron jobs.

4.4.2.2 Adding scheduled tasks

Recall that a task can be a single command, shell script, or any application program that can run unattended. When you or a user adds tasks, the **Task Scheduler** creates a single file for each user containing the scheduled times and tasks. This file is:

- Named for the user scheduling the task
- Placed in the `/var/spool/cron/crontabs` directory

Before adding a scheduled task, decide:

- The name of the user running the task.
- The full pathname of the command or program. If the full pathname is not entered, the **Task Scheduler** examines the user's home directory.
- The day of the week or the date of the month that the task is scheduled.
- The time. The task can be scheduled to run at a specific time or every hour. Hours are expressed in a 24-hour format. Task can also be scheduled to run every minute.

For example, to add a task that runs at 1:00 p.m. on Wednesday and Friday, perform these steps:

Step 1. Start **SCOadmin**. Select **Task Scheduler**

The next step is optional. The task is created for the user who is running the **Task Scheduler**. If you are logged in as **root**, and want to create a task for a different user, you must perform Step 2.

Step 2. Select **View** ⇒ **Tasks by Users**. Select the authorized user.

Step 3. Click on **Task** ⇒ **Add Task** and enter the full pathname of the command or program.

Step 4. Click on **Day of Week**. Select **Wednesday** and **Friday** as the days of the week.

Step 5. Click on "Every Hour" and "Every Minute." This "turns off" this option.

Step 6. Click on **Hour**. Select 13. Click on **Minute**. Select 0.

- Step 7. Click on **OK**.
- Step 8. Select **Host** ⇒ **Exit** to exit the **Task Scheduler**.

4.4.2.3 Modifying scheduled tasks

When you are logged in as **root** and enter the **Task Scheduler**, **root**'s scheduled tasks display. From the **Task Scheduler**, to modify a task:

- Step 1. Select the task to modify.
- Step 2. Click on **Task** ⇒ **Modify Task**.
- Step 3. Modify the task by following Steps 4 through 7 under Section 4.4.2.2, "Adding scheduled tasks," on page 4-19.

The **root** user can modify any user's tasks. Other users can only modify their own tasks.

When you are logged in as **root** and want to modify another user's scheduled tasks, perform these steps. From the **Task Scheduler**:

- Step 1. Select **View** ⇒ **Tasks by Users**.
- Step 2. Select the name of the user. Click on **OK**.
- Step 3. Click on **Task** ⇒ **Modify Task**.
- Step 4. Modify the task by following Steps 4 through 7 under Section 4.4.2.2, "Adding scheduled tasks," on page 4-19.

4.4.3 Deleting scheduled tasks

To delete a task, perform these steps. From the **Task Scheduler**:

- Step 1. Select the task.
- Step 2. Click on **Delete**.
- Step 3. Click on **OK**.

The **root** user can delete any user's task. Other users can only delete their own tasks.

If you are logged in as **root** and want to delete another user's task, first list the user's tasks. Click on **View** ⇒ **Tasks by Users**.

4.5 Modifying System Tasks

In addition to creating your own scheduled tasks, some tasks are automated by default. You can modify these tasks or add tasks to each file. These files are stored in the `/var/spool/cron/crontabs` directory:

adm Maintains a log of user logins. You can view this log. Enter:

who -a /var/adm/wtmp

You can also use this file to collect system startup and performance information.

lp Removes log information about the print service that is recorded in the `/var/lp/logs` directory

root Performs various administrative functions.

sys Collects performance information using the **sar**(1M) command

uucp Automates and performs maintenance tasks for UUCP

It is recommended that you not remove these files. If you do not want these tasks to run, precede the file entries with a pound (#) sign.

4.6 Lesson Summary

Processes comprise a large portion of system operation. From time to time you will need to terminate hung processes so that a user can resume working. You can also schedule jobs to automate routine administration tasks.

Review questions

1. What is the difference between a program and a process?

The difference between a program and process is that a program is an executable file in the filesystem, while a process is an instance of a program that is currently executing.

2. Why is it preferable to use **kill -15** instead of **kill -9**?

It is preferable to use kill -15 instead of kill -9 because many processes will trap a signal 15 and remove any temporary files before exiting. A signal 9 cannot be trapped, and any temporary files created would not be deleted.

3. List the steps to add the **Accumulated Time** field for viewing processes using the **SCOadmin Process Manager**.

The steps to add the Accumulated Time field to the Process Manager are: run scoadmin(1M) Double click on Process Manager. Select View's Attributes. Select Time. Click on Add. Click on OK.

4. Which factors should you consider before scheduling a task in the **SCOadmin Task Scheduler**?

The factors that you should consider before scheduling a task in the scoadmin(1M) Task Scheduler are the user name of the person running the task, full pathname of the program, the day of the week or the date of the month that the task is scheduled, and the time.

4.7 Lab: Scheduling Processes

In this lab you will schedule tasks to run automatically.

4.7.1 Overview

Using your student account, create a scheduled task to mail the last 50 lines of `/var/adm/syslog` to **root** at 8:00am on Mondays.

Procedure

Authorize your student account to schedule tasks:

- Step 1. Log in as **root**.
- Step 2. Start **SCOadmin** ⇒ **Task Scheduler**.
- Step 3. Select **Task** ⇒ **Authorization**.
- Step 4. Click on your student account name ⇒ **Add** ⇒ **OK**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Task Scheduler**.
- Step 6. Exit the desktop.

Create the task:

- Step 1. Log in using your student account.
- Step 2. Create an executable file in your home directory. Name the file *mailroot*. Enter this line into the *mailroot* file:

```
tail -50 /var/adm/syslog | mail root
```

- Step 3. Start **SCOadmin** ⇒ **Task Scheduler**.
- Step 4. Click on **Task** ⇒ **Add Task**.
- Step 5. Enter the full pathname of the program.
- Step 6. Click on **Day of Week**. Select **Monday** as the day of the week.
- Step 7. Click on **Hour**. Select 8.
- Step 8. Click on **Minute**. Select 0.
- Step 9. Click on **OK**.
- Step 10. Select **Host** ⇒ **Exit** to exit the **Task Scheduler**.

4.8 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

cron (1M)	Executes commands scheduled by crontab (1)
crontab (1)	Schedules commands to be executed at regular intervals
kill (1)	Sends a kill signal to a process
ps (1)	Displays information about active processes
sar (1M)	Reports usage information for individual processors, as well as summary information for average processor usage
scoadmin (1M)	Invokes SCOadmin applications (in this lesson, the Cron Manager and the System Time Manager)

Relevant files

<code>\$HOME/crontab.eg</code>	Suggested file containing a user's cron (1M) requests
--------------------------------	--

4.9 Answers to Exercises and Review Questions

This section provides the answers to exercises and review questions presented in this lesson.

Review questions

1. The difference between a program and process is that a program is an executable file in the filesystem, while a process is an instance of a program that is currently executing.
2. It is preferable to use `kill -15` instead of `kill -9` because many processes will trap a signal 15 and remove any temporary files before exiting. A signal 9 cannot be trapped, and any temporary files created would not be deleted.
3. The steps to add the Accumulated Time field to the Process Manager are: run **scoadmin(1M)** Double click on **Process Manager**. Select **View** ⇨ **Attributes**. Select **Time**. Click on **Add**. Click on **OK**.
4. The factors that you should consider before scheduling a task in the **scoadmin(1M)** Task Scheduler are the user name of the person running the task, full pathname of the program, the day of the week or the date of the month that the task is scheduled, and the time.

5

Working with Filesystems

Instructor Guide

Instructor Guide

Lesson 5

Working with Filesystems

Suggested lesson duration

This lesson should take approximately 2 hours to complete, including the lab exercise.

Pre-lesson classroom preparation

Create a *vxfs* floppy filesystem diskette for each student in the class. Students will mount and umount this floppy filesystem in several exercises throughout the lesson.

Use this command to create a primary drive, 3.5" *vxfs* filesystem floppy:

```
/sbin/mkfs -F vxfs -o ninode=711 /dev/dsk/f03ht 2844
```

When mounting the *vxfs* filesystem floppy, enter:

```
mount -F vxfs /dev/dsk/f03ht /mnt
```

When unmounting the floppy from the */mnt* directory, enter:

```
umount /mnt or umount /dev/dsk/f03ht
```

You can also use the **SCOadmin Filesystem Manager**.

Instructor preparation

Review the manual pages for the **mkfs(1M)**, **fsck(1M)**, **mount(1M)**, and **umount(1M)**. Practice using the **mkfs(1M)**, **mount(1M)**, and **umount(1M)** commands and the **SCOadmin Filesystem Manager**.

AV 5-1

Working with Filesystems

- Describe filesystem basics
- Use different filesystem types
- Mount and unmount a filesystem
- Repair a non-root filesystem
- Monitor filesystems
- Locate and manage user files
- Manage system logs and temporary directories

sa1g-0501 © The Santa Cruz Operation, Inc.

Instructor Guide

Introduction

A filesystem is a structure that allows the UNIX operating system to store and access files and directories. Unless you make a filesystem available to your users, they cannot access any of the stored information.

If a filesystem becomes damaged, you are unable to access any of the data until it is repaired.

If a filesystem becomes full, performance degrades and users may not be able to save their work. Maintaining filesystems ensures that users can access the programs and data needed.

Objectives

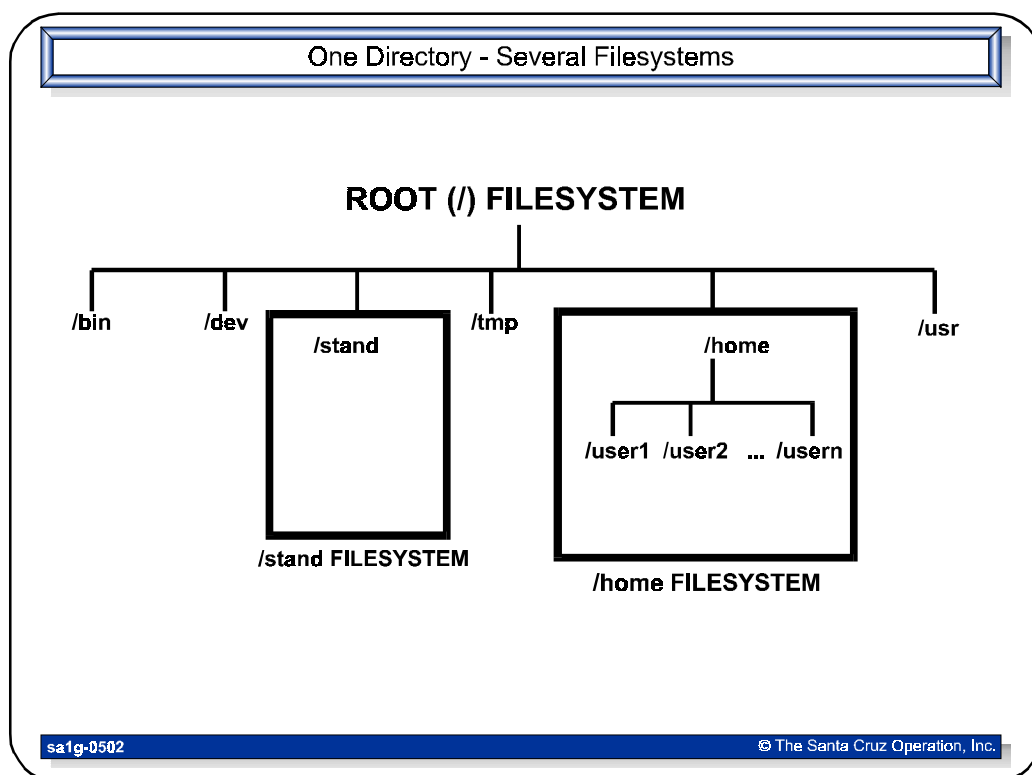
This lesson shows you how to manage and repair filesystems. By the end of this lesson, you will be able to:

- Describe filesystem basics
- Use different filesystem types
- Mount and unmount a filesystem
- Repair a non-root filesystem
- Monitor filesystems
- Locate and manage user files
- Manage system log files and temporary directories

AV 5-1: Working with Filesystems

This slide describes the overall topics covered in this lesson.

AV 5-2



Instructor Guide

5.1 Describing Filesystem Basics

AV 5-2: One Directory — Several Filesystems

This graphic illustrates that several filesystems can make up the hierarchical directory structure that users see. When the students change directory to `/home`, they are accessing a different filesystem.

Understanding what a filesystem is will help you manage user data efficiently. Filesystems must be handled properly to prevent data corruption. The capabilities of each filesystem type differ.

Although a user sees all data organized as a single hierarchical directory structure, that directory structure can consist of more than one filesystem.

A UNIX filesystem is a data structure that stores files. All files in the UNIX hierarchical directory structure are stored in filesystems. Filesystems hold all regular, special, and directory files, as well as the information needed to locate and access them.

A filesystem contains files much as a library bookshelf holds books. Like bookshelves, filesystems can fill up—and when a filesystem is full, it cannot hold any more data.

Permanent filesystems can reside on hard disks, floppy disks, CD-ROMs, and in RAM. RAM filesystems are not permanent; they disappear along with their contents when you turn off the system.

Filesystems must be *mounted* to be available for use.

Filesystems are *unmounted* when they are no longer available for use.

5.2 Using Different Filesystem Types

The HTFS, DTFS, and EAFS filesystem types are not supported in UnixWare 7. At this time there is not an “upgrade” path for these filesystem types. Students should use the SCO OpenServer™ **cpio(C)** command to back up filesystems and the **cpio(C)** command found in */OpenServer/bin* to restore the data on a UnixWare 7 system. The S5 filesystem is compatible with the OpenServer filesystem.

Filesystem types differ in capabilities that can affect how they are used. The most frequently used filesystem types are:

<i>vxfs</i>	The Veritas filesystem. This is the default type created for root and user filesystems. It provides enhanced performance and reliability.
<i>bfs</i> (boot filesystem)	Is a special-purpose filesystem that contains all the stand-alone programs, such as unix (located in <i>/stand</i>), and the text files necessary for boot procedures.
<i>dosfs</i> (DOS filesystem)	Lets users access DOS-formatted floppies and hard disk partitions using UNIX system commands and calls.
<i>cdfs</i> (CD-ROM filesystem)	Supports ISO-9660 and the High Sierra file system format specifications.
<i>memfs</i> (memory filesystem)	Is a high-performance, volatile memory filesystem type.
<i>nucfs</i> (NetWare® UNIX client filesystem)	Provides NetWare client file services on a UnixWare 7 platform.

The *s5*, *ufs*, *sfs* are standard UNIX filesystems that are available for compatibility with other UNIX systems. The *vxfs* is the most feature-rich filesystem available with UnixWare 7.

5.2.1 Default *vxfs* features

The *vxfs* filesystem provides enhancements that increase the UnixWare 7 usability and make the system more viable for use in the commercial marketplace. It is particularly useful in environments that require high performance and availability and deal with large volumes of data.

The *vxfs* filesystem is available in two forms:

- Base *vxfs*
- Separately licensed *vxfs* advanced feature set, which provides additional functionality and better performance

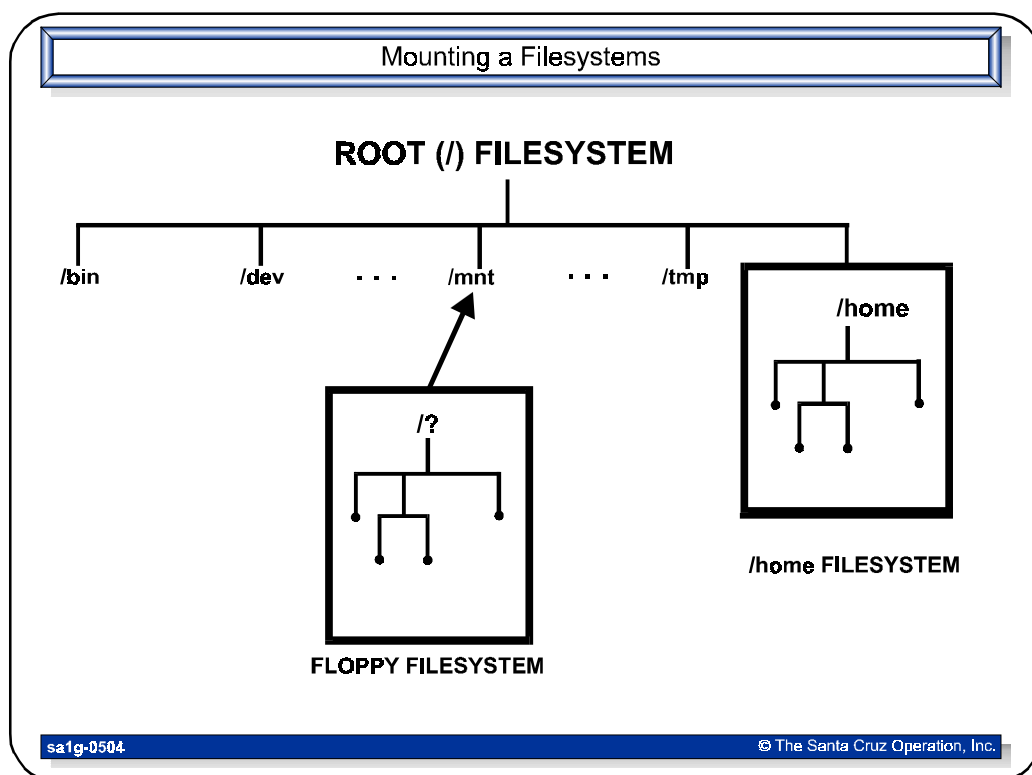
The base *vxfs* filesystem:

- Supports a maximum file and filesystem size of 1TB. The default is 2GB.
- Uses intent logging. The filesystem transactions are recorded in a log and then committed to disk. This increases system recovery speed with a very small performance penalty.

Using extents means that disk I/O to and from a file can be done in units of multiple blocks. This type of I/O can occur if storage is allocated in units of consecutive blocks. For sequential I/O, multiple block operations are considerably faster than block-at-a-time operations. Almost all disk drives accept I/O operations of multiple blocks.

- Supports extent-based allocation. An extent is defined as one or more adjacent blocks of data within the filesystem. When storage is added to a file on the *vxfs* filesystem, it is grouped in extents rather than being allocated one block at a time.
- Provides enhanced data integrity. If the system crashes or is shutdown improperly, only files that are currently being written to media can lose data.
- Supports a default logical block size of 1KB. Can support block sizes of 2048, 4096, and 8192 bytes.
- Supports filesystem concatenation.
- Is not a bootable filesystem.

AV 5-3



Instructor Guide

5.3 Mounting and Unmounting a Filesystem

Filesystems allow easy expansion of the hierarchical directory structure because storage can be added to the system in a completely seamless manner. For example, if you make a floppy disk available to users, the filesystem on it appears within the existing directory structure. The user cannot distinguish between data on the floppy disk and data on the hard disk.

When the filesystem data is no longer needed, unmount the filesystem.

5.3.1 Describing filesystem information

AV 5-3: Mounting a Filesystem

This graphic illustrates the mounting process. Specifically, the root (/) directory of the filesystem to be mounted is given the name of the mount point directory.

A directory file contains the name of the file and its inode. When you mount a filesystem, the first entry in the mount point directory points to the root (/) directory of the mounted filesystem.

Most permanent filesystems are mounted at boot time. Floppy and CD-ROM filesystems are mounted on occasion and only when the media is in the proper drive. When you mount a filesystem, you are attaching it to the current directory structure. You must have these two pieces of information:

- The device file that is associated with the filesystem.
- The existing directory on which to mount the filesystem. This is known as the *mount point*.

5.3.1.1 Filesystem device files

The primary floppy device, `/dev/fd0`, is linked to `/dev/dsk/f03ht`. This file represents a 3.5 inch high-density floppy device located in floppy drive 0. The CD-ROM device is `/dev/cdrom/c1b0t510`.

Each filesystem has an associated device file. Common filesystems with their respective device files include:

The <i>root</i> filesystem	<code>/dev/root</code>
Primary floppy disk	<code>/dev/dsk/f03ht</code>
Primary CD-ROM	<code>/dev/cdrom/c1b0t510</code>

5.3.1.2 Mount point

A mount point is an existing directory. When a filesystem is mounted, the directory entry for the mount point is redirected to the root (/) directory of the filesystem.

5.3.2 Adding the mount configuration

Explain to students that adding the mount configuration is automatically done through the install process of most hard disk filesystems.

Before a floppy filesystem can be mounted using the **Filesystem Manager** you must first add the mount configuration.

Mount configuration information includes:

- If it is a local device or one that is installed on a remote system
- The device file
- The mount point. If the mount point directory contains any files, you are not able to access those files as long as a filesystem is mounted to that point. Specify the mount point as an absolute pathname. The mount point should always be an empty directory.
- Filesystem type
- Access mode
- When to mount it. Mount it now or during system startup.

The Advanced Options let you specify the type of Intent Logging used for this filesystem. By default all transactions are logged before the system call is returned to the application. Delayed Mode allows less logging and Temporary Mode allows almost no logging. These modes increase system throughput at the expense of data integrity. Clear Blocks before allocating to a file ensures that existing data is always overwritten with zeroes before disk space is released. The default is no, increasing system throughput.

For example, to add the mount configuration and mount a floppy filesystem:

Step 1. Start **SCOadmin**. Select **Filesystem Manager**.

Step 2. Specify the device file. For example, to mount a 3.5 inch, 1.44MB floppy, enter:

`/dev/dsk/f03ht`

- Step 3. Insert the floppy disk into the floppy drive. The filesystem type is determined. Click on **Continue**.
- Step 4. Specify the mount point, enter:
- /mnt*
- Step 5. Enter a description of the floppy. This step is optional.
- Step 6. Specify the access mode. The filesystem can be *read-only* or *read-write*.
Click on **read-write**.
- Step 7. Specify when to mount the filesystem:
- **Now** mounts the filesystem immediately.
 - **At System Startup** mounts the filesystem when the system enters multiuser mode. This option is not recommended for a floppy disk filesystem unless you have access to the floppy drive during startup.
- Click on **Now**.
- Step 8. Click on **OK**. The filesystem is mounted.
- To unmount the filesystem:
- Step 9. Select the filesystem:
- /dev/dsk/f03ht*
- Step 10. Click on **Mount** ⇨ **Unmount** ⇨ **Yes**.
- Step 11. Select **Host** ⇨ **Exit** to exit the **Filesystem Manager**.

Exercise: Mounting and unmounting a floppy disk filesystem

Following the steps in Section 5.3.2, “Adding the mount configuration,” on page 5-12 to add the mount configuration for a floppy disk filesystem. Mount and unmount the filesystem.

5.3.3 Mounting a filesystem

You can also use the **mount**(1M) command to mount a filesystem. For example to mount a *vxfs* filesystem floppy on the */mnt* directory:

```
mount -F vxfs /dev/dsk/f03ht /mnt
```

The *mount_point* directory does not need to exist immediately under the root (*/*) directory. Any subdirectory can be a mount point.

A CD-ROM filesystem must be mounted as *read-only*. For example, to mount a CD-ROM using the primary drive on the */mnt* directory, use this command:

```
mount -r /dev/cdrom/c1b0t5l0 /mnt
```

■ The filesystem floppy should be unmounted from the previous exercise. If not, remind students to do so.

Exercise: Mounting a floppy disk filesystem

Mount the *vxfs* floppy disk filesystem on the */mnt* directory using the **mount**(1M) command. Change to the */mnt* directory. Copy the */etc/default/tar* file to the filesystem floppy. List the contents. Do not umount the floppy.

5.3.4 Why mounting can fail

If a mount operation fails, check for these situations:

- Have you specified a non-existent device file or mount directory?
- If mounting a floppy disk or CD-ROM, is the media in the drive?
- Are you or someone else in the mount directory using a file? Use **fuser**(1M) to determine if anyone is using the directory:

```
fuser -u /directory
```

This command normally displays the process ID of any process accessing that directory. The **-u** option also displays the user who owns the process. Use the **-ku** option to display the user and to send a kill signal to the process.

5.3.5 Unmounting a filesystem

To unmount a filesystem, users, including root, cannot be using the directory as their present working directory. Also, no one should be using any of the files in the filesystem.

Use **fuser -u** to determine if anyone is using the filesystem:

fuser -u /dev/filesystem_device

To unmount a *vxfs* filesystem floppy from the command line, use the **umount(1M)** commands:

umount /dev/filesystem_device

■ Practice unmounting a filesystem. The students should remount the filesystem for future exercises.

Exercise: Unmounting a floppy disk filesystem

Unmount the floppy disk filesystem, then mount it again on the */mnt* directory.

5.4 Repairing a Non-root Filesystem

If a filesystem becomes corrupt, you must repair it before you can use it safely. When a filesystem mounts during startup, the system usually checks and repairs it transparently without intervention before mounting it.

Check the filesystem manually under the following conditions:

- The filesystem is not mounted during startup.
- The filesystem is configured to be mounted during startup, but the system is not configured to check it.

5.4.1 Causes of filesystem corruption

When a filesystem becomes corrupted, either the actual data or the structures used to locate the data become damaged. Several situations can cause filesystem corruption:

- Hardware failure
- Program failures; for example, an error occurs that causes a program to fail, possibly resulting in data loss
- System crash

If filesystem corruption occurs, when you reboot the system, the root filesystem is automatically cleaned and repaired. Any user filesystems (if configured to do so) are also cleaned and repaired.

5.4.2 The *lost+found* directory

While repairing a filesystem, the system will attempt to recover any lost files and put them in the *lost+found* directory located in each filesystem. After a filesystem repair, check this directory for lost files.

5.4.3 Repairing a non-root filesystem manually

■ You cannot repair filesystems using the **Filesystem Manager**.

The **fsck(1M)** command is used to manually check and repair a filesystem. Before running **fsck**, you must determine the filesystem type using the **fstyp(1M)** command. Most user filesystems are of the *vxfs* type.

One of the features of the *vxfs* filesystem is to record pending filesystem updates in an *intent log*. This reduces the amount of time that **fsck** uses to repair the filesystem as only transactions in the intent log are checked. This is the default.

If a full filesystem check is required, run **fsck** with the **-ofull** option.

WARNING: Do not perform this procedure on the *root* filesystem.

Follow these steps to repair the */dev/dsk/f03ht* filesystem:

Step 1. Determine the filesystem type.

```
fstyp /dev/dsk/f03ht
```

Step 2. Umount the filesystem.

```
umount /dev/dsk/f03ht
```

If students ask about the difference between */dev/dsk* and */dev/rdisk*, explain that different commands are executed on different device types. This is covered in the **UnixWare 7 System Administration II** class.

Step 3. Run **fsck**.

```
fsck -F vxfs /dev/rdisk/f03ht
```

If a full check is required, enter:

```
fsck -F vxfs -ofull /dev/rdisk/f03ht
```

Step 4. Mount the filesystem.

```
mount /dev/dsk/f03ht /mnt
```

Exercise: Repairing a floppy disk filesystem

Check and repair the floppy filesystem.

AV 5-4

Filesystem Manager Disk Usage

Filesystem	Mount Point	Total (MB)	Used (MB)	Free (MB)	% Used
/dev/dsk/f0t	/install	0.0	0.0	0.0	0%
/proc	/proc	0.0	0.0	0.0	0%
/dev/stand	/stand	23.5	2.7	20.7	12%
/processorfs	/system/processor	0.0	0.0	0.0	0%
/tmp	/tmp	10.0	0.0	9.9	1%
/var/tmp	/var/tmp	40.0	0.0	39.9	1%

Total: 10 items

SCOadmin

sa1g-0505

© The Santa Cruz Operation, Inc.

Instructor Guide

5.5 Monitoring Filesystems

When a filesystem comes close to being full, performance starts to suffer. If the filesystem actually fills up, users and programs cannot save any data to the filesystem. Never allow a filesystem to completely fill up.

UnixWare 7 filesystem performance begins to degrade when filesystem free space drops below 15%. As the system administrator, it is your responsibility to keep track of filesystem usage.

5.5.1 Determining filesystem free space

AV 5-4: Filesystem Free Space

Screen shot of the **Filesystem Manager** disk usage display.

The first statistic you should check is overall usage. These steps describe how to check the free space on all mounted filesystems:

Step 1. Start **SCOadmin**.

Step 2. Select **Filesystem Manager** ⇒ **View** ⇒ **Disk Usage**.

Note the list displays the total size of each filesystem, the number of megabytes used, the number of megabytes free, and the percentage of the filesystem used.

Step 3. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

Use the **df(1)** command to check the free space on all filesystems. From the command line, enter:

df -k

To check free space on a single filesystem, enter:

df -k /dev/filesystem_name

The **-k** option displays the size in 1KB blocks.

AV 5-5.

Determining the Size of a Directory

```
# du -ks /etc
16352      /etc
```

SIZE IN 1K BLOCKS

-s: DISPLAY GRAND TOTAL
-k: DISPLAY SIZE IN 1K BLOCKS

sa1g-0506© The Santa Cruz Operation, Inc.

Exercise: Determining free space on a filesystem

Use the **Filesystem Manager** to determine how much free space is in each of the filesystems.

5.5.2 Determining the size of a directory

AV 5-5: Determining the Size of a Directory

Screen shot of a sample **du(1)** command.

If a filesystem is close to being full, you can determine if a particular directory seems inordinately large. This can help determine if there are files that you can remove to free disk space.

Use the **du(1)** command to locate the directories using the most disk space:

du /home | sort -nr | head

The **-n** option sorts by numeric value. The **-r** option reverses the order of the sort so that the directories using the most disk space are first.

This exercise lets students practice locating large directories. Depending on the size of the filesystem, this command can take several minutes to run.

Exercise: Identifying the largest directories

Determine the ten largest subdirectories on the */home* filesystem.

AV 5-6

Determining Disk Usage by a User

#quot	/dev/u
312348	john
86298	mary
5024	sue
⋮	

SIZE IN 512 BYTE BLOCKS

sa1g-0507 © The Santa Cruz Operation, Inc.

5.5.3 Determining disk usage by user

AV 5-6: Determining Disk Usage by User

Screen shot of a sample **quot(1M)** command.

Some administrators list the top ten users of disk space in */etc/motd* as a reminder to those users to cleanup their files.

If a filesystem is close to full, you can check how much space each user is occupying. If a few are using an inordinate amount of space, you might request that they clean up their files.

Use the **quot(1M)** command to determine space used by each user. It is reported in 1KB blocks.

For example, to determine the space used by each user in the */home* filesystem, enter:

quot -F vxfs /home

This exercise lets the students practice using **quot(1M)**. Ask the students to convert the output to megabytes.

Exercise: Determining disk usage

Determine disk usage by user for the *root* filesystem. Remember to specify the filesystem type.

5.6 Locating and Managing User Files

Throughout normal operation, both users and programs save files to a filesystem. Most of these files are normal data files, but some can be *core* files. A core file can be created when a program fails. Maintain free disk space by periodically deleting these files.

Additionally, when you remove a user account, you need to decide what to do with files owned by that user. You can transfer ownership to another user or delete the files. Ignoring them can use valuable free space.

You can also track large files as a way to manage free space. If an individual file is growing, or if there is an increasing number of large files, adjust your filesystem organization to compensate for usage.

In any of these situations, the **find**(1) command will help you manage user files.

5.6.1 Finding large files

Use the **find** command with the **-size +n** option (the size of the file in 512-byte blocks) to find files larger than a specific size:

```
find / -size +n
```

5.6.2 Finding files by owner

Use the **find** command with the **-user** option to find files owned by a specific user:

```
find / -user username
```

5.6.3 Finding and removing *core* files

A *core* file is created when a program aborts either from an error or from receiving a “quit” signal from a user ({CTRL} \ or **kill -3**). The file is always named *core.pid#* and contains a copy of the terminated program. The *pid* is the process id of the aborted process.

Use the **find**(1) command to automatically delete core files:

```
find / -name 'core.*' -exec rm {} \;
```


Use the **find(1) -ok** option or the **rm(1) -i** option if you would rather be prompted before deleting each file:

```
find / -name core.* -ok rm {} \;
```

Exercise: Deleting *core* files

First, create a *core* file using the **sort(1)** command:

```
sort /etc/termcap
```

While the command is running, press  \. Now use the **find(1)** command to delete all *core* files on the system.

5.7 Managing System Log Files and Temporary Directories

The UnixWare 7 system maintains several log files that contain information about system usage. When new information is generated, the system appends it to the appropriate log file, preserving the previous contents of the file.

Because some log files can rapidly become quite large, check these files periodically, and if necessary, clear them by deleting their contents.

A temporary file contains data created as an intermediate step during execution of a program. This file can be left behind if a program encounters an error or a user stops it prematurely. In most cases, the user has no use for temporary files, and you can safely remove them.

5.7.1 Clearing key system logs

The command line used in the *Student Guide*:

> *log_filename*

Uses the I/O redirection feature of the Bourne shell to zero out the file size without changing other file attributes. This command does not work if the students are using the C shell. For the C shell use `cp /dev/null log_filename`.

You might want to print or archive a log before clearing it. Do not delete a log file because the file ownership and permissions can change when it is recreated. Instead, enter the following:

> *log_filename*

Many of the system log files are stored in the `/var/adm` directory. Some of the key log files are:

<i>loginlog</i>	Contains unsuccessful login attempts
<i>su</i> <i>log</i>	Contains su (1) attempts
<i>syslog</i>	Contains system startup information and errors
<i>wtmp</i>	Contains a history of all logins

5.7.2 Using the System Logs Manager

The **System Logs Manager** lets you add system log files so that you can easily view, print, and clear them.

Use the **SCOadmin System Logs Manager** to manage log files:

Step 1. Start **SCOadmin**. Select **System** ⇒ **System Logs Manager**. To:

Add a log file. Select **Log** ⇒ **Include Log**.

Or you can select a log file and:

Remove. Select **Log** ⇒ **Exclude Log**.

Clear. Select **Log** ⇒ **Clear Log**.

View. Select **File** ⇒ **View content**.

Print. Select **File** ⇒ **Print**.

Save. Select **File** ⇒ **Save as**.

Step 2. Select **Host** ⇒ to exit the **System Logs Manager**.

5.7.3 Clearing key temporary directories

These directories include:

- *lost+found* (for each filesystem)
- */tmp*
- */usr/tmp*

Check these directories periodically and remove older files.

5.8 Lesson Summary

Filesystems store data and programs used on the system. As an administrator, mount filesystems to make the data available. When a filesystem becomes corrupt, it must be cleaned before using it again.

Monitoring and managing disk space assures that the system can continue to support your users' work. Monitoring can provide you with information that helps you decide when disk upgrades and additions are necessary.

Review questions

1. What must occur before a user can access the files on a filesystem?

Before a user can access the files on a filesystem, the filesystem must be mounted.

2. Which filesystem type is the default used by UnixWare 7?

The default filesystem type used by UnixWare 7 is vxfs.

3. List three situations that might cause a mount command to fail.

Three situations that can cause a mount to fail are: specifying a non-existent device file or mount directory; mounting a floppy disk or CD-ROM without the media in the drive; or someone is either in the mount directory or using a file in the mount directory.

4. If the system is cleaning the `/home` filesystem, in which directory will recovered files be stored?

If the system is cleaning the `/home` filesystem, recovered files are stored in `/home/lost+found`.

5. Which command shows how much space each user is utilizing on a filesystem?

■ The `du(1M)` command shows how much space each user is using in the filesystem.

6. How would you find every file on the system that is larger than 3MB?

■ To find every file on the filesystem that is larger than 3MB, enter: `find / -size +6144`.

7. Should you clear, rather than delete, a log file?

■ It is better to clear a log file rather than delete it because file permissions and ownership are also deleted.

5.9 Lab: Working with a Floppy Disk Filesystem

This lab emphasizes the difference in a directory on which a filesystem is mounted.

5.9.1 Overview

If the floppy filesystem is still mounted, unmount it. Copy `/etc/default/passwd` to `/mnt` and write down the contents of `/mnt`. Mount a floppy disk filesystem on `/mnt`. Copy `/etc/default/login` to that filesystem and write down the contents of `/mnt`. Unmount the floppy filesystem and record the contents of `/mnt`. Compare the contents of `/mnt` when the floppy filesystem is mounted and when it is not.

5.9.2 Procedure

In this procedure, unmount the floppy disk filesystem (if it is mounted), copy a file to */mnt*, and record the original contents of that directory. Next, mount the floppy disk filesystem, copy a different file to */mnt*, and record the contents. Then, unmount the floppy disk filesystem, examine the contents of */mnt*, and compare the directory listings.

Step 1. Use the **umount(1M)** command to unmount the floppy disk:

```
umount /mnt
```

Step 2. Copy */etc/default/passwd* to */mnt*:

```
cp /etc/default/passwd /mnt
```

Step 3. Obtain a directory listing of */mnt* and record the output.

```
l /mnt
```

Step 4. Start **SCOadmin**. Select **Filesystem Manager**.

Step 5. **Select Mount** ⇒ **Add Mount Configuration** ⇒ **Local**.

Step 6. Enter **/dev/dsk/f03ht** for the **Device File**, **/mnt** for the **Mount Point**, and select **Now** for **When to Mount**. Verify that **At System Startup** is *not* selected for **When to Mount**.

Step 7. Click on **OK**.

Step 8. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

Step 9. Copy */etc/default/login* to the floppy disk filesystem:

```
cp /etc/default/login /mnt
```

Step 10. Obtain a directory listing of */mnt* and record the output:

```
l /mnt
```

Step 11. Start **SCOadmin**. Select **Filesystem Manager**.

Step 12. Select the **/dev/dsk/f03ht** filesystem.

Step 13. Select **Mount** ⇒ **Unmount**.

- Step 14. Click on **Yes** to verify the operation.
- Step 15. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.
- Step 16. Obtain a directory listing of */mnt* and record the output:
- l /mnt**
- Step 17. Compare the directory listings from Step 3, Step 10, and Step 16.

5.10 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

df (1)	Reports number of free disk blocks
du (1)	Summarizes disk usage
find (1)	Finds files
fsck (1M)	Checks and repairs filesystems
fstyp (1M)	Determines filesystem type
fuser (1M)	Identifies processes using a filesystem or directory
mount (1M)	Mounts a filesystem
quot (1M)	Summarizes filesystem ownership
scoadmin (1M)	Invokes SCOadmin applications (in this lesson, the Filesystem Manager)
umount (1M)	Unmounts a filesystem

Relevant files

<i>/etc/wtmp</i>	Accounts record file
------------------	----------------------

5.11 Answers to Exercises and Review Questions

This section contains answers to exercises and review questions presented in this lesson.

Review questions

1. Before a user can access the files on a filesystem, the filesystem must be mounted.
2. The default filesystem type used by UnixWare 7 is *vxfs*.
3. Three situations that can cause a mount to fail are: specifying a non-existent device file or mount directory; mounting a floppy disk or CD-ROM without the media in the drive; or someone is either in the mount directory or using a file in the mount directory.
4. If the system is cleaning the */home* filesystem, recovered files are stored in */home/lost+found*.
5. The **quot(1M)** command shows how much space each user is using in the filesystem.
6. To find every file on the filesystem that is larger than 3MB, enter: **find / -size +6144 .**
7. It is better to clear a log file rather than delete it because file permissions and ownership are also deleted.

6

Working with Disks and Tapes

Instructor Guide

Instructor Guide

Lesson 6

Working with Disks and Tapes

Suggested lesson duration

This lesson should take approximately 2.5 hours to complete, including the lab exercise.

Pre-lesson classroom preparation

Each student must have a blank floppy for use with this lesson. ARCserveIT 6.6 does not lock the tape drive.

Instructor preparation

Review the manual pages for the **tar**(1), **cpio**(1) and **find**(1) commands. Practice using the **tar**(1), **cpio**(1) and **find**(1) commands.

AV 6-1

Instructor Guide

Working with Disks and Tapes

- Work with floppy disks
- Work with tape drives
- Transfer data to tape or disk using the **tar(1)** and **cpio(1)** commands

sa1g-0601 © The Santa Cruz Operation, Inc.

Introduction

There are times when you will copy one or more files to another system. If the two systems are not networked together, copying the files to a floppy disk is the easiest way to do this.

You might also need to duplicate one or more directories on another system. If the amount of data is large, it can require many diskettes. Transferring the data by tape is the quickest way to accomplish this.

Objectives

This lesson covers all of the common ways to transfer data using both floppy disks and tapes. By the end of this lesson, you will be able to:

- Work with floppy disks
- Work with tape drives
- Transfer data to tape or disk using the **tar**(1) and **cpio**(1) commands

AV 6-1: Working with Disks and Tapes

This slide describes the overall topics covered in this lesson.

AV 6-2

Floppy Disk Device Names

Name	Capacity	Size
f015ht	1.2MB	5.25 inch
f03ht	1.44MB	3.5 inch
f03et	2.88MB	3.5 inch

Examples: Floppy Disk 0 3.5 inch 1.44MB /dev/rdisk/f03ht
Floppy Disk 1 5.25 inch 1.2MB /dev/rdisk/f115ht

sa1g-0602

© The Santa Cruz Operation, Inc.

6.1 Working with Floppy Disks

Transfer data with floppy disks using these guidelines:

- Know the correct device file to use for a specific floppy disk
- When transferring data to a floppy disk, format the disk before using it

6.1.1 Identifying floppy device names

AV 6-2: Floppy Disk Device Names

This graphic shows how the floppy disk device names are constructed. The first part of the graphic identifies the floppy disk drive type. The second part shows how that integrates with the rest of the device name.

The standard UNIX data transfer commands use device files. Each floppy disk type is represented by a device file.

Floppy devices use these naming conventions:

- The *dsk* designates a block device interface. Block devices use the buffer cache, providing fast, high level access.
- The *rdsk* indicates a raw (character) interface. Raw device files bypass the buffer cache. They are sometimes used by special applications and databases that maintain their own high performance hardware cache when storing data.

The **format(1M)** command uses the raw floppy device.

- The *0* or *1* selects the drive to be accessed: *f0* selects floppy drive *0*, *f1* selects drive *1*.

This list further describes the 3.5" floppy devices:

3e	3.5" extra high density floppy disk (2.88MB)
3h	3.5" high density floppy disk (1.44MB)
3d	3.5" double density floppy disk (720KB)

AV 6-3

Floppy Disk Attributes

```
alias='mdens1HIGH'
bdevice='/dev/dsk/f03ht'
bdevlist='/dev/dsk/f03h'
capacity='2844'
cdevice='/dev/rdisk/f03ht'
cdevlist='/dev/rdisk/f03h'
copy='true'
desc='3.5 inch 1.44 Mbyte (High Density)'
display='false'
erasescmd='/usr/sadm/sysadm/bin/floperase /dev/rdisk/f03ht'
fmtcmd='/usr/sbin/format -v /dev/rdisk/f03ht'
mdenslabel='dtmedia:293^1.44 Mbyte'
mkdtab='true'
mkfscmd='/sbin/mkfs -F s5 /dev/dsk/f03ht 2844:711 2 36'
mkvxfsd='/sbin/mkfs -F vxfs -o ninode=711 /dev/dsk/f03ht
2844'
mountpt='/install'
removable='true'
type='mdens'
volume='diskette'
```

sa1g-0603

© The Santa Cruz Operation, Inc.

6.1.2 Formatting a floppy disk

Use the **format(1M)** command to format a new floppy disk before using it.

AV 6-3: Floppy Disk Attributes

Use this slide to show students the complete output of the **devattr(1M)** command. Note that this information is coming from the device file, not the floppy disk. For an explanation of the attributes listed, refer to the **putdev(1M)** manual page. Because filesystem floppies were previously used, you might want to point out the command that creates a filesystem floppy.

If you don't know the floppy device name, use the **getdev(1M)** command to identify the device name:

```
getdev | pg
```

A list of all device names display.

To further distinguish the device, enter:

```
devattr -v diskette1
```

To view the attributes of a specific floppy device file, enter:

```
devattr -v /dev/rdisk/f03ht
```

Important attributes to note before formatting a floppy include:

- The description of the device.
- The command to use to format the floppy device (**fmtcmd=**).

To format a floppy disk, enter:

```
format -v /dev/rdisk/f03ht
```

The **-v** option (verbose) displays the formatting information.

This exercise lets students practice formatting a disk.

Exercise: Formatting a floppy disk

Format a floppy disk.

6.2 Working with Tape Drives

Follow these guidelines when transferring data with tapes:

- Know the correct device file to use for a specific tape drive
- If you receive a tape that includes data, you must know how the data was transferred to it. Label your tapes. The label should include, a description of the archive, the date of the archive, the size of the tape, the command the tape was archived with, and the number of tapes in the archive.

Computer tapes share some of the same limitations as audio tapes. The tape can develop slack, which can lead to data errors. Tapes need to be rewound before you can access data on them. Just as you can format floppy disks to remove data, you can also erase data from tapes.

The next section addresses the steps for preparing your tape for use.

6.2.1 Identifying tape device names

A tape drive (whether for a cartridge, 9-track, 8-millimeter, or DAT tape) is a character device and uses device names in the `/dev/rmt` directory.

Five character device files describe your tape drive. They include:

<code>/dev/rmt/ctape1</code>	Non-retensioning rewinding device.
<code>/dev/rmt/ntape1</code>	Non-retensioning, non rewinding device.
<code>/dev/rmt/rtape1</code>	Retensioning and rewinding device.
<code>/dev/rmt/nrtape1</code>	Retensioning non rewinding device.
<code>/dev/rmt/utape1</code>	Unloads on the device close.

6.2.2 Working with tapes

The **tape(1)** command is provided for backward compatibility with SCO OpenServer Release 5. Encourage users to use **tapecntl(1)**.

ARCserveIT 6.6 does not lock the tape drive.

You can retention, rewind, or erase tapes using the **tapecntl(1)** command. Depending upon the type of tape drive installed, there are also other options available. To determine which options are available, enter:

tapecntl

You can use the **tapecntl** command with any tape device. If you do not specify a device, **/dev/rmt/ntape1** is used. Use the **tapecntl** command to:

- Reset a tape. This option initializes the tape controller and positions the tape at the beginning of the tape.

tapecntl -r

- Rewind a tape. This option moves the tape to the beginning of the tape.

tapecntl -w

- Erase a tape. This option erases the tape from beginning to end.

tapecntl -e

- Use a tape drive other than the default by specifying the appropriate device file at the end of the command. For example, to retention a tape using a cartridge tape drive, enter:

tapecntl -t /dev/rmt/ctape1

You can show students any of the **tapecntl** options.

Exercise: Using the tapecntl command.

List the **tapecntl** options that are available for use with your tape drive. Is the unload option available? If so, unload your tape from your tape drive.

6.3 Transferring Data to Tape or Disk

The two major data transfer utilities are **tar**(1) and **cpio**(1). Both commands can copy files and directories. They also have advantages and limitations. This section addresses when and how to use these commands.

6.3.1 Absolute versus relative pathnames

You can specify files to transfer using either absolute or relative pathnames. The method you use to create an archive affects how you restore data from that archive.

6.3.1.1 Absolute pathnames

When using absolute pathnames, specify the file location relative to the root (/) directory.

The default behavior when restoring the file is to place it in the original location in the directory tree. For example, when creating the archive */etc/default/login*, you can create the archive from within any directory. You can also restore the file from any directory, and the file is placed in */etc/default*.

You can override absolute pathnames during a restore.

6.3.1.2 Relative pathnames

When using relative pathnames, specify the file location relative to the current working directory.

The default behavior when restoring the file is to place it in a location relative to the current working directory. For example, your current directory is */etc/default*. To specify a relative pathname, use *./login* to designate the file. If you restore the file while in the */tmp* directory, the file *login* is restored to */tmp*.

6.3.2 Transferring symbolically linked files

The root filesystem contains files that are symbolically linked. When performing a directory listing, a symbolically linked file displays as:

```
lrwxrwxrwx 1 root sys                8 Apr 23 15:02      lib -> /usr/lib
```

The contents of the */lib* directory are actually stored in the */usr/lib* directory.

When backing up an entire filesystem, all files are archived. However, consider the following when backing up a single directory containing symbolic links:

- If you back up the directory containing the link, the default behavior is to back up the link only, not the data
- With both **cpio**(1) and **tar**(1), the **L** option backs up the actual data associated with the link. However, if you restore the file, the link is broken and the data now exists in that directory.

If you want to backup the actual data and preserve the links, you must back up both the directory containing the symbolic link and the directory containing the actual data. In this situation, do not use the **L** option.

AV 6-4

tar(1) Options	
OPTION	DESCRIPTION
v	Verbose (display output)
L	Follow symbolic links
c	Create archive
r	Append to archive
t	Table of contents
x	Extract from archive
#	Archive device in <i>/etc/default/tar</i>

sa1g-0604 © The Santa Cruz Operation, Inc.

Instructor Guide

6.3.3 The tar(1) command

AV 6-4: tar(1) Options

This graphic highlights some of the commonly used **tar**(1) options. Have the students experiment with the commands as you cover them.

The **tar**(1) command can archive only subdirectories that are within 17 levels of subnesting.

The **tar**(1) command saves files on an archive and restores them from that archive. The advantages of **tar** include:

- It is easy to use.
- It can override absolute pathnames when restoring files. In other words, you can specify the final destination of a file even if the archive is created using absolute pathnames.
- The limitations of **tar**(1) include:
- Compatibility problems with systems that have versions of **tar** that do not support archiving empty directories. The UnixWare 7 version of **tar** does not archive empty directories.
- It does not support filename expansion for extracting data.
- Data archives created with **tar** might be difficult to transfer to computer platforms other than UnixWare 7 systems when archives span media.

The default device used by **tar** is specified in */etc/default/tar*. This file also contains references to other devices that **tar** can access. For example, **archive8** points to the primary tape drive.

This exercise lets students set the default **tar**(1) device to the tape drive. If the tape drive is not the default archive device for this class, have the students set it to the appropriate device.

Exercise: Modifying the default device

Edit */etc/default/tar* so that the default device is the tape drive in your system.

AV 6-5

Defining the Default Device in `/etc/default/tar`

```
archive0=/dev/rdisk/f0q15dt      15      1200      n
archive1=/dev/rdisk/f1q15dt      15      1200      n
archive6=/dev/rdisk/f03ht        18      1440      n
.
.
.
archive8=/dev/rmt/c0s0           20       0         y
.
.
.

# The default device in the absence of a numeric or "-f device" argument
archive=/dev/rdisk/f0t           15      1200      n
```

sa1g-0605

© The Santa Cruz Operation, Inc.

6.3.3.1 Copying data

AV 6-5: Defining the Default Devices

This graphic displays the format of */etc/default/tar*. The bottom line shows the default device. Also point out *archive6*, the floppy disk device, and *archive8*, the tape device.

Listed are several examples of creating archives using **tar**(1): Create an archive of */etc/default* using absolute pathnames. Store the archive on the default device:

```
tar cv /etc/default
```

- Create an archive of */etc/default* using relative pathnames. Store the archive on the primary floppy disk, identified as *archive6* in */etc/default/tar*:

```
cd /etc/default
```

```
tar cv6 *
```

- Create an archive of */etc/default*. Store the archive in */tmp/tarfile*:

```
tar cvf /tmp/tarfile /etc/default
```

- Create an archive of a symbolically linked directory.

```
tar cvL6 /directory_name
```

6.3.3.2 Viewing the contents of a tar(1) file

Use **tar tv** to view the contents of an archive:

```
tar tv
```

```
tar tv6
```

```
tar tvf /tmp/tarfile
```

6.3.3.3 Extracting data from a tar(1) archive

■ When overriding the absolute pathname, you must specify the file without the leading slash.

Several examples of extracting data from a **tar(1)** archive include:

- Restore the entire archive from the primary floppy disk to */tmp*:

```
cd /tmp
```

```
tar xv6
```

- Restore the *./login* file from the primary floppy disk to */usr/tmp*:

```
cd /usr/tmp
```

```
tar xv6 ./login
```

- Restore */etc/default/login* from */tmp/tarfile*. Override the absolute pathname and restore it to */tmp*:

```
cd /tmp
```

```
tar xvAf /tmp/tarfile etc/default/login
```

Note that **tar** extracts the entire directory structure under */tmp*.

AV 6-6

cpio(1) Options

Creating an Archive: (vocBL)

v	Verbose
o	Write archive out
c	ASCII header (for moving to different types of systems)
B	Blocking factor set to 5KB
L	Follow symbolic links

Extracting an Archive (vicdumB)

v	Verbose
i	Read archive in
c	ASCII header
d	Create directories as required
u	Copy unconditionally
m	Retain previous modification times
B	Blocking factor set to 5KB

sa1g-0806

© The Santa Cruz Operation, Inc.

6.3.4 The **cpio(1)** command

AV 6-6: **cpio(1)** Options

This graphic highlights some of the commonly used **cpio(1)** options.

The advantages of the **cpio(1)** command include:

- It allows use of filename expansion on extraction.
- It offers an ASCII header option, making it more portable between different platforms that offer **cpio**.
- It is the only standard data transfer utility that accurately archives entire filesystems.
- It can override absolute pathnames when restoring files. In other words, you can specify the final destination of a file even if the archive is created using absolute pathnames.
- Combined with the **find(1)** command it offers a high degree of control and flexibility.

6.3.4.1 Copying data

Use the **-o** option with **cpio** to create an archive. This command must receive a complete file list from *stdin* to back up the data.

The easiest way to generate a current file list is to use the **find(1)** command. Two important options to the **find(1)** command are:

- | | |
|---------------|---|
| -depth | Always true; causes descent of the directory hierarchy to be done so that all entries in a directory are acted on before the directory itself. This can be useful when find(1) is used with cpio(1) to transfer files that are contained in directories without write permission. |
| -mount | Always true; restricts the search to the filesystem containing the directory specified. |

Listed are several examples of creating archives with **cpio(1)**:

- Create an archive of the current directory. Store the archive on the primary floppy drive:

```
find . | cpio -vocBL -O /dev/rdisk/f03ht
```

Because the **c** option is used, this archive can be restored onto a different type of UNIX system. For System V Release 3.2 or earlier system use the **-H odc** option rather than the **c** option.

- Create an archive of `/etc/default` using absolute pathnames. Store the archive on the primary floppy drive:

```
find /etc/default | cpio -voBL -O /dev/dsk/f03ht
```

- Create an archive of the `/stand` filesystem. Store the archive on tape:

```
cd /stand
```

```
find . | cpio -voBL -O /dev/rmt/ctape1
```

6.3.4.2 Viewing the contents of a cpio archive

Use this command to display a table of contents for a **cpio** archive:

```
cpio -Bitv -I /dev/device_name
```

For example, use this command to display the contents of a **cpio** archive on the primary tape drive:

```
cpio -Bitv -I /dev/rmt/ctape1 | pg
```

To print the contents to the default printer, enter:

```
cpio -Bitv -I /dev/rmt/ctape1 | lp
```

6.3.4.3 Extracting data from a cpio archive

Explain to students that if the directory structure does not exist, **cpio** creates the directory structure when extracting the file(s).

Follow these examples when extracting files from a **cpio** archive:

- Extract all files from an archive created with absolute pathnames, enter:

```
cpio -vidumB -I /dev/rdsk/f03ht
```

- Extract a single file archived with an absolute pathname, enter:

```
cd /
```

```
cpio -vidumB -I /dev/rdsk/f03ht /etc/default/login
```


6.4 Copying Data to DOS filesystems

DOS filesystem support is automatically available in UnixWare 7. Students can mount a DOS hard or floppy disk without adding DOS filesystem support to the kernel. Note that doscmds are not supported under UnixWare 7.1. The doscmds can be found on the Skunkware CD-ROM.

UnixWare 7 systems let you integrate DOS applications and files. Although DOS filesystems have a different structure than UNIX filesystems, you can mount them to the UNIX directory structure the same as any other UNIX filesystem. This provides two benefits:

- You can copy, move, rename, and delete files using UNIX commands. This eliminates the need to learn special commands.
- You can back up the files in the DOS filesystems using the same commands that are used to back up UNIX filesystems.

DOS filesystems (character devices) include:

Floppy disks */dev/rdisk/f0t and /dev/rdisk/f1t*

Hard disk partitions */dev/rdisk/c0b0t1d0p(1-4)*

Mounting and unmounting DOS filesystems are the same as for UNIX filesystems, always mount the block device. To mount a DOS floppy disk on the */mnt* directory, enter:

mount -F dosfs /dev/dsk/f03ht /mnt

You cannot execute DOS files and applications from a mounted DOS filesystem; to do this, you must boot DOS from the DOS partition.

This exercise lets students practice mounting and copying files.

Exercise: Using a DOS filesystem

Mount a DOS floppy filesystem on */mnt*. Copy */etc/default/login* to the DOS floppy. Don't forget to unmount the floppy when you are finished.

6.5 Lesson Summary

UnixWare 7 systems provide several ways to back up data to diskette or tape. Each method has its advantages and limitations. The correct tool to use depends upon the job being performed and upon your level of comfort with each tool.

Review questions

1. What is the raw device name for a 3.5-inch, 1.44KB floppy disk drive if it is the second floppy disk drive in the system?

The device name for a 3.5 inch, 1.44MB floppy disk drive, if it is the second floppy disk drive in the system, is `/dev/rdisk/f13ht`.

2. What type of tape device is `/dev/rmt/ctape1`?

The tape device, `/dev/rmt/ctape1` is the first tape device. It is a non-retentioning rewinding tape device.

3. Which **tar**(1) command option backs up the actual data associated with a symbolically-linked file?

The **L** option of the **tar**(1) command backs up the actual data associated with a symbolically linked file.

4. What are the benefits to mounting a DOS filesystem?

Mounting a DOS filesystem has these benefits: you can copy, move, rename, and delete files using the same commands as for UNIX files. This eliminates the need to learn special commands.

6.6 Lab: Creating an Archive and Extracting Selected Files

In this lab, you use the **cpio**(1) and **tar**(1) commands to create archives and extract selected files from them.

6.6.1 Overview

Create a relative backup of the */etc/default* directory to either tape or disk. Rename */etc/default/login*, then restore */etc/default/login* from the archive.

Create a backup of the */dev* directory. Rename */dev/lp2*. Restore */dev/lp2* from the archive.

6.6.2 Procedure

These steps describe how to create an archive and extract selected files:

Step 1. Change directory to */etc/default*:

```
cd /etc/default
```

Step 2. Use the **tar**(1) command to create a relative backup of the directory:

- For a floppy disk, enter:

```
tar cvf /dev/rdisk/f03ht ./*
```

- For a cartridge tape, enter:

```
tar cvf /dev/rmt/ctape1 ./*
```

Step 3. Rename the */etc/default/login* file:

```
mv login login.bak
```

Step 4. View the **tar**(1) archive:

- For a floppy disk, enter:

```
tar tvf /dev/rdisk/f03ht
```

- For a cartridge tape, enter:

```
tar tvf /dev/rmt/ctape1
```

Step 5. Use the **tar**(1) command to extract */etc/default/login*:

- From a floppy disk, enter:

```
tar xvf /dev/rdisk/f03ht ./login
```

- From a cartridge tape, enter:

```
tar xvf /dev/rmt/ctape1 ./login
```

Step 6. Change to the root (*/*) directory.

```
cd /
```

-
- Step 7. Create an archive of the `/dev` directory using **cpio(1)**:
- For a disk, enter:
find /dev | cpio -ov -0 /dev/rdisk/f03ht
 - For a tape, enter:
find /dev | cpio -ov -0 /dev/rmt/ctape1
- Step 8. Change to the `/dev` directory.
- Step 9. Rename `lp2`:
- mv /dev/lp2 /dev/lp2.bak**
- Step 10. View the **cpio(1)** archive:
- For a disk, enter:
cpio -Bitv -I /dev/rdisk/f03ht
 - For a tape, enter:
cpio -Bitv -I /dev/rmt/ctape1
- Step 11. Using **cpio(1)**, restore `/dev/lp2`:
- From a disk, enter:
cpio -ivmu -I /dev/rdisk/f03ht /dev/lp2
 - From tape, enter:
cpio -ivmu -I /dev/rmt/ctape1 /dev/lp2
-

6.7 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

cpio (1)	Copies archives
find (1)	Locates files
tapectl (1)	Maintains tapes
tar (1)	Copies archives

Relevant files

<i>/etc/default/tar</i>	tar (1) device configuration file
-------------------------	--

6.8 Answers to Exercises and Review Questions

This section contains the answers to exercises and review questions presented in this lesson.

Review questions

1. The device name for a 3.5 inch, 1.44MB floppy disk drive, if it is the second floppy disk drive in the system, is `/dev/rdisk/f13ht`.
2. The tape device, `/dev/rmt/ctape1` is the first tape device. It is a non-retentioning rewinding tape device.
3. The **L** option of the **tar(1)** command backs up the actual data associated with a symbolically linked file.
4. Mounting a DOS filesystem has these benefits: you can copy, move, rename, and delete files using the same commands as for UNIX files. This eliminates the need to learn special commands.

7

Backup Administration

Instructor Guide

Instructor Guide

Lesson 7

Backup Administration

Suggested lesson duration

This lesson should take approximately 2 hours to complete.

Pre-lesson classroom preparation

Stock classroom with blank tapes for both students and demonstration use.

Instructor preparation

ARCserve®IT™ v6.6 from Computer Associates® requires 64MB of RAM. Also, ARCserveIT no longer locks the tape device.

This lesson covers restoration of non root filesystems, directories, and files. Recovering a root filesystem is covered in the **UnixWare 7 System Administration II** class. For those not attending this class, refer them to **scohelp** ⇒ **Backup and Restore** ⇒ **Creating and using emergency recovery media**.

Review the online guide, release, and installation notes in **scohelp** ⇒ **Backup and Restore ARCserveIT from Computer Associates**. Practice using ARCserveIT to backup and restore files and filesystems.

AV 7-1

Backup Administration

- Organize and maintain filesystem backups
- Describe ARCserveIT products
- Back up filesystems and files
- Verify a filesystem backup
- Restore filesystems and files
- Schedule unattended backups

sa1g-0701 © The Santa Cruz Operation, Inc.

Instructor Guide

Introduction

The most expensive component of any system is the data. Unlike hardware, lost data is often irreplaceable. To protect this business critical information, routine backups are essential. Maintaining system backups and restoring lost data is an important and common task for system administrators.

Although you can transfer data with the **tar**(1) and **cpio**(1) utilities, you can also use ARCserve®IT™ from Computer Associates®. ARCserveIT provides an easy to use graphical interface, integrated tape device management, and reports.

Objectives

This lesson describes how to use ARCserveIT to perform backups that enable the restoration of a non-root filesystem or critical files. By the end of this lesson, you will be able to:

- Organize and maintain filesystem backups
- Describe ARCserveIT products
- Back up filesystems and files
- Verify a filesystem backup
- Restore filesystems and files
- Schedule unattended backups

AV 7-1: Backup Administration

This first slide describes the objectives covered in this lesson.

7.1 Organizing and Maintaining Filesystem Backups

Filesystem backups are a copy of one or more filesystems saved to a tape. From a filesystem(s) backup, you can restore a single:

- Filesystem or multiple filesystems
- File or multiple files

7.1.1 Deciding when to back up filesystems

Backing up a filesystem when the fewest number of users are logged into the system results in these benefits:

- The backup does not affect system performance during peak times of system use
- Users are not modifying files

7.1.2 Storing backup media

After creating your backups, store them in a secure place. Consider archiving tapes off-site or in a fire safe for additional protection.

WARNING! Store your tapes in a secure location! If an unauthorized person can access your tapes, any data on those tapes is no longer secure.

For correct retrieval, label your tapes with this information:

- System name
- Filesystem name
- Backup date and who performed the backup
- Backup method, list which utility was used to create the backup
- Specify the sequence of volumes if the backup required multiple volumes. For example, specify “1 of 3” to identify the first tape of a backup that required three (3) tapes.
- Rotation date. The date after which a tape can be reused.

7.1.3 Maintaining backup logs

Maintaining a written backup log book for each computer also helps you to keep your backups organized. If you are using a backup utility that does not provide a backup log, for each backup of your system, record this information:

- Filesystem name
- Backup date
- Who performed the backup
- Number of volumes (tapes) required for the backup
- Any problems that occurred during the backup

Online reports are also kept by ARCserveIT. These reports can be printed and placed in your log book:

Activity Log	Contains comprehensive information about the operations performed by ARCserveIT and provides an audit trail of ALL activity
Media Server Log	Provides an audit trail of all media activity

7.2 Describing ARCserveIT Products

There is no *lite* version of ARCserveIT 6.6. An additional product, ARCserveIT 6.6 Changer Option, is available under separate license.

ARCserveIT is a fully featured, high performance data management tool used to back up and restore data on servers and all workstations attached to a network.

ARCserveIT uses the client/server architecture that functions within a group of ARCserveIT servers. The components include:

Web browser	Provides access to all of ARCserveIT operations using Java Applets
ARCserveIT manager	Functions as an information bridge between the browser and back-end services
Command line	Provides access to all ARCserveIT operations from the command line

You do not have to install the Client Agent for a single server.

Client Agent for UNIX	Enables UNIX workstations to be browsed and handles the transfer of data. The client module must be present on all systems that you want to backup or restore. Client Agents are included for:
-----------------------	--

- UnixWare 7 and SCO UnixWare® 2.1x
- SCO OpenServer™ Release 5
- Microsoft Windows 3.x, Windows 95/98, and Windows NT workstations

New features of ARCserveIT include:

Browser must support Java Virtual Machine 1.1.

- Java/HTML Graphical User Interface (GUI) using Netscape Communicator 4.09 on UnixWare 7 and SCO OpenServer Release 5 and Netscape Communicator 4.07 on Windows.
- Multiple SCSI card support. Automatically detects tape drives on all SCSI cards.

- No device locking. Devices can be used by other backup programs, i.e., **tar**(1) and **cpio**(1).
- Other backup methods. You can specify to use either **tar**, **cpio**, or ARCserveIT as the method for backing up files. Note that ARCserveIT cannot restore tapes that are created using the **tar** and **cpio** command-line interfaces.

7.2.1 System requirements

Your system must be configured to meet ARCserveIT 6.6 minimum requirements:

Processor	Pentium Class
Memory	64MB
Disk space	250MB
Tape device	1 SCSI or IDE

7.2.2 Licensing ARCserveIT

ARCserveIT is licensed by default in all editions except the Base and Free UNIX Editions. You must purchase a license if it is not licensed by an edition.

The ability to backup up to 250 machines is included in each license.

7.2.3 Installing ARCserveIT

You can choose to install ARCserveIT during system installation. If not, add it later with the **SCOadmin Application Installer** or the **pkgadd(1M)** command.

For more information on how to install ARCserveIT, **refer to scohelp ⇒ Backup and Restore ⇒ ARCserveIT from Computer Associates ⇒ ARCserveIT Release and Installation Notes ⇒ Installing and removing ARCserveIT products.**

7.2.4 Configuring ARCserveIT

Before presenting this section, explain to students that ARCserveIT is already installed and running. They will not configure it in class. Use this information as a sequence of events, first you install and then configure.

After installing the ARCserveIT component, configure ARCserveIT before using it. You are required to answer several prompts during the configuration:

Primary discovery host	A host that manages ARCserveIT data between a group of machines.
Domain name	One or more ARCserveIT servers can be configured to form a distinct group. This group is referred to as an <i>ARCserveIT domain</i> .
Secondary discovery host	A host which is used when the primary is not available. (Optional)
Port number	The web server port number. The default port number is 6060.
Printer name	Name of printer used for log file printing.
Password	The arcroot account is used to manage ARCserveIT. You must assign the account a password.

To configure ARCserveIT after installation, log in as **root** and enter:

/usr/sbin/asetup

7.2.5 Starting ARCserveIT

The ARCserveIT services are started during configuration. After configuration, ARCserveIT services are automatically started each time the system boots to the networking state.

ARCserveIT is started automatically from the */etc/rc2.d/S96ARCserveIT* file.

If it becomes necessary to manually start ARCserveIT, enter:

/usr/sbin/astart

These ARCserveIT services are started:

ARCserveIT Loader (arcserve)	Responsible for loading and unloading all ARCserveIT services.
The Discovery Service (asdiscovd)	Responsible for starting and monitoring the discovery servers.
Authentication Service (asauthd)	Controls ARCserveIT resources on a per domain basis and verifies a user's permissions associated with each ARCserveIT server.
Scheduler (asqd)	Manages the jobs that are scheduled through the ARCserveIT Manager or from the command line.
Media Server (asmediad)	Handles the transfer of data to and from the media.
Database Server (asdbd)	Keeps track of the jobs run and all of the files backed up or restored by ARCserveIT.
Processing Server (aprocess)	Manages the backup and restoring of current jobs.
Event Logger (asloggerd)	Handles message logging and retrieving.

Use the **astatus** command to list the services started by ARCserveIT.

Exercise: Listing ARCserveIT services

List the services started by ARCserveIT.

7.2.6 Stopping ARCserveIT services

ARCserveIT services are automatically stopped during shut down. If it becomes necessary to manually stop the ARCserveIT services, enter:

/usr/sbin/astop

AV 7-2



7.3 Accessing ARCserveIT

AV 7-2: ARCserveIT Home Page

Show students where the LOG ON button is located on the ARCserveIT home page. If students forget to log on, they are prompted to do so when making their first selection.

You can also start ARCserveIT from your Web Browser by entering **http://localhost:6060**. Replace `localhost` with your machine name.

To access ARCserveIT, follow these steps:

- Step 1. Log in as **root**.
- Step 2. Start **SCOadmin**. Select **ARCserveIT Backup Manager**.

Menu options include:

- **Backup**—Backs up selected files and filesystems or an entire system
- **Restore**—Restores selected filesystems or files
- **Job Status**—Allows you to view and manage jobs currently in the job queue
- **Devices**—Displays information about your tape device and tapes. It is also used to perform tape maintenance.
- **Database**—Displays the amount of space required for a full system backup
- **Merge**—Merges one or more sessions on a given tape into the database
- **Scan** —Scans to see what sessions/files are on a given tape
- **Reports**—Allows you to view and manage logs and reports
- **Profiles**—Allows the **root** user to customize user access to ARCserveIT
- **Media pool**—Is a collection of media managed as a unit

Before making a selection you must log on.

■ Remind students that the **arcroot** password was assigned during the configuration of ARCserveIT.

Step 3. Click on **LOG ON**. Enter the user name **arcroot** and the password. Click on **OK**.

Step 4. Click on **OK** to accept the default host.

7.3.1 Exiting ARCserveIT

Before exiting the **Backup Manager**, you must log off. Continuing with the above steps:

Step 5. Click on **LOG OFF**.

Step 6. Select **File** ⇒ **Exit** to exit **ARCserveIT**.

7.3.2 Setting up user profiles

The **Profiles** menu selection lets the ARCserveIT **arcroot** user customize user access to ARCserveIT. This is done by adding a user to a specific group. The group determines what level of access a user has. Groups include:

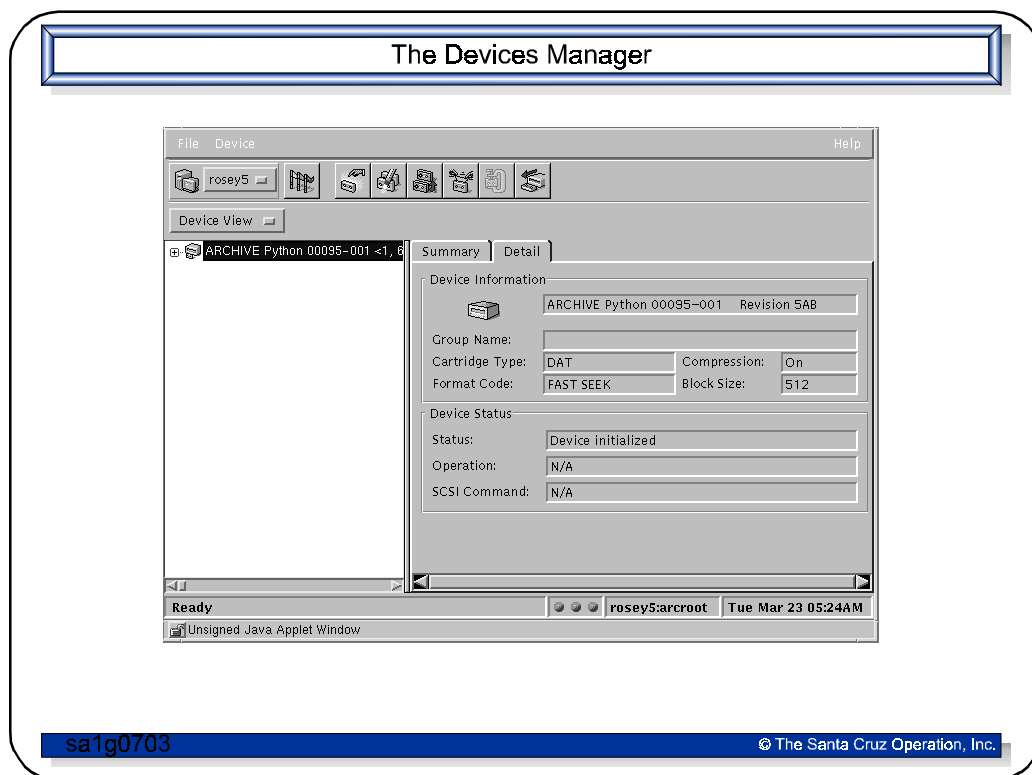
ARCserve Administrator Group	Access to all functions. Equivalent to arcroot .
ARCserve Operator Group	Access to all functions except Profiles
ARCserve User Group	Access to functions required by a user to manage jobs owned by that user. Exceptions include: ● Profiles—can change own password ● Device configuration and media pool modification ● Control over ARCserveIT services (daemons) ● Adding of clients ● Database ● Cannot add or delete groups

7.3.3 Creating a user

From the ARCServeIT main menu, follow these steps to add an ARCServe user:

- Step 1. Select **Profiles**.
- Step 2. Click on the **Add User** icon.
- Step 3. Enter the user name and password. Confirm the password.
- Step 4. Click on the group to which the user belongs. Click on **OK**.

AV 7-3



7.4 Accessing Tape Device(s)

AV 7-3: The Devices Manager

This is a screen shot of the **Devices Manager** with the **Device View** selected.

Use the **Devices Manager** to access important information about your tape device. Before accessing the tape device:

- The tape device must be installed and configured.
- You must log in as **arcroot**.

7.4.1 Selecting devices and device views

The **Devices Manager** provides three ways to view your tape device using a detailed or summary view:

- The **Adapter View** displays information about your host adapters installed on your system.
- The **Device View** displays the name and a description of your tape device.
- The **Group View** displays to which group the device is a member.

To retrieve device information:

Step 1. Select **Devices**.

Step 2. Click on **Device View**. Click on **Detail**.

Important details to note:

- The name of the tape device
- The cartridge type
- Whether the tape device supports data compression
- The status of the tape device

Exercise: Retrieving tape information

Access the **Devices Manager**. What is the cartridge type? Does your tape device support data compression?

7.5 Maintaining Media

ARCserveIT provides three basic tape maintenance functions:

■ Formatting destroys all existing data on the media.

- Formatting—ARCserveIT automatically formats blank media. However, you can use this option to name and manually format your media. You can also assign an expiration date:

Expiration dates are based on how you will use the media. For example, if you are using the media only once a month, set the expiration date to two or three years from the current date.

A media's life is generally based on *passes*. For example, a backup without verification constitutes one pass. With verification, two passes.

■ The expiration date tracks how long a tape has been in service so that you can stop using it before it reaches the end of its useful life. When it reaches its expiration date, information is recorded in the Activity Log.

Media manufacturers rate their media's life span from 500 to 1500 passes. You can use the media beyond the expiration date.

- Erasing—All data is removed from the media and all references to the contents of the media are removed from the database. You can perform three types of an erase:

Quick Erase—Erases the media label. The data is inaccessible.

Quick Erase Plus—Erases the label and allows you to re-label it.

Long Erase—Erases the label and the data.

- Retensioning—Ensures that a tape is evenly wound and properly tensioned. If you are having problems writing to, or reading from a tape, retension the tape.

You can only retension a Quarter Inch (QIC) tape. Do not retension an 8mm or 4mm Digital Audio Tape (DAT).

For example, to perform a Quick Erase of your tape, follow these steps:

- Step 1. Select the **Device Manager**. Verify that you are in the **Device View**.
- Step 2. Click on **Device**. Click on **Erase**.
- Step 3. Click on **Quick Erase**. Click on **OK**.
- Step 4. Click on **OK** for a successful completion.
- Step 5. Click on **File** ⇒ **Close** to exit the **Device Manager**.

7.5.1 Ejecting a tape

You can eject a tape from the **Devices Manager** if your tape device supports automatic ejection.

If you eject a tape that does not support ejection, ARCserveIT acts as though the tape is ejected. Physically eject the tape and reinsert.

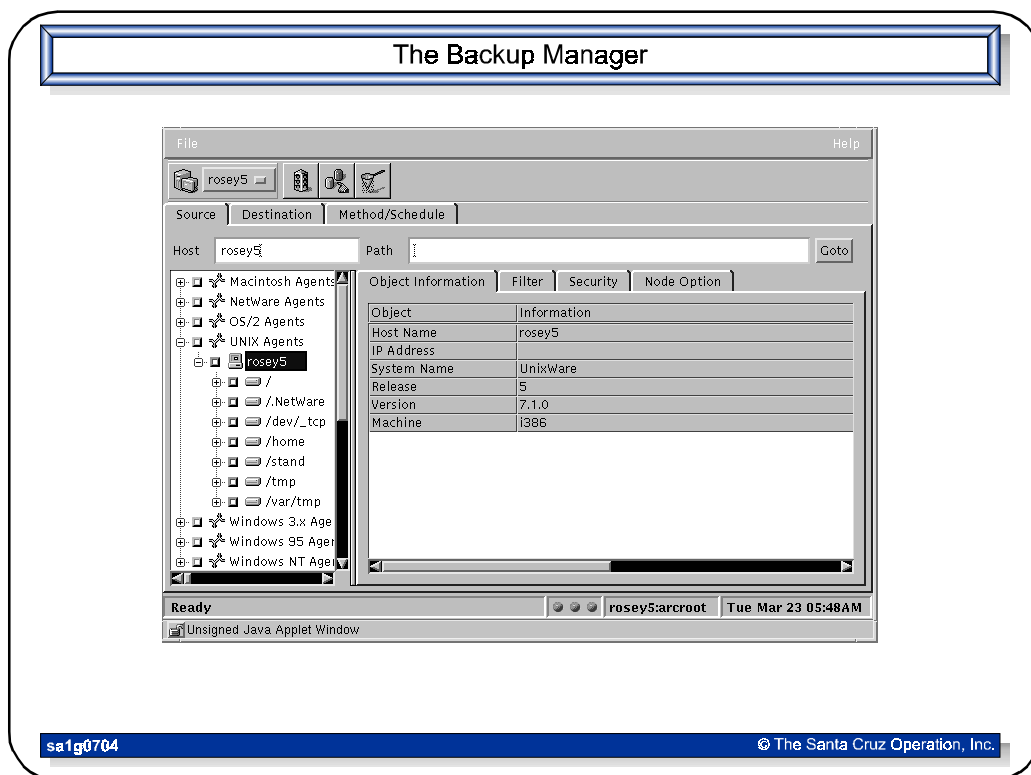
7.5.2 Using compression

If your tape device supports data compression, ARCserveIT turns it on by default. If it does not support data compression, N/A appears in the **Compression** window. To view if compression is applicable, select **Devices** ⇨ **Detail**.

Exercise: Performing Tape Maintenance

Perform a quick erase of your tape. When finished, eject the tape.

AV 7-4



7.6 Backing up files and filesystems

AV 7-4: The Backup Manager

Use this screen to show students how to expand and collapse directory structures.

During this lesson, students should be logged in as **root**.

From the **ARCserveIT** home page, select **Backup** to back up individual files and filesystems.

The **Backup Manager** appears with the **Source** tab selected by default. The default view option “View all filesystems agents” lets you see the Client Agents that are running.

When you select the “UNIX Agents”, the UNIX machine(s) display. Each machine is known as an *object*.

7.6.1 Expanding and object

You can select the entire machine or select filesystems, directories, or files within a machine.

The password required is the root password for the machine being selected. It is not the **arcroot** user and password.

The machine’s **root** password is required before viewing data on a machine. After you enter this information, the machine’s filesystems display.

7.6.2 Viewing filesystems and files

ARCserveIT provides a *Tree* view for viewing filesystems and files. This view displays files in a single file hierarchy:

- The machine name
- The root (/) filesystem
- Mounted non-root filesystems appear as a disk drive with the name of the mount point (directory) adjacent. Mounted filesystems are shown in the directory structure to which they are mounted.

To expand and collapse the directory tree, click on the plus sign or minus sign adjacent to the system name.

To expand and collapse a machine's directory structure, follow these steps:

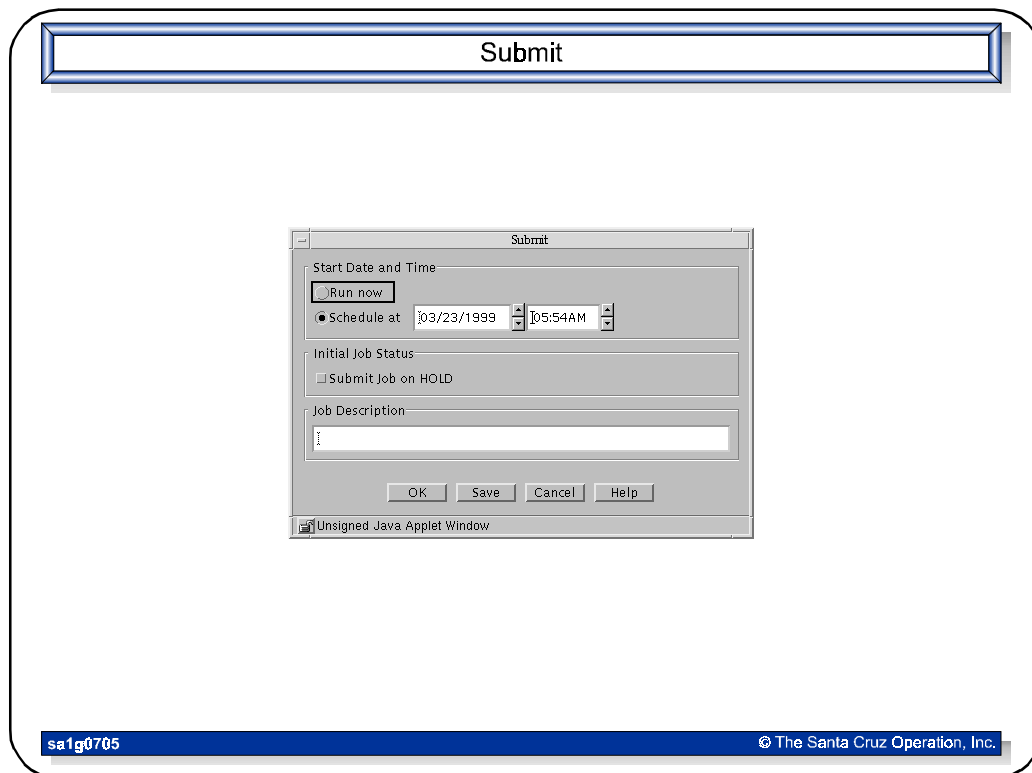
- Step 1. Select **Backup** from the ARCserveIT home page.
- Step 2. Click on **Unix Agents**.
- Step 3. Click on the plus sign adjacent to the machine name.
- Step 4. Enter the user name, **root**, and password. Click on **OK**.
- Step 5. Click on the plus sign adjacent to the root (/) directory to expand the directory and view files.
- Step 6. Click on the plus sign adjacent to a directory to view directories and files.
- Step 7. Click on the minus sign adjacent to a directory to collapse the directory and files.
- Step 8. Click on **File** ⇌ **Close** to return to the **Backup Manager**.

■ Demonstrate expanding the */etc* directory.

Exercise: View filesystems and files

Follow the steps in Section 7.6.2, “Viewing filesystems and files,” on page 7-24 and expand the */etc* directory. Collapse the tree so that only the machine name displays. Return to the **Backup Manager**.

AV 7-5



7.6.3 Performing a system backup

AV 7-5: Submit

After you click on the “Traffic Light” icon in Step 7, the Submit screen displays.

You can quickly perform a complete backup of your system. The features of ARCserveIT are powerful, yet simple to use.

Depending on the capacity of your tape device, you might need several tapes to perform a complete system backup. During the backup you are prompted to insert additional tapes.

From the **ARCserveIT** home page, you can determine the approximate number of tapes needed for a full system backup from the **Database Manager**.

From the **ARCserveIT** home page, perform a complete backup of your system by following these steps:

- Step 1. Insert a tape into the tape drive.
- Step 2. Click on the **LOG ON** button. Enter the **arcroot** user name and password. Click on **OK** twice.
- Step 3. Select **Backup**. Click on **Unix Agents**.
- Step 4. Click on the box adjacent to your machine name in the **Source** area of your screen.
- Step 5. Enter the user name **root** and password for the machine.

 This box becomes solid, indicating that all files on the system are selected.
- Step 6. Click on **Destination** ⇨ “Tape group.”
- Step 7. Click on the **Traffic Light** icon. Click on **Run now**.
- Step 8. Enter a description of the job.
- Step 9. Click on **OK** to acknowledge a successful submission. The backup begins.
- Step 10. Select **File** ⇨ **Close** to exit the **Backup Manager**.

Because of the length of time it takes to perform a full system backup, you might want to demonstrate this exercise on a machine in the classroom. You can also have students to perform this as a lab at the end of the lesson.

Exercise: Performing a full system backup.

Follow the steps under Section 7.6.3, “Performing a system backup,” on page 7-27 and perform a full system backup.

7.6.4 Backing up filesystems

Explain to students that it is not necessary to specify the **Destination** if only one tape drive is installed on the system.

When you select the mount point of a filesystem, all files in that filesystem are selected for backup.

From the **ARCserveIT** home page, you can backup a filesystem by following these steps:

- Step 1. Insert a tape into the tape drive.
- Step 2. Perform this step if you are not logged on. Click on the **LOG ON** button. Enter the **arcroot** user name and password. Click on **OK** twice.
- Step 3. Select **Backup**. Click on **Unix Agents**.
- Step 4. Click on the box beside your machine name in the **Source** area of your screen.
- Step 5. Enter the user name **root** and password for the machine. Click on **OK**.
- Step 6. Click on the box adjacent to the appropriate filesystem.
- Step 7. Click on the **Traffic Light** icon. Click on **Run now**.
- Step 8. Enter a description of the job.
- Step 9. Click on **OK** to acknowledge a successful submission. The backup begins.
- Step 10. Select **File** ⇒ **Close** to exit the **Backup Manager**.

7.6.5 Backing up selected files

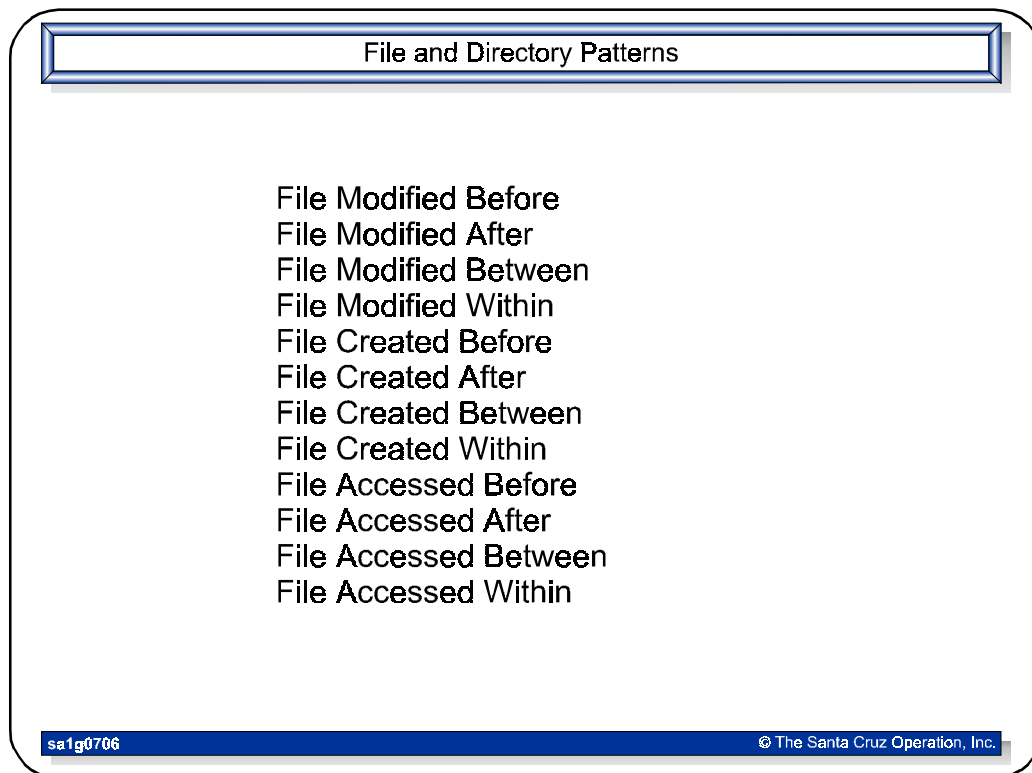
You can also backup selected files within a filesystem. From the ARCserveIT home page, follow these steps to backup selected files:

- Step 1. Complete Steps 1 through 6 in Section 7.6.4, “Backing up filesystems,” on page 7-28.
- Step 2. Click on the plus sign adjacent to the filesystem that contains the files. The filesystem is expanded.
- Step 3. Click on the box adjacent to the filesystem that contains the files. This deselects all files in the filesystem.
- Step 4. Click on the box adjacent to the files that you want to back up.
- Step 5. Click on **the Traffic Light** icon. Click on **Run now**.
- Step 6. Enter a description of the job.
- Step 7. Click on **OK** to acknowledge a successful submission. The backup begins.
- Step 8. Select **File** ⇒ **Close** to exit the **Backup Manager**.

Exercise: Backing up selected files

Use the above steps and back up all of the files in the `/etc/default` directory.

AV 7-6



Instructor Guide

7.6.6 Monitoring the status of a backup

Depending on the speed of your system, monitoring the status of a full system backup can take several minutes to load while the backup is taking place.

You can monitor the status of the backup by following these steps:

- Step 1. Click on **Job Status** from the **ARCserveIT** home page.
- Step 2. Select the **Job**.
- Step 3. Select **Job Status** ⇨ **Monitor Job**.
- Step 4. Select **File** ⇨ **Close** to exit **Job Status**.

7.6.7 Backup filter options

AV 7-6: File and Directory Patterns

A list of the Backup Filter options

Filter options are provided as a means to further distinguish files that you want to include as part of your backup. Filter options allow you to include or exclude both files and directory patterns as well as other options.

For example, to include all files that were created before a specified date, enter:

- Step 1. **Backup** ⇨ **Source**.
- Step 2. Click on the **Filter** icon.
- Step 3. Select **Include**.
- Step 4. Click on **File Accessed Before**.
- Step 5. Enter the date. Click on **Add**.
- Step 6. Click on **OK**.

The filter is added. You can select this filter for future backups or delete the filter when it is no longer needed.

7.6.8 Backup method

You can apply options to the destination media which include:

Eject Media	If you select this option, the media is ejected after the backup job completes.
First Media Options	Use these options if you have one tape drive. By default, ARCserveIT appends any data to the selected media. Select from the following to override the default: ● Overwrite Same Media Name, or Blank Media. The media name must be the same or must be blank media to overwrite the media. If it is not, the backup will fail. ● Overwrite Same Media Name, or Blank Media First, then any Media. Overwrite <i>any</i> media that is in the drive. ● Overwrite Same Media Name, or any Media first, then Blank Media. This is the same as the first option, except that if the media has been used in a rotation scheme, the backup will fail.
Span Media Options	Use these options in addition to First Media Options if you have multiple tape drives. The definitions are similar to First Media Options.
Time-out for First Media	Number of minutes ARCserveIT waits before accessing the media. If ARCserveIT cannot access the media in the specified time, the job is cancelled.

To apply any of these options, from the **Backup Manager**, select **Destination** ⇒ **Method/Schedule** ⇒ **Custom** ⇒ **Media Rules**.

7.6.9 Backup schedule

In addition to running the backup immediately, you can schedule the backup to run at a specified time, or submit a backup that is on hold.

After specifying the source and destination, to schedule the backup for a later time, select the **Submit** icon from the **Backup Manager**:

- To schedule the job at a specified date and time, click on **Schedule at**. Enter the date and time.
- To submit a job that is on on hold, click on **Schedule** ⇒ **Submit job on HOLD** and select from the jobs in the queue.

A backup schedule can also be created to run on a repeating basis. For example, if you wanted a backup to run every Monday, Wednesday, and Friday at 3:30 a.m., follow these steps:

- Step 1. Select **Method/Schedule** from the **Backup Manager**.
- Step 2. Enter 3 in the **Hours(s)** field and 30 in the **Minute(s)** field.
- Step 3. Exclude the days that you do not want the backup to run. For this example, click on Sunday, Tuesday, Thursday, and Saturday in the “Exclude Days” menu.
- Step 4. Click on the **Submit** icon. Click on **OK** to submit the job.

7.6.10 Placing backup jobs on hold

If you have scheduled a backup job to run at a future time and decide that you do not want the job to run, place the job on hold using the **Job Status Manager**.

7.6.11 Saving backup jobs as scripts

When running the same backup repeatedly, rather than performing the steps to create a backup each time, you can save the information to a script (file).

Before submitting the job, save the information to a script.

The script contains the:

- Source
- Destination
- Any scheduling information
- Any filters to include or exclude directories and files

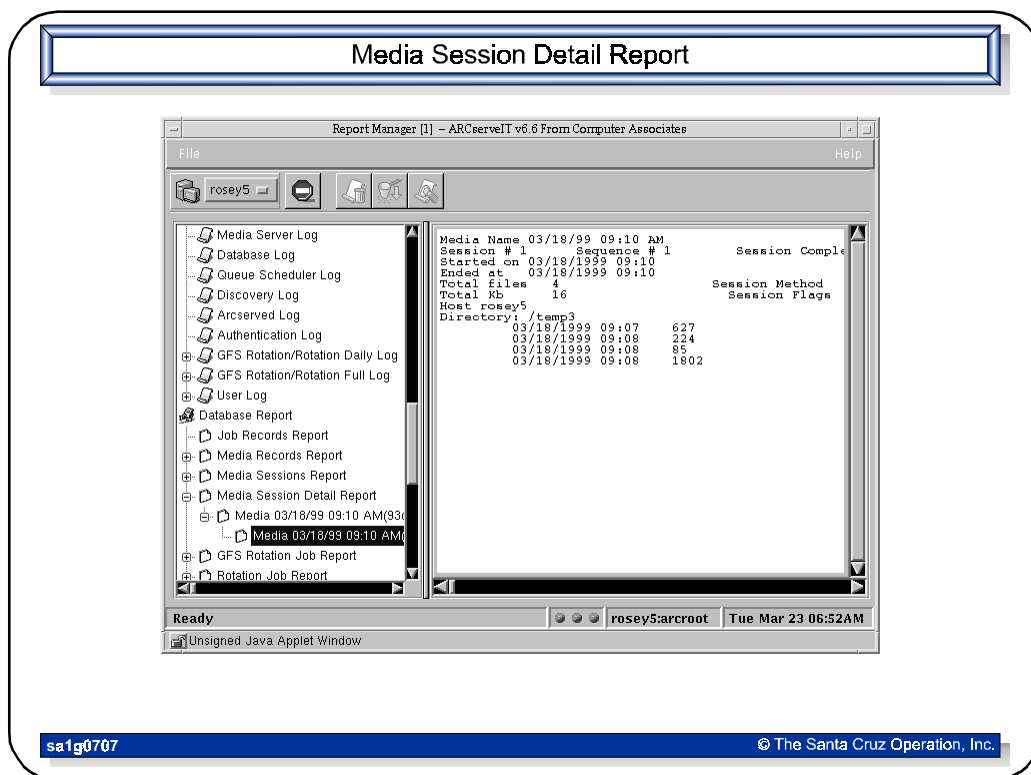
Follow these steps to create a script:

- Step 1. Initiate a job from the **Backup Manager**.
- Step 2. Schedule and customize the job
- Step 3. Enter the backup job description.
- Step 4. Click on **Save**.
- Step 5. Enter the script name. Click on **OK**. Click on **OK** for a successful save of the script.
- Step 6. Click on **OK** to submit the job. Click on **OK** for a successful submission.

To run the backup script:

- Step 1. Select the **Backup Manager**.
- Step 2. Click on **File** ⇨ **Open**.
- Step 3. Click on the **Run** icon.

AV 7-7



7.7 Verifying the backup and checking logs

You can verify the results of your backup by scanning your media and checking the available backup logs.

7.7.1 Scanning media

AV 7-7: Media Session Detail Report

You must run the **Scan** option to generate this report.

Use the **ARCserveIT Scan Manager** to verify your media. This manager provides you with information about your media sessions. You can scan a single session or the entire media. Results of the media scan can be viewed in the **Reports Manager** under the **Database Log**.

To scan the contents of your tape that is currently in the tape drive:

- Step 1. Select **Scan** from the **ARCserveIT** home page.
- Step 2. Click on **All Sessions** ⇒ Click on **Current media in drive**.
- Step 3. Click on the **Run** icon. Click on **Run now**. Click on **OK**.
- Step 4. Click on **OK** for a successful submission.
- Step 5. Click on **File** ⇒ **Close** to exit the **Scan Manager**.

The contents of the tape is scanned and detailed information including filenames and sizes is written to the **Reports Manager** ⇒ **Database Report** ⇒ **Media Session Detail Report**.

7.7.2 Viewing Reports and Logs

Whenever a job is submitted to the scheduler, the ARCserveIT logs are updated. The logs should be viewed on a regular basis to make certain errors are not encountered while performing backup jobs. ARCserveIT communicates errors to the operator through these reports.

Important logs include the **Activity Log** and the **Media Server Log**.

7.7.2.1 Activity Log

The **Activity Log** contains information about the operations performed by ARCserveIT. For each job, the log includes the following:

- Date and time the job started and ended
- Type of job
- Average throughput of the data
- Job session number
- Result of the job
- Messages that indicate errors display in red

To display the **Activity Log**:

- Step 1. Select **Report** from the ARCserveIT home page.
- Step 2. Select **Activity Log**.
- Step 3. The **Activity Log** displays.

Exercise: Viewing the Activity Log

View the **Activity Log** for your classroom system.

7.7.2.2 Media Server Log

The **Media Server Log** provides an audit trail of all ARCserveIT Media Server activity, including when the Media Server is loaded and unloaded.

The **Media Server Log** also provides information about tape jobs including:

- Backups
- Formatting
- Retension
- Erasing

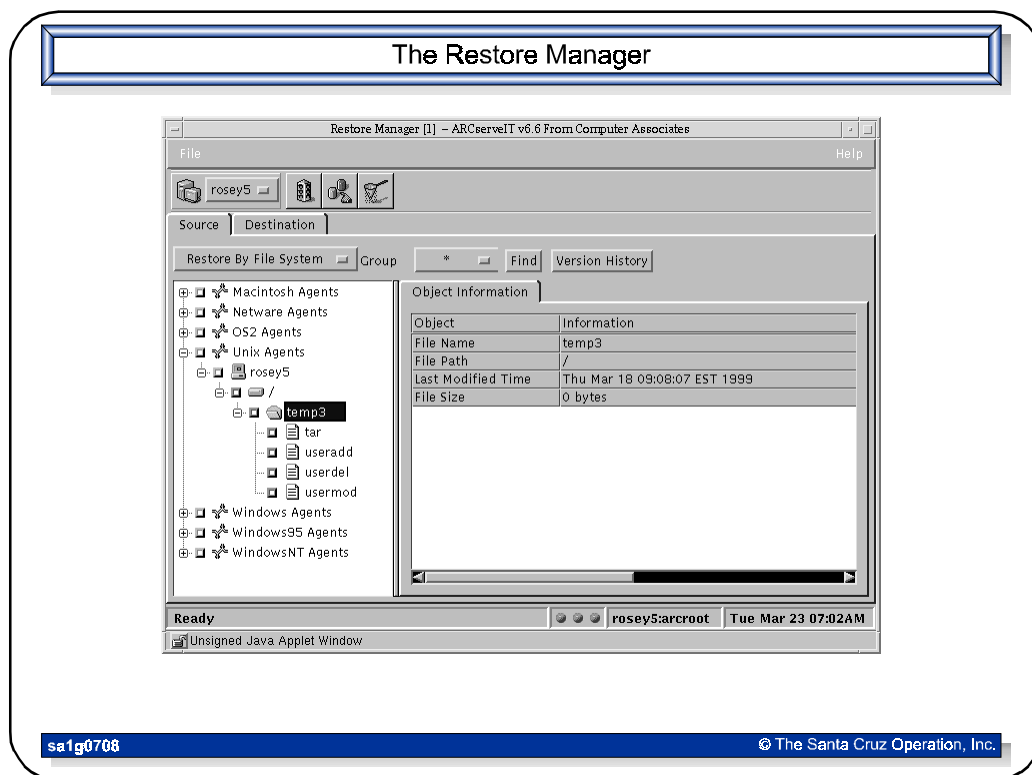
For each job, the log includes:

- Time the job started
- ID number of the job
- User who submitted the job
- Activity performed
- Job session number
- Errors displayed in red

Exercise: Viewing the Media Server Log

View the Media Server Log for your classroom system.

AV 7-8



7.8 Restoring files and filesystems from backups

AV 7-8: The Restore Manager

The **Source** is expanded.

You can restore files, directories, and filesystems using the ARCserveIT **Restore Manager**. View and restore data using three different methods:

Restore by File System	This is the default method. Using this method shows you a graphical directory tree of each filesystem. You can restore an entire filesystem(s) or specific files and directories.
Restore by Session	This method allows you restore an entire single session or select files within the session.
Restore by Backup Media	This method restores all files in a session.

7.8.1 Browsing media

The **Restore Manager** is divided into two sections:

- The **Source** section describes how the data is stored on your media. You specify what data is being restored.
- The **Destination** section displays the directory hierarchy of the machine to which data is restored. You specify to where the data is being restored.

To access the **Restore Manager**,

Step 1. Select **Restore** from the ARCserveIT home page.

The **Source** tab and **Restore by File System** are selected by default.

Step 2. Click on the plus sign adjacent to Unix Agents. Continue expanding the directory structure.

To view files by session:

Step 3. Click on **Restore by File System** and select **Restore by Session**.

Step 4. Click on the plus sign adjacent **Media** icon. Select a media session. Continue expanding the media session.

Step 5. Exit the **Restore Manager**. Click on **File** ⇒ **Close**.

7.9 Performing a Basic Restore Job

Restoring data can be a quick and flexible task. When accessing the **Restore Manager**, remember that **Restore by Filesystem** is the default method. To restore files using the **Restore Manager**:

- Step 1. Insert the tape into the drive.
- Step 2. Select **Restore** from the ARCserveIT home page.
- Step 3. Click on the plus sign adjacent to the UNIX Agents.
- Step 4. Click on the plus sign adjacent to the machine name.
- Step 5. Click on the plus sign adjacent to the root (/) directory.
- Step 6. Continue expanding the directory structure until you reach the directories and files to restore.
- To restore all files in a non root filesystem, click on the box adjacent to the filesystem name.
- To restore an entire directory structure, click on the box adjacent to the directory name.
- Step 7. Specify the destination. Click on **Destination**.
- Step 8. Click on the plus sign adjacent to UNIX Agents.
- Step 9. Click on the plus sign adjacent the destination machine. Enter the root user name and password. Click on **OK**.
- Step 10. Expand the directory structure until you reach the destination directory.
- Step 11. Restore the data. Click on the **Run** icon.
- Step 12. Click on **Run now**. Click on **OK**.
- Step 13. Click on **OK** for a successful submission. The files are restored.
- Step 14. Click on **File** ⇨ **Close** to exit the **Restore Manager**.

Information about your restore can be found in the **Reports Manager**.

7.9.1 Restore filter options

Show the Filter icon and remind students that the restore filter options are specified in the same manner as the backup filter options.

Filter options are provided as a means to further distinguish files that you want to include as part of your restore. Filter options allow you to include or exclude certain file or directory patterns.

To access the filter options, click on the **Filter** icon in the **Restore Manager** and set the filters before restoring the job.

Exercise: Restoring the /etc/default/directory

Restore all files in the /etc/default/directory to /tmp. As a guide, follow the steps in Section 7.9, “Performing a Basic Restore Job,” on page 7-42.

7.10 Lesson Summary

Creating system backups is the only way to recover your system in case of either hardware failure or accidental loss of data. The UnixWare 7 system provides the ARCserveIT backup tool. This tool allows you to quickly backup and restore either entire filesystems or selected files.

Review questions

1. Why should you store backup tapes off-site from the location of the system?

You should store backup tapes off-site from the location of the system to prevent complete data loss in case of on-site property destruction caused by fire or other disasters.

2. How are the files and directories displayed and accessed in the source section of the ARCserveIT Backup Manager?

The backup source files and directories are displayed in a Tree View. By clicking on the directory icons you can expand or collapse the tree.

3. How can you verify that a backup and/or a restore is executed free of errors?

To verify that a backup and/or restore executed free of errors you can scan the tape contents using the Scan Manager. You can also check the activity and tape server logs for any error messages displayed in red.

4. What are the two areas where you must make selections when performing a restore?

When performing a restore you must select the directory or files to be restored by clicking on the desired filesystem, file, or directory tree in the Source Area. The arrow designates whether or not a directory tree is expanded. You must also select the directory to be used for the restored data, in the Destination Area. The destination can be different than the location from where the files were backed up.

7.11 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

scoadmin(1M)	Invokes SCOadmin applications (in this lesson, the ARCserveIT Backup Manager)
/usr/bin/asetup	Configures ARCserveIT after installation
/usr/bin/astart	Starts ARCserveIT from the command line
/usr/bin/astatus	Lists the services started by ARCserveIT
/usr/bin/astop	Stops ARCserveIT from the command line

Relevant files

<i>/etc/rc2.d/S96ARCserveIT</i>	Starts up ARCserveIT when entering the networking state
---------------------------------	---

7.12 Answers to Review Questions

This section contains the answers to review questions presented in this lesson.

1. You should store backup tapes off-site from the location of the system to prevent complete data loss in case of on-site property destruction caused by fire or other disasters.
2. The backup source files and directories are displayed in a Tree View. By clicking on the directory icons you can expand or collapse the tree.
3. To verify that a backup and/or restore executed free of errors you can scan the tape contents using the Scan Manager. You can also check the activity and tape server logs for any error messages displayed in red.
4. When performing a restore you must select the directory or files to be restored by clicking on the desired filesystem, file, or directory tree in the Source Area. The arrow designates whether or not a directory tree is expanded. You must also select the directory to be used for the restored data, in the Destination Area. The destination can be different than the location from where the files were backed up.

8

Managing Printers

Instructor Guide

Instructor Guide

Lesson 8

Managing Printers

Suggested lesson duration

This lesson should take approximately 1.5 hours to complete, including the lab exercise.

Pre-lesson classroom preparation

Create the laser1 and laser2 printers on each system in the classroom.

Instructor preparation

Practice using the **SCOadmin Printer Setup Manager** and the **Print Job Manager**.

AV 8-1

Managing Printers

- Manage the print service
- Accept and reject print jobs
- Disable and enable printers
- Manage print jobs
- View and change printer settings
- Troubleshoot printer problems

sa1g-0801 © The Santa Cruz Operation, Inc.

Instructor Guide

Introduction

Printing is one of the most common functions that users perform. Maintaining printers, print services, and print queues lets your users print out reports and other items required for their jobs.

This lesson describes how to manage print queues when bringing a printer down for maintenance. It also shows you how to manage user print requests and how to configure printers for specific functions.

Objectives

This lesson addresses the tasks required to manage printing services. By the end of this lesson, you will be able to:

- Manage the print service
- Accept and reject print jobs
- Disable and enable printers
- Manage print jobs
- View and change printer settings
- Troubleshoot printer problems

AV 8-1: Managing Printers

This slide describes the overall topics covered in this lesson.

8.1 Managing the Print Service

Print services are controlled through the **SCOadmin Printer Setup Manager** and the **Print Job Manager**.

8.1.1 Describing the print service

When a user prints a file, a daemon process called the printer scheduler, **lpsched**(1M), sorts the print requests and puts them into the designated printer queue. As soon as the designated printer is ready for that print job, the scheduler runs an interface program to print the file.

The print service is responsible for performing these tasks:

- Receives files to be printed
- Schedules the work of one or more printers
- Starts the programs that interface with specific printers
- Tracks the status of print jobs
- Alerts you to printer problems
- Issues error messages when problems occur

Use the **lpstat(1)** command to view the status of the various printers, enter:

```
lpstat -t | more
```

■ This exercise lets students practice using **lpstat(1)**.

Exercise: Determining printer status

View the status of the printers on your system.

8.1.2 Stopping the print service

The print service starts as soon as the system enters a multiuser state. Under normal operation, you should never have to stop and start the print service manually. However, sometimes you must stop the print service to clear up a problem.

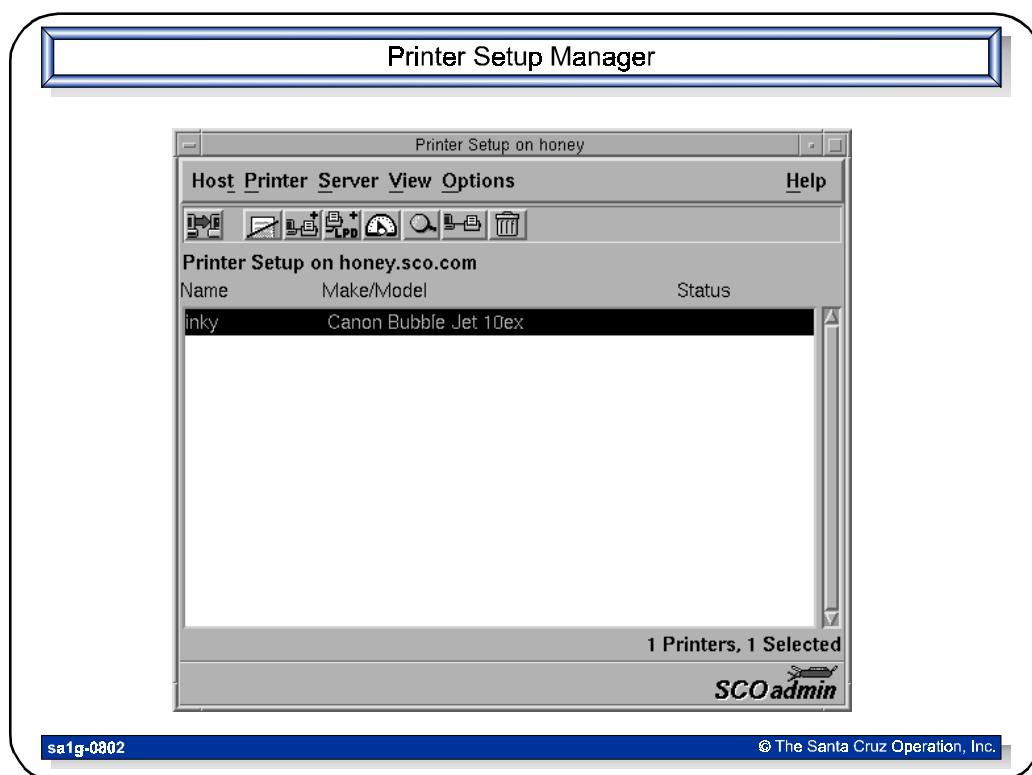
Follow these steps using the **SCOadmin Printer Setup Manager** to stop the print service.

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select **Server** ⇒ **Halt**.
- Step 3. Click on **OK** to stop the print services.
- Step 4. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use the **lpshut(1M)** command to stop the print service, enter:

```
/usr/lib/lpshut
```

AV 8-2



Instructor Guide

8.1.3 Starting the print service

AV 8-2: Starting and Stopping the Print Service

Screen shot of the **Printer Setup Manager** dialog box.

Follow these steps using the **SCOadmin Printer Setup Manager** to start the print service:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select **Server** ⇒ **Start**.
- Step 3. Click on **OK** to start the print services.
- Step 4. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use the **lpsched(1M)** command to start the print service, enter:

/usr/lib/lpsched

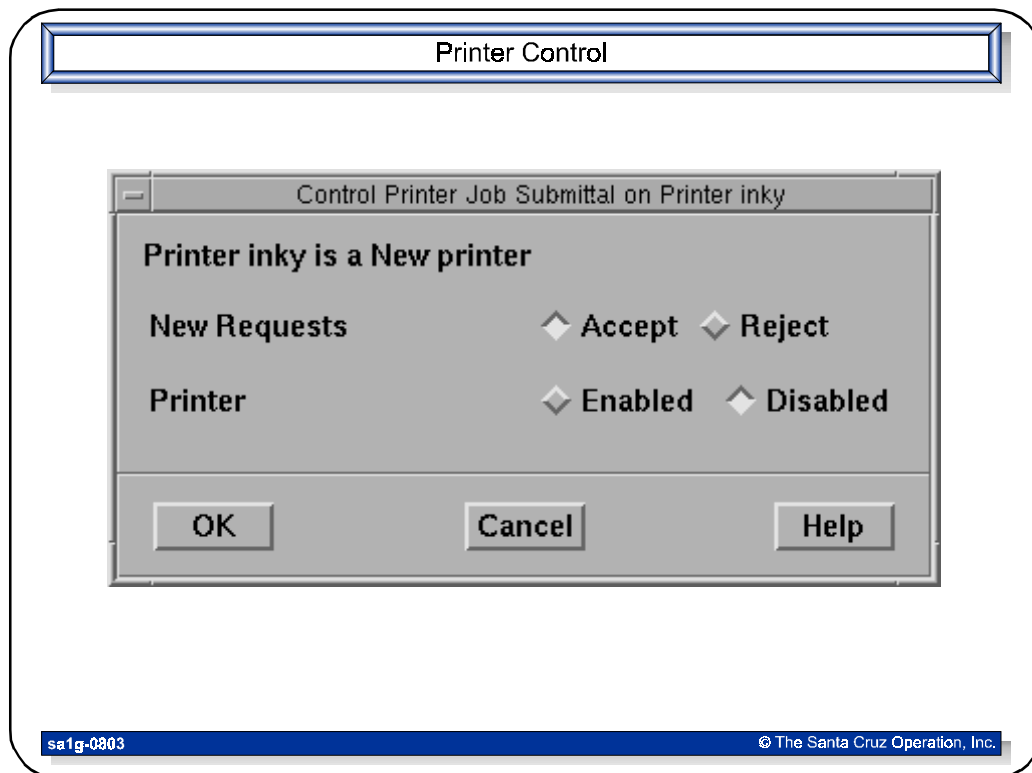
This exercise lets students see what happens when the print service is stopped. Students can also practice stopping and starting the print service.

Exercise: Stopping the print service

Shut down the print service and print a file. What is the error message? Run **lpstat(1)**. What is the meaning of the message?

Restart the print service. Run **lpstat(1)** to verify that the print service is running.

AV 8-3



Instructor Guide

8.2 Accepting and Rejecting Print Jobs

AV 8-3: Controlling a Printer

Screen shot of the **Printer Setup Manager** "Printer Control" dialog box.

Sometimes a printer needs major maintenance, possibly requiring a trip to the repair shop. Maybe you are waiting for a toner cartridge that is on back-order. In these situations, set the print queue to reject print jobs so that users know to send requests to another printer.

8.2.1 Rejecting print jobs

Use the **SCOadmin Printer Setup Manager** to reject print requests:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select the printer.
- Step 3. Select **Printer** ⇒ **Control**.
- Step 4. Click on **Reject**.
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use the **reject(1M)** command to stop a printer from accepting print jobs:

```
reject printername
```

To add a message stating why the printer is down or to redirect your users to another printer:

```
reject -r"reason" printername
```

To display the "reason," enter:

```
lpstat -a
```

8.2.2 Accepting print jobs

Use the **SCOadmin Printer Setup Manager** to accept printer requests:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select the printer.
- Step 3. Select **Printer** ⇒ **Control**.
- Step 4. Click on **Accept**.
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use the **accept(1M)** command to allow a printer to begin accepting print jobs, enter:

accept printername

This exercise lets students see what happens when the print service rejects print jobs for a specific queue. They will also practice rejecting and accepting print jobs.

Exercise: Rejecting print jobs

Reject print jobs, and provide a message that informs users to redirect print requests to *laser2*.

reject -r"printer down, use laser2" laser1

Run **lpstat(1)**. What does it report? Try to send a print job to *laser1*. What message displays?

Accept print jobs. Run **lpstat(1)** and note the difference. Try to print a file to *laser1*.

8.3 Disabling and Enabling Printers

Printers occasionally need routine checks and maintenance, such as replacing toner cartridges or removing jammed paper. If the maintenance requires only a short disruption of printing, disable the printer. A disabled printer continues to accept print jobs in its queue, but does not print them until you re-enable it.

If you disable the printer while it is in the middle of a print job, the printer restarts the job from the beginning after you enable it.

8.3.1 Disabling a printer

Use the **SCOadmin Printer Setup Manager** to disable printers:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select the printer.
- Step 3. Select **Printer** ⇒ **Control**.
- Step 4. Click on **Disable**.
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use the **disable(1M)** command to disable a printer, or printers:

```
disable printername ...
```

Use the **-r** option to disable the printer so that a reason appears in an **lpstat(1)** report, enter:

```
disable -r"reason" printername ...
```

8.3.2 Enabling a printer

Use the **SCOadmin Printer Setup Manager** to enable printers:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select the printer.
- Step 3. Select **Printer** ⇒ **Control**.

Step 4. Click on **Enabled**.

Step 5. Click on **OK**.

Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

You can also use **enable(1M)** to enable the printer, or printers:

`enable printername ...`

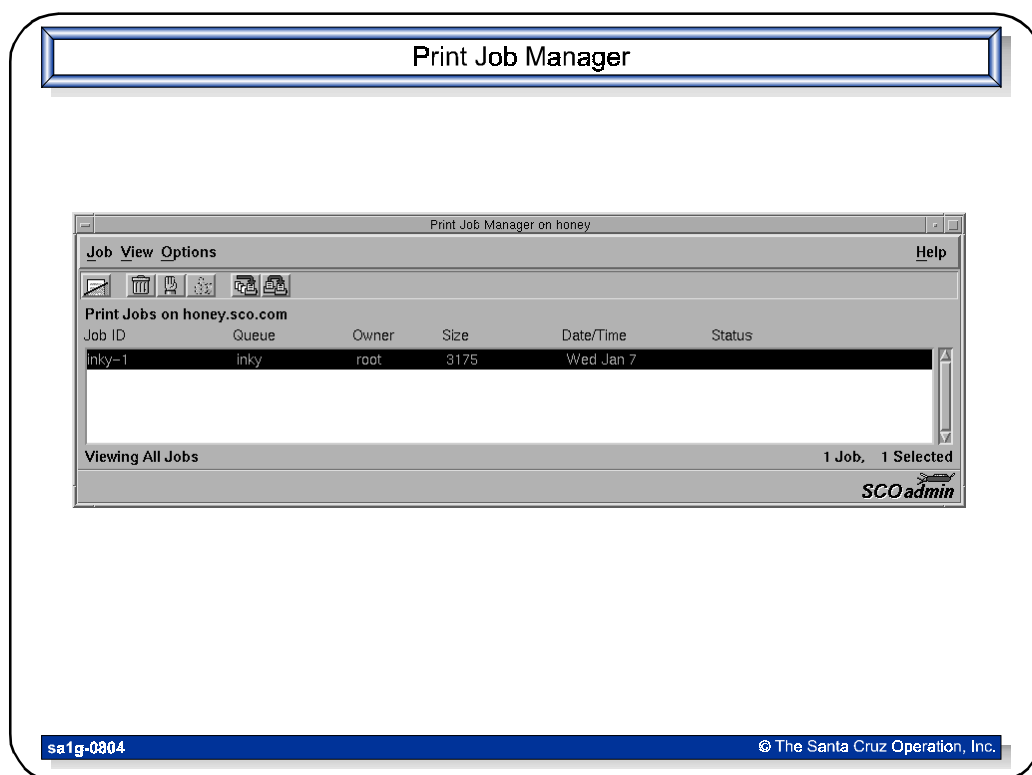
This exercise lets students see what happens when the print service disables a printer. They will also practice disabling and enabling printers.

Exercise: Disabling a printer

Disable *laser1* and try to print a file to *laser1*. What happens? What does **lpstat -a** report? What does **lpstat -t** report?

Enable *laser1* and run **lpstat(1)** again. What happens to the print job?

AV 8-4



Instructor Guide

8.4 Managing Print Jobs

AV 8-4: Print Job Manager

Screen shot of the **Print Job Manager**.

Printer authorizations grant users the capability to cancel jobs submitted by other users. Use the **SCOadmin Account Manager** and assign the **Administer Printers** authorization. Be aware that other printer authorizations are also assigned.

What can you do if one of these situations occur?

- A printer breaks down, but there are several jobs already waiting in its queue.
- Someone sends a very large job to the printer several times by accident.
- An extremely important and urgent report is sitting in a queue behind many time-consuming and less important print jobs.

The **Print Job Manager** lets you manipulate individual print requests and groups of print requests to keep the *print queues* running smoothly. A print queue is a list of all the print jobs that belong to individual users. By default, the **Print Job Manager** lists *all* print jobs.

You can also view print jobs by a single *user* or *queue*.

8.4.1 Viewing print jobs

Use the **SCOadmin Print Job Manager** to view print jobs.

Step 1. Start **SCOadmin**. Select **Print Job Manager**.

A list of print jobs that are in the printer queues appear in the order in which they were submitted.

Step 2. Select **View** ⇨ **By User(s)**. Select from the list of available users.

Step 3. Select **View** ⇨ **By Queue(s)**. Select from the list of available queues (printers).

Step 4. Select **View** ⇨ **All Jobs** to view all print jobs in all queues.

Step 5. Select **Job** ⇨ **Exit** to exit the **Printer Job Manager**.

You can also use the **lpstat(1)** command to view print jobs:

- To view print jobs by queue, list the queues:

```
lpstat laser1 laser2
```

- To list print jobs by user, use the **-u** option:

```
lpstat -u user1,user2
```

Exercise: Viewing print jobs

Disable both *laser1* and *laser2*. As the **root** account, send several print jobs to each printer. Log in as an ordinary account and send several print jobs to each printer.

Now view the print requests. Sort the jobs by queue, then by user.

8.4.2 Deleting print jobs

Use the **Print Job Manager** to delete print jobs:

Step 1. Start **SCOadmin**. Select **Print Job Manager**.

Step 2. Select the print job(s) to delete.

To delete all jobs:

Step 3. Select **Select All Jobs**.

Step 4. Select **Job** ⇒ **Delete**.

Step 5. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

Note that each print job has a unique job ID that consists of two parts:

- Name of the printer queue
- Sequence number

You can also use the **cancel**(1) command to cancel print jobs:

```
cancel job_id1 job_id2 ...
```

This exercise lets students practice canceling print jobs. They will also view the **Print Job Manager** as the remaining print jobs are processed.

Exercise: Canceling print jobs

Cancel one print job from each queue. Enable both printers, and monitor the print queues as the printer service processes the requests.

8.4.3 Holding print jobs

You can suspend the processing of a large print job temporarily until several smaller jobs have processed. In this case you can *hold* a print job. The print service continues to process other jobs in the queue until you resume the job.

Use the **Print Job Manager** to hold a print job:

- Step 1. Start **SCOadmin**. Select **Print Job Manager**.
- Step 2. Select the print job(s) to place on hold. To hold all print jobs:
Select **Select All Jobs**.
- Step 3. Select **Job** ⇒ **Hold**.
- Step 4. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(1)** command to hold print jobs:

```
lp -i job_id -H hold
```

8.4.3.1 Resuming print jobs

Use the **Print Job Manager** to resume a print job:

- Step 1. Start **SCOadmin**. Select **Print Job Manager**.
- Step 2. Select the print job(s) to resume. To resume all jobs:
Select **Select All Jobs**.
- Step 3. Select **Job** ⇒ **Resume**.
- Step 4. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(1)** command to resume print jobs:

```
lp -i job_id -H resume
```

This exercise lets students place print jobs on hold, then watch the **Print Job Manager** as the print service processes the remaining jobs. The students then resume the held job. Emphasize that held jobs remain in the queue until resumed or canceled.

Exercise: Holding and resuming print jobs

Disable *laser1* so that print jobs accumulate. Send several print jobs to *laser1*.

Place the second print job in the queue on hold. Enable *laser1* and monitor its print queue.

Resume the printing of the held print job. Monitor the print queue.

8.4.4 Moving print jobs

You can move or *promote* a print job to a higher level in the queue. You can also move print jobs within a single queue or between different queues.

8.4.4.1 Promoting print jobs

Promoting a print job places it higher in the print queue. Promoting a job does not necessarily mean that the job prints first. If there is a job currently printing, the job moves to next in line in the queue, unless you place the printing job on hold.

Use the **SCOadmin Print Job Manager** to promote a print job:

- Step 1. Start **SCOadmin**. Select **Print Job Manager**.
- Step 2. Select the print job(s), then select **Job** ⇒ **Promote**. The job or jobs move to the top of the queue.
- Step 3. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(1)** command to promote a print job:

```
lp -i job_id -H immediate
```

This exercise lets students practice moving print jobs within a single queue. It also shows how the print service orders the promoted print jobs.

Exercise: Promoting a print job

Disable *laser1* and send several print requests to the queue. Promote the last item in the queue, then promote the second-to-last. What is the print order now?

Promote the second item again to place it first in the list. Enable *laser1* and monitor the queue.

8.4.4.2 Transferring print jobs between queues

Use the **SCOadmin Print Job Manager** to transfer print jobs between queues:

- Step 1. Start **SCOadmin**. Select **Print Job Manager**.
- Step 2. Select the job(s) to transfer. To transfer all jobs:
Select **Select All Jobs**.
- Step 3. Select **Job** ⇒ **Transfer**.
- Step 4. Select the destination queue, then click on **OK**.
- Step 5. Click on **OK** again when prompted to confirm the destination queue.
- Step 6. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(1)** command with the **-d** option to transfer print jobs between queues:

```
lp -i -d job_id -dprint_queue
```

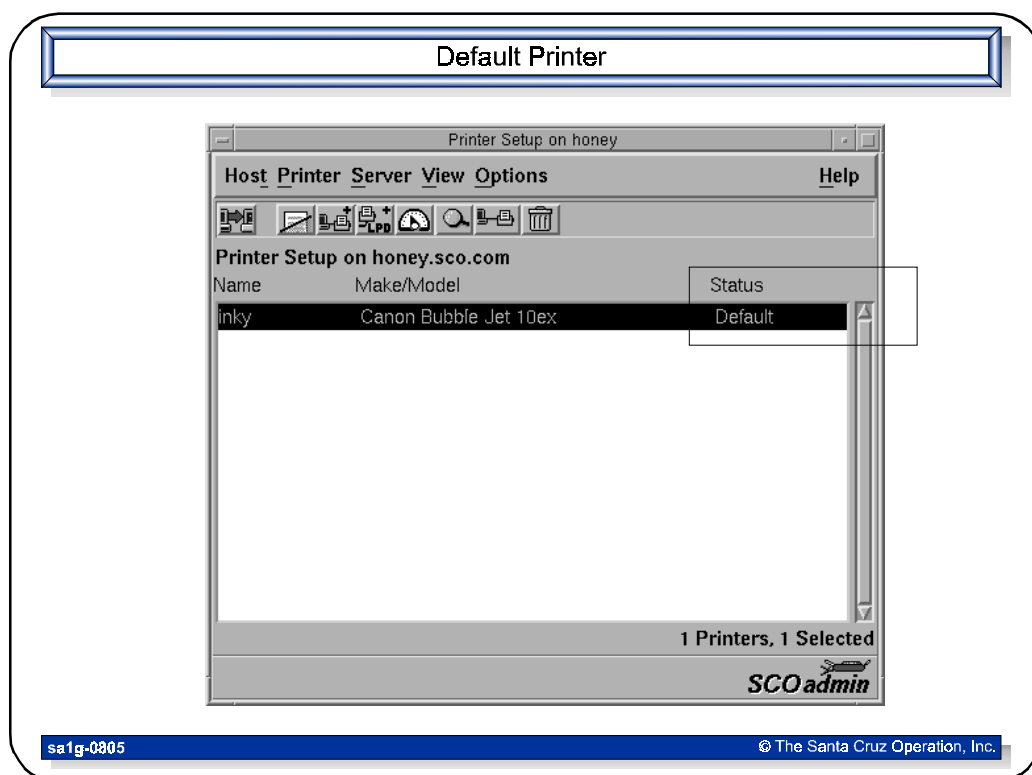
This exercise lets students practice moving print jobs between different queues. Emphasize the print ID of a transferred print job does not change.

Exercise: Transferring print jobs

Disable *laser1* and *laser2*. Send several print jobs to *laser1*. Transfer the last job in the queue to *laser2*.

Does the job ID change when you transfer a job?

AV 8-5



8.5 Viewing and Changing Printer Settings

You can designate a printer to be the system default printer, set a default printer for an individual user, control user access to a printer, and determine whether or not a printer produces banner pages.

8.5.1 Setting the default printer

AV 8-5: Default Printer

Screen shot of the **Printer Manager** highlighting the default printer identification in the lower right corner of the screen.

When a user does not specify a destination, print jobs go to the system default printer. Setting the default simplifies the environment for the user.

Use the **SCOadmin Printer Setup Manager** to set up a printer as the default printer:

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select a printer, then select **Printer** ⇨ **Make default**.
- Step 3. Select **Host** ⇨ **Exit** to exit the **Printer Setup Manager**.

8.5.2 Setting a default printer for a user

You can specify default printers for individual users, overriding the system default.

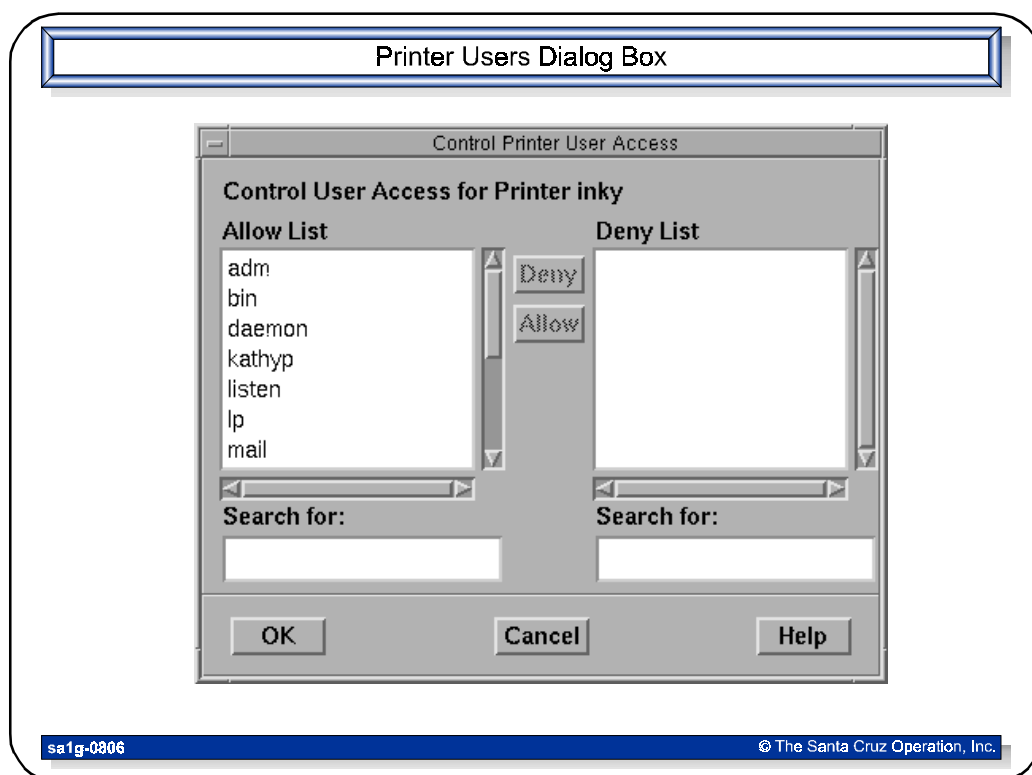
For Bourne and Korn shell users, edit the user's *.profile* and add these two lines:

```
LPDEST=prntername  
export LPDEST
```

For C shell users, edit the user's *.cshrc* and add this line:

```
setenv LPDEST prntername
```

AV 8-6



Instructor Guide

8.5.3 Controlling access to a printer

AV 8-6: Controlling Printer Access

Screen shot of the **Printer Manager** "Printer Users" dialog box.

There are situations in which you might want to restrict who can send jobs to a specific printer. For example:

- A department needs to print a large job as quickly as possible.
- You want to minimize wear on a high-end printer.
- You have a printer stocked with blank company checks.

Use the **SCOadmin Printer Setup Manager** to restrict access to a printer:

Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.

Step 2. Select the printer.

Step 3. Select **Printer** ⇒ **Set User Access**.

The "Control printer user access" dialog box appears with an **Allow** and a **Deny** list.

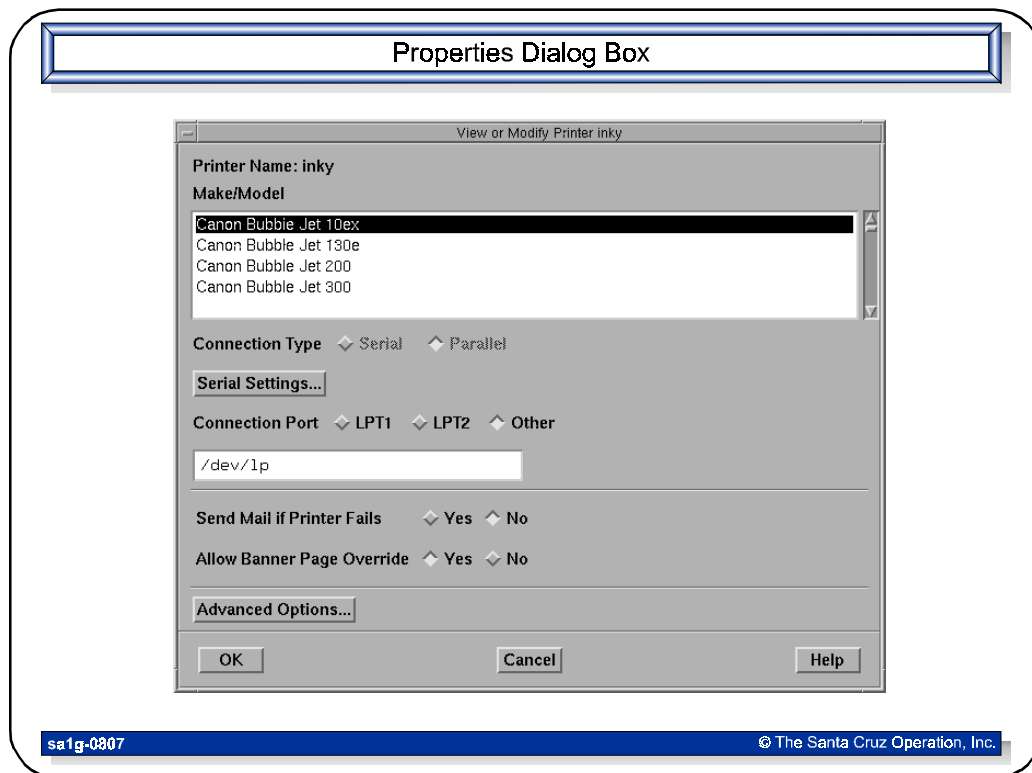
Step 4. Allow or deny access to the printer:

- If a user is on the **Allow** list, and you want to deny that user access to the printer, select the user name, then select **Deny**. The user name moves to the **Deny** list.
- If a user is on the **Deny** list, and you want to allow that user to access the printer, select the user name, then select **Allow**. The user name moves to the **Allow** list.

Step 5. Click on **OK**.

Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

AV 8-7



This exercise provides students with the opportunity to limit access to a specific printer. They will also see the error message a user receives when trying to print to a restricted printer.

Exercise: Controlling access to a printer

Set up the *laser2* printer to deny access to your student account. Log in using your student account, then try to print */etc/default/login* to *laser2*. Interpret the error message.

8.5.4 Preventing banner pages

AV 8-7: Controlling Banner Pages

Screen shot of the **Printer Setup Manager** "Properties" dialog box.

If you have a printer dedicated to printing special forms, such as checks, you can disable banner pages so that the printer does not print a banner across the form.

Use the **SCOadmin Printer Setup Manager** to let users send the **nobanner** option when submitting print requests:

- Step 1. Start **SCOadmin**. (1M) ⇒ **Printer Setup Manager**.
- Step 2. Select the printer.
- Step 3. Select **Printer** ⇒ **Properties**.
- Step 4. Click on **Yes** at "Allow banner page override."
- Step 5. Click on **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Setup Manager**.

To submit a print request using the **nobanner** option to the default printer, enter:

```
lp -o nobanner /etc/default/login
```

8.6 Troubleshooting Printer Problems

If a printer stops printing, try these troubleshooting tips:

- Check your e-mail. Error messages that occur during printing are often mailed to the user who made the request.
- Use **lpstat -t** to view the status of the printing system. Verify that the printer scheduler is running and that the printer is enabled and accepting requests.
- Make sure the printer is online.
- Check the power and cables to the printer.
- Verify that the printer hardware is working by checking the printer documentation for a self-test. Switch the printer off and on again.
- Shut down the print service. Use **ps(1)** to verify that **lpsched(1M)** is not running. Restart the print service.

If none of the above work, shut down the system and restart it.

Refer to **scohelp** ⇨ **Printing** ⇨ **Managing the print service** ⇨ **Troubleshooting the print system** for a list of common problems and suggested solutions.

This exercise encourages students to use SCOhelp to resolve system problems.

Exercise: Online help troubleshooting suggestions

Use **SCOhelp** to find suggestions if the printer output is illegible.

8.7 Lesson Summary

The print service lets you control how users access printers. You can temporarily disable a printer for quick maintenance, or you can reject all print jobs if you require a specific printer to be unavailable for a few days.

The print service also lets you control individual print requests. Print jobs can be redirected to different printers, canceled, or moved ahead in the queue.

In addition, the print service lets you control who can access a printer, and how specific printers behave. You can also designate a default printer—system-wide or for individual users.

Review questions

1. What tasks does the print service perform?

The print service performs these tasks: receives files for printing, schedules the work on one or more printers, starts the interface with specific printers, tracks the status of print jobs, alerts you to printer problems, and issues error messages when problems occur.

2. When should you set up a printer to reject print requests?

You should set up a printer to reject print requests when the printer is going to be unavailable for more than one to two hours.

3. When should you disable a printer?

You should disable a printer when it is going to be unavailable for only a brief amount of time.

4. What is the difference between transferring a print job and promoting it?

Transferring a print job sends it to a different print queue. Promoting a print job places it at the top of the current print queue.

5. How would you limit user access to a specific printer?

You can edit the allow and deny user lists found in the Control Printer User Access dialog box in the Printer Setup Manager.

6. List three things to check when a printer stops printing.

Instructor Guide

Check any of these when a printer stops working: check your mail—error messages that occur during printing are often mailed to the user who made the request; use `lpstat -t` to view the status of the printing system—verify that the printer schedule is running and that the printer is enabled and accepting requests; check the power and cables to the printer; verify that the printer hardware is working by checking the printer documentation for a self-test—switch the printer off and on again.

8.8 Lab: Managing Printers

In this lab, *laser1* needs to be shut down for repairs. Reject any new print requests for that printer and redirect any jobs in its queue to *laser2*.

8.8.1 Overview

Disable *laser1* and *laser2* so that the print requests accumulate. Send several print requests to both *laser1* and *laser2*. Set *laser1* to reject requests, then move the jobs in *laser1*'s queue to *laser2*'s queue.

8.8.2 Procedure

These steps describe how to shut down *laser1* for repairs, reject any new print requests for that printer, and send new print requests to *laser2*.

- Step 1. Start **SCOadmin**. Select **Printer Setup Manager**.
- Step 2. Select *laser1* and Select **Printer** ⇒ **Control**.
- Step 3. Click on **Reject** and then click on **Disabled**.
- Step 4. Open a **Terminal** window or multiscreen and send several print requests to both printers. Some examples are listed below:
- ```
lp -dlaser1 /etc/default/login
lp -dlaser2 /etc/default/tar
```
- Step 5. Go back to the **Printer Setup Manager**. Select *laser1* and select **Printer** ⇒ **Control**.
- Step 6. Click on **Accept new requests**.
- Step 7. Click on **OK** to activate your choices.
- Step 8. Open a **Terminal** window or multiscreen. Try to send a print job to *laser1*:
- ```
lp -dlaser1 /etc/passwd
```
- Step 9. Start **SCOadmin**. Select **Print Job Manager**.
- Step 10. Select **View** ⇒ **By Queue(s)** to list all print jobs on *laser1*.
- Step 11. Select all print jobs currently on *laser1*, then select **Job** ⇒ **Transfer**. Transfer the jobs to *laser2*. Click on **OK**.
- Step 12. Click on **OK** again when prompted to transfer the jobs to *laser2*.
- Step 13. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.
- Step 14. Go back to the **Printer Setup Manager**. Select *laser2*, then select **Printer** ⇒ **Control**. Click on **Enable Printing**.
- Step 15. Click on **OK**.
- Step 16. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

8.9 Relevant Commands and Files

The following commands and files were presented in this lesson.

Relevant commands

accept(1M)	Allows print requests to a printer or class of printers
cancel(1)	Cancels print requests
disable(1)	Turns off a printer or class of printers
enable(1)	Turns on a printer or class of printers
lp(1)	Sends requests to a printer
lpsched(1M)	Starts the print service
lpshut(1M)	Stops the print service
lpstat(1)	Prints information about the current status of the print service
lpusers(1M)	Sets printing queue priorities
reject(1M)	Prevents print requests to a printer or class of printers
scoadmin(1M)	Invokes SCOadmin applications (in this lesson, the Print Job Manager and the Printer Setup Manager)

Relevant files

\$HOME/.cshrc	User's C shell login file where a default printer can be set
\$HOME/.profile	User's Bourne or Korn shell login file where a default printer can be set

8.10 Answers to Exercises and Review Questions

This section provides the answers to exercises and review questions presented in this lesson.

Exercise: Stopping the print service

Trying to print the file gives the following error message:

```
Can't establish contact with the LP print service
```

Running the **lpstat(1)** command gives the following error message:

```
The LP print service isn't running or can't be reached
```

Exercise: Rejecting print jobs

Running the **lpstat(1)** command gives the following report:

```
laser1 not accepting requests since DATE - printer  
down, use laser2
```

Trying to print the file gives the following error message:

```
Requests for destination "laser1" aren't being accepted
```

Exercise: Disabling a printer

The system accepts the print request.

Running the **lpstat(1)** command shows the waiting print request.

After the printer is enabled, the print service sends the waiting print job to the printer.

Exercise: Promoting a print job

After the first two promotions:

- The print job that was originally last is now first in the queue
- The print job that was originally second-to-last is now second in the queue

After promoting the originally second-to-last print job again:

- The print job that was originally last is now second in the queue

The print job that was originally second-to-last is now first in the queue

Exercise: Transferring print jobs

The job ID does not change when you transfer a print job to another queue.

Review questions

1. The print service performs these tasks: receives files for printing, schedules the work on one or more printers, starts the interface with specific printers, tracks the status of print jobs, alerts you to printer problems, and issues error messages when problems occur.
2. You should set up a printer to reject print requests when the printer is going to be unavailable for more than one to two hours.
3. You should disable a printer when it is going to be unavailable for only a brief amount of time.
4. Transferring a print job sends it to a different print queue. Promoting a print job places it at the top of the current print queue.
5. You can edit the allow and deny user lists found in the **Control Printer User Access** dialog box in the **Printer Setup Manager**.
6. Check any of these when a printer stops working: check your mail—error messages that occur during printing are often mailed to the user who made the request; use `lpstat -t` to view the status of the printing system—verify that the printer schedule is running and that the printer is enabled and accepting requests; check the power and cables to the printer; verify that the printer hardware is working by checking the printer documentation for a self-test—switch the printer off and on again.

9

Stopping and Starting the System

Instructor Guide

Instructor Guide

Lesson 9

Stopping and Starting the System

Suggested lesson duration

This lesson should take approximately 1.5 hours to complete, including the lab exercise.

Pre-lesson classroom preparation

None.

Instructor preparation

Practice using the SCAdmin System Shutdown Manager.

AV 9-1

The slide is titled "Stopping and Starting the System" in a blue-bordered box at the top. Below the title, there is a bulleted list of three items. At the bottom of the slide, there is a blue footer bar containing the text "sa1g-0901" on the left and "© The Santa Cruz Operation, Inc." on the right.

- Stop (shut down) a UnixWare 7 system
- Start (boot) a UnixWare 7 system
- Switch between system states

sa1g-0901 © The Santa Cruz Operation, Inc.

Instructor Guide

Introduction

Starting and stopping a UnixWare 7 system requires more than just turning the power on and off. You must follow a standard set of procedures to start and stop the system. An improper shut down can result in the loss of data and a corrupted system. This lesson demonstrates the necessary steps to ensure proper operation.

Objectives

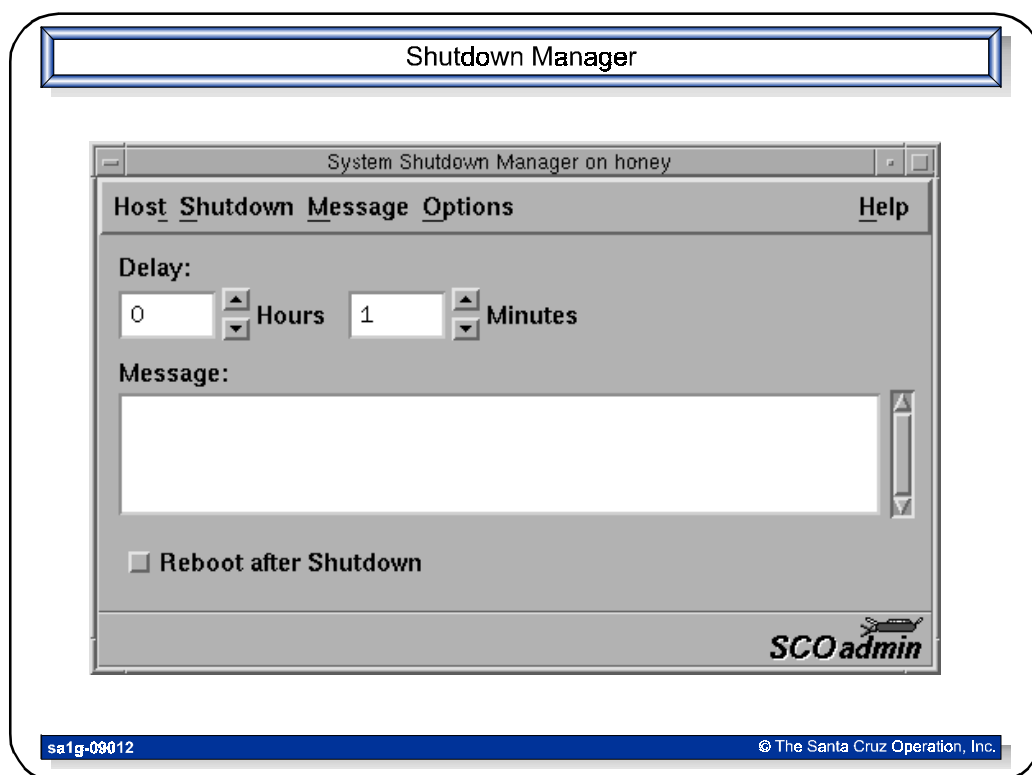
This lesson describes the proper way to shut down and start up a UnixWare 7 system. By the end of this lesson, you will be able to:

- Stop (shut down) a UnixWare 7 system
- Start (boot) a UnixWare 7 system
- Switch between system states

AV 9-1: Stopping and Starting the System

This slide describes the overall topics covered in this lesson.

AV 9-2



9.1 Stopping a UnixWare 7 System

AV 9-2: System Shutdown Manager

Screen shot of the **System Shutdown Manager**.

When performing routine system maintenance you can shut down your system to:

- Replace system hardware
- Clear up hung (defunct) processes or a hung system
- Upgrade system resources, such as processors, memory, or hard disks

Although the UnixWare 7 filesystems are more robust than earlier releases, a proper shut down is still the best way to protect filesystems and user data from corruption.

These precautions are necessary when executing a safe shut down:

- Users must save their work and stop any user processes, including any background processes.
- All users should be logged off the system.

Only the **root**, **owner**, or a user with **shutdown** privileges can shut down the system with the **SCOadmin System Shutdown Manager**. Only the **root** user can shut down the system with the **shutdown(1M)** command.

The following topic describes how you can use the **SCOadmin System Shutdown Manager** to set:

- How many hours and minutes before the system shut down begins.
- What message (if any) displays before the shut down begins.
- Whether or not the system should automatically reboot after the shut down.

For additional information on the **System Shutdown Manager**, refer to **scohelp** ⇒ **System Management** ⇒ **Starting and stopping the system** ⇒ **Stopping the system**.

9.1.1 Normal shut down

These steps describe how to perform a normal shut down:

- Step 1. Start **SCOadmin**. Select **System** ⇒ **System Shutdown Manager**.
- Step 2. Select **Reboot after shut down** if you want the system to automatically reboot.
- Step 3. Enter the amount of time that elapses before the shut down takes place. If you:
- Do not enter an amount of time, the system automatically shuts down in 60 seconds when you perform Step 7.
 - Enter 0 in the **Delay** field, the system shuts down immediately when you perform Step 7.
 - Enter 1 in the **Delay** field, and 15 in the **Minutes** field, the system shuts down in 1 hour and 15 minutes when you perform Step 6.

Step 4. Enter a warning message in the **Message** box to alert users to save their work and log off the system. If you entered 0 in Step 4, you are unable to enter a message.

If your message is consistent, you can create a message and save it to a file. Retrieve the message, select **Message** ⇨ **Retrieve from File**.

Step 5. Note that to save your settings as the default you can Select **Shutdown** ⇨ **Save**.

Step 6. Select **Shutdown** ⇨ **Begin Shutdown**.

Step 7. Click on **OK** to confirm the shut down. Select **Cancel** if you decide to stop the shut down.

You can also use the **shutdown(1M)** command to execute a shut down. You must be in the root (/) directory before issuing this command:

shutdown -g900 -y

This list describes the options used in this example:

- **-g** sets the number of seconds until the shut down starts.
- **-y** allows the shut down to proceed without any further prompts, halts the system, and prompts with “Hit any key to reboot.”

■ This exercise lets students practice a shut down that warns users.

Exercise: Shutting down the system

Create a warning message in */tmp*. Follow the steps under Section 9.1.1, “Normal shut down,” on page 9-8 to shut down the system so that the system warns users and then shuts down in 2 minutes.

9.1.2 Other shut down circumstances

If you bring the system down while users are still logged into the system, they can lose unsaved work. You should only bring the system down quickly if:

- The system is in single-user state
- The shut down process fails
- A hard disk crashes
- A security breach is detected

If the system is in network state, to bring it down quickly, use the **shutdown(1M)** command without any delay:

shutdown -y

If your system is in single-user mode, to shut down and reboot your system, enter:

shutdown -i6 -y

Note that you can run **-i6** in the multiuser and networking states, however a warning is not issued to your users.

The **shutdown(1M)** command uses defaults stored in the */etc/default/shutdown* file. The default delay (grace) set in this file is 0 minutes. If you alter the grace period and then need to bring down the system quickly, use the **-g** option to override the default set in */etc/default/shutdown* with:

shutdown -g0 -y

or

shutdown -g0 -i6 -y

9.2 Starting a UnixWare 7 System

When you power up a system, it goes through several stages before the operating system is fully operational. These stages include:

- Loading the kernel program `/stand/unix` into memory
- Mounting the root filesystem. If necessary, the root filesystem is cleaned before mounting.
- Selecting the state of system operation

At any given time, the system is in one of eight possible states. A system state is a software configuration where a selected group of processes are set to execute. The **init**(1M) program is the general purpose process spawner of the system states. Refer to **init**(1M), for more information on each system state.

9.2.1 Autoboot to network state

Under normal circumstances you can let the system boot automatically.

In previous courses we have covered “Checking and repairing the root filesystem” during boot. By default UnixWare 7 does not prompt the user for interaction. The system runs `/sbin/ckroot`. If necessary, the filesystem is cleaned.

In addition to checking, cleaning if necessary, and mounting the root filesystem, it cleans and mounts any other filesystems that are configured to mount during system boot.

This automatic boot process is useful if the system loses power. When power is restored, the system can usually reboot to normal operations without requiring intervention.

Refer to **boot**(1M) and **boot**(4) for instructions on how to change the automatic boot default values.

9.2.2 Other boot options

If you need to boot a kernel other than `/stand/unix` or enter single-user state, you must respond at the `Starting UnixWare...` message or during the display of the SCO logo image.

9.2.2.1 Booting other versions of the UNIX kernel

During the boot process, the UnixWare 7 logo screen displays. You can interrupt the automatic boot process and go to the UnixWare 7 boot prompt by pressing **ENTER**.

Your screen displays:

```
Bootstrap Command Processor
Ready for boot commands... [? for help]
```

```
[boot]
```

If you press **ENTER**, the system boots the default kernel.

If the default kernel does not load correctly, you can load another version of the kernel. For example, to boot the *unix.old* kernel, enter:

```
[boot] BOOTPROG=unix.old ENTER
[boot] boot ENTER
```

9.2.2.2 Booting to single-user state

Some forms of system maintenance can require you to run the system in single-user state. For example, backing up the root filesystem in single-user state ensures that users are not modifying files while the backup occurs.

Boot the system to single-user state. Access the boot prompt and enter:

```
[boot] INITSTATE=S ENTER
[boot] boot
```

Enter the **root** password to remain in single-user state. While in single-user state:

- Only the **root** account is logged into the system.
- Many system services, such as printing and networking are not operating.
- No user filesystems are mounted.

■ Ask students to stay in single-user state. The next exercise has them return to network state.

Exercise: Booting to single-user state

Boot your system to single-user state. While in single-user state, enter the **ps(1)** command. Which processes are running? Enter the **mount(1M)** command. Which filesystems are mounted?

When you complete your tasks in single-user state, enter the network state.

9.2.2.3 Entering network state

Recall that entering single-user state at the boot prompt required you to enter:

INITSTATE=S

This command initializes single-user state. The two most common states are:

1,S	single-user state
3	networking state

From single-user state, to proceed with normal startup (networking state), enter:

 **d**

Enter Run-Level **3**

When the system enters network state, the following occurs:

- Mounts any non-root filesystems that have been configured to mount during startup. If necessary, the filesystems are cleaned.
- All system-generated processes are running.
- Users can log into the system.

9.3 Switching Between System States

If you are in network state and need to enter single-user state, you can switch to single-user state without rebooting your system. This is useful when performing some system administration tasks.

Use the **shutdown(1M)** command to enter single-user state.

shutdown -i1 -g300 -y

The **-i1** option represents the single-user state also referred to as *run-level 1*.

When the change completes, log in as **root**.

■ There have been reported problems when using **init 3** to return to the networking state.

To return to the networking state, shut down your system and reboot.

9.4 Lesson Summary

Shutting down the system in an orderly fashion provides users with enough warning to save their work. In addition to the **SCOadmin System Shutdown Manager**, you can also use the **shutdown(1M)** command to switch between system states.

Left alone, the system can start up and enter the network state automatically. You can also boot different versions of the UNIX kernel, or bring the system into single-user state for system maintenance.

Review Questions

1. Which users can perform a shut down?

■ The root, owner, and a user with shutdown privileges can perform a shut down.

2. What is the difference between single-user and network state?

■ In single-user state only the root account is logged into the system, and many system services, such as printing and networking, are not operating. Also, the system mounts only the boot (/stand) and root filesystems. In network state, the system checks and repairs filesystems, if necessary, and then mounts any non-root filesystems that are configured to mount during startup. In addition, all system-generated processes are running and users can log into the system.

3. Which command would you use to bring the system from the networking state to single-user state in 15 minutes, and warn the users that the system is coming down?

■ To warn users and bring the system down to single-user state in 15 minutes, enter this command: `shutdown -g900 -i1 -y`

9.5 Relevant Commands and Files

Relevant commands

The following commands were presented in this lesson:

init (1M)	Is the general purpose process spawner of the system states
scoadmin (1M)	Invokes SCOadmin applications (in this lesson, the System Shutdown ⇨ Manager)
shutdown (1M)	Shuts down the system in an orderly manner

Relevant files

<i>/stand/unix</i>	The UnixWare 7 kernel that is loaded into memory during system startup.
<i>/etc/default/shutdown</i>	The file where system shut down defaults are kept.

9.6 Answers to Exercises and Review Questions

This section contains the answers to exercises and review questions covered in this lesson.

Review questions

1. The root, owner, and a user with shutdown privileges can perform a shut down.
2. In single-user state only the root account is logged into the system, and many system services, such as printing and networking, are not operating. Also, the system mounts only the boot (/stand) and root filesystems. In network state, the system checks and repairs filesystems, if necessary, and then mounts any non-root filesystems that are configured to mount during startup. In addition, all system-generated processes are running and users can log into the system.
3. To warn users and bring the system down to single-user state in 15 minutes, enter this command:

shutdown -g900 -i1 -y

.