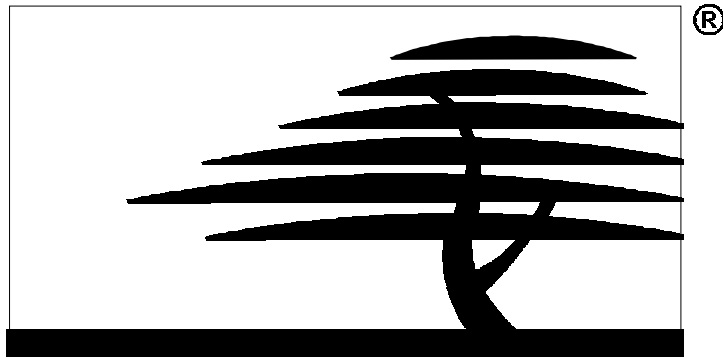




# SCO

**SCO OpenServer™  
Release 5  
Administration I: User  
Services**

Student Guide

Course Release: 2.0.1

For Software: SCO OpenServer™ Release 5



© 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

|                                                      |            |
|------------------------------------------------------|------------|
| <b>Lesson 1: Course Introduction</b>                 | <b>1-1</b> |
| Introduction.....                                    | 1-3        |
| Course goal and purpose.....                         | 1-3        |
| Target audience .....                                | 1-3        |
| Student Materials .....                              | 1-4        |
| The <i>Student Guide</i> .....                       | 1-4        |
| Job aids .....                                       | 1-4        |
| SCO documentation .....                              | 1-4        |
| Using scoadmin(ADM).....                             | 1-5        |
| Sample exam items .....                              | 1-6        |
| Typographical Conventions .....                      | 1-8        |
| <b>Lesson 2: Using SCO Administration Tools</b>      | <b>2-1</b> |
| Using <b>scoadmin</b> (ADM).....                     | 2-5        |
| <b>scoadmin</b> (ADM) clients.....                   | 2-7        |
| Screen areas .....                                   | 2-9        |
| Graphical mode.....                                  | 2-11       |
| Character mode .....                                 | 2-13       |
| Locating Topics in SCO Documentation .....           | 2-14       |
| Overview of documentation.....                       | 2-14       |
| Using online help .....                              | 2-15       |
| Newsgroups .....                                     | 2-20       |
| Other resource sites.....                            | 2-20       |
| Technical support .....                              | 2-21       |
| Using the Superuser Account .....                    | 2-22       |
| Maintaining a System Log.....                        | 2-23       |
| Lesson Summary.....                                  | 2-24       |
| Relevant Commands and Files .....                    | 2-25       |
| Answers to Review Questions .....                    | 2-26       |
| <b>Lesson 3: Administering User Accounts</b>         | <b>3-1</b> |
| Analyzing User Account Requirements .....            | 3-4        |
| User ID.....                                         | 3-5        |
| Login .....                                          | 3-5        |
| Password .....                                       | 3-7        |
| Home directory .....                                 | 3-11       |
| Groups.....                                          | 3-11       |
| Reviewing permissions .....                          | 3-17       |
| Default Discretionary Access Control (DAC) .....     | 3-19       |
| Login environment.....                               | 3-20       |
| Creating, Removing, and Retiring User Accounts ..... | 3-23       |

---

---

|                                                      |      |
|------------------------------------------------------|------|
| Creating a default account .....                     | 3-25 |
| Creating an account using modified defaults.....     | 3-26 |
| Retiring and removing user accounts.....             | 3-27 |
| Modifying Individual Accounts.....                   | 3-31 |
| Modifying individual account information.....        | 3-31 |
| Modifying an individual account environment.....     | 3-32 |
| Modifying the <b>umask</b> of a single account ..... | 3-33 |
| Modifying user passwords .....                       | 3-35 |
| Controlling password expiration.....                 | 3-37 |
| Controlling password selection.....                  | 3-39 |
| Managing User Groups .....                           | 3-40 |
| Modifying group membership .....                     | 3-40 |
| Removing a group.....                                | 3-41 |
| Locking and Unlocking Accounts .....                 | 3-43 |
| Setting login restrictions on user accounts .....    | 3-45 |
| Locking and unlocking a user account .....           | 3-46 |
| Setting login restrictions on terminals .....        | 3-49 |
| Locking and unlocking a terminal .....               | 3-49 |
| Using Account Activity Reports.....                  | 3-53 |
| Reporting password status .....                      | 3-53 |
| Reporting terminal status.....                       | 3-55 |
| Reporting login activity .....                       | 3-57 |
| Troubleshooting User Accounts.....                   | 3-58 |
| Fixing forgotten or compromised passwords.....       | 3-58 |
| Fixing an incorrect terminal type.....               | 3-58 |
| Lesson Summary.....                                  | 3-59 |
| Lab: Creating Groups.....                            | 3-60 |
| Overview.....                                        | 3-60 |
| Procedure .....                                      | 3-60 |
| Lab: Creating New Users.....                         | 3-61 |
| Overview.....                                        | 3-61 |
| Procedure .....                                      | 3-61 |
| Relevant Commands and Files .....                    | 3-63 |
| Answers to Exercises and Review Questions .....      | 3-65 |

---

## Lesson 4: Managing Processes

**4-1**

---

|                                          |     |
|------------------------------------------|-----|
| Describing a Process .....               | 4-4 |
| Definitions .....                        | 4-4 |
| The process table .....                  | 4-4 |
| Viewing current processes .....          | 4-4 |
| Process genealogy .....                  | 4-7 |
| Foreground and background processes..... | 4-7 |
| Daemon processes.....                    | 4-7 |
| Defunct processes .....                  | 4-7 |
| Terminating Processes .....              | 4-9 |

---



---

|                                                       |      |
|-------------------------------------------------------|------|
| The <b>kill</b> (C) command.....                      | 4-10 |
| Using the <b>kill</b> (C) command .....               | 4-11 |
| Scheduling Jobs .....                                 | 4-13 |
| Setting the system date and time.....                 | 4-13 |
| Specifying jobs and scheduled times .....             | 4-17 |
| Listing and modifying user <b>cron</b> (C) jobs ..... | 4-18 |
| Removing <b>cron</b> (C) jobs .....                   | 4-19 |
| Authorizing a user to schedule jobs .....             | 4-21 |
| Lesson Summary.....                                   | 4-22 |
| Lab: Scheduling Processes.....                        | 4-23 |
| Overview.....                                         | 4-23 |
| Procedure .....                                       | 4-23 |
| Relevant Commands and Files .....                     | 4-24 |
| Answers to Exercises and Review Questions .....       | 4-25 |

---

|                                           |            |
|-------------------------------------------|------------|
| <b>Lesson 5: Working with Filesystems</b> | <b>5-1</b> |
|-------------------------------------------|------------|

---

|                                                           |      |
|-----------------------------------------------------------|------|
| Understanding Filesystem Basics .....                     | 5-5  |
| Using Different Filesystem Types.....                     | 5-7  |
| Disk filesystems .....                                    | 5-9  |
| DOS filesystems .....                                     | 5-11 |
| Viewing filesystem information.....                       | 5-11 |
| Mounting and Unmounting a Filesystem.....                 | 5-13 |
| Mounting a filesystem .....                               | 5-13 |
| 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 .....            | 5-19 |
| Monitoring Filesystems .....                              | 5-23 |
| Determining filesystem free space.....                    | 5-23 |
| Determining the size of a directory.....                  | 5-25 |
| Determining disk usage by user .....                      | 5-27 |
| Locating and Managing User Files .....                    | 5-28 |
| Finding large files .....                                 | 5-28 |
| Finding files by owner .....                              | 5-28 |
| Finding and removing <i>core</i> files .....              | 5-28 |
| Managing System Log Files and Temporary Directories ..... | 5-30 |
| Clearing key system logs .....                            | 5-30 |
| Clearing key temporary directories.....                   | 5-31 |
| Lesson Summary.....                                       | 5-32 |
| Lab: Working with a Floppy Disk Filesystem .....          | 5-33 |
| Overview.....                                             | 5-33 |
| Procedure .....                                           | 5-33 |
| Relevant Commands, Files, and Syntax .....                | 5-35 |
| Answers to Review Questions .....                         | 5-36 |

---

---

|                                               |            |
|-----------------------------------------------|------------|
| <b>Lesson 6: Working with Disks and Tapes</b> | <b>6-1</b> |
|-----------------------------------------------|------------|

---

|                                                             |      |
|-------------------------------------------------------------|------|
| Working with Floppy Disks .....                             | 6-5  |
| Identifying floppy device names.....                        | 6-5  |
| Determining a disk media type .....                         | 6-7  |
| Formatting a floppy disk.....                               | 6-9  |
| Working with Tape Drives .....                              | 6-11 |
| Identifying tape device names .....                         | 6-11 |
| Working with tapes .....                                    | 6-12 |
| Transferring Data to Tape or Disk .....                     | 6-13 |
| Absolute versus relative pathnames.....                     | 6-13 |
| Transferring symbolically linked files .....                | 6-14 |
| The <b>tar(C)</b> command.....                              | 6-17 |
| The <b>cpio(C)</b> command.....                             | 6-23 |
| Transferring Data to and from a DOS Disk .....              | 6-27 |
| DOS disk designations.....                                  | 6-27 |
| DOS utilities .....                                         | 6-27 |
| Copying data to DOS filesystems .....                       | 6-28 |
| Lesson Summary.....                                         | 6-30 |
| Lab: Creating an Archive and Extracting Selected Files..... | 6-31 |
| Overview.....                                               | 6-31 |
| Procedure .....                                             | 6-31 |
| Relevant Commands and Files .....                           | 6-34 |
| Answers to Exercises and Review Questions .....             | 6-35 |

|                                     |            |
|-------------------------------------|------------|
| <b>Lesson 7: Filesystem Backups</b> | <b>7-1</b> |
|-------------------------------------|------------|

---

|                                                     |      |
|-----------------------------------------------------|------|
| Organizing and Maintaining Filesystem Backups ..... | 7-4  |
| Using different backup levels .....                 | 7-4  |
| Using a backup schedule.....                        | 7-4  |
| Deciding when to back up filesystems .....          | 7-5  |
| Storing backup media .....                          | 7-5  |
| Maintaining backup logs.....                        | 7-6  |
| Managing Backup Schedules.....                      | 7-7  |
| Creating or modifying a schedule .....              | 7-9  |
| Deleting a Schedule .....                           | 7-10 |
| Backing up a Filesystem .....                       | 7-11 |
| Running a scheduled backup .....                    | 7-13 |
| Examining the backup history .....                  | 7-15 |
| Running an unscheduled backup .....                 | 7-16 |
| Scheduling an Unattended Backup .....               | 7-18 |
| Verifying a Filesystem Backup .....                 | 7-20 |
| Restoring Selected Files.....                       | 7-23 |
| Restoring a Non-root Filesystem .....               | 7-25 |
| Lesson Summary.....                                 | 7-26 |
| Lab: Creating a Default Backup Schedule.....        | 7-27 |
| Overview.....                                       | 7-27 |

---

---

|                                                 |      |
|-------------------------------------------------|------|
| Procedure .....                                 | 7-27 |
| Lab: Backing up and restoring a filesystem..... | 7-28 |
| Overview.....                                   | 7-28 |
| Procedure .....                                 | 7-28 |
| Relevant Commands .....                         | 7-29 |
| Answers to Exercises and Review Questions ..... | 7-30 |

---

|                                    |            |
|------------------------------------|------------|
| <b>Lesson 8: Managing Printers</b> | <b>8-1</b> |
|------------------------------------|------------|

---

|                                                 |      |
|-------------------------------------------------|------|
| Managing the Print Service.....                 | 8-5  |
| Defining the print service .....                | 8-5  |
| Stopping the print service .....                | 8-7  |
| Starting the print service .....                | 8-7  |
| Accepting and Rejecting Print Jobs .....        | 8-11 |
| Rejecting print jobs .....                      | 8-11 |
| Accepting print jobs.....                       | 8-11 |
| Disabling and Enabling Printers .....           | 8-13 |
| Disabling a printer .....                       | 8-13 |
| Enabling a printer.....                         | 8-13 |
| Managing Print Jobs .....                       | 8-17 |
| Viewing print jobs.....                         | 8-17 |
| Canceling print jobs .....                      | 8-18 |
| Holding print jobs .....                        | 8-19 |
| Moving print jobs.....                          | 8-20 |
| Viewing and Changing Printer Settings.....      | 8-23 |
| Setting the default printer .....               | 8-23 |
| Setting a default printer for a user .....      | 8-23 |
| Controlling access to a printer .....           | 8-25 |
| Preventing banner pages .....                   | 8-27 |
| Troubleshooting Printer Problems .....          | 8-28 |
| Lesson Summary .....                            | 8-29 |
| Lab: Managing Printers .....                    | 8-30 |
| Overview.....                                   | 8-30 |
| Procedure .....                                 | 8-30 |
| Relevant Commands and Files .....               | 8-32 |
| Answers to Exercises and Review Questions ..... | 8-33 |

---

|                                                   |            |
|---------------------------------------------------|------------|
| <b>Lesson 9: Stopping and Starting the System</b> | <b>9-1</b> |
|---------------------------------------------------|------------|

---

|                                                    |      |
|----------------------------------------------------|------|
| Stopping an SCO OpenServer System.....             | 9-5  |
| Normal shutdown.....                               | 9-6  |
| Other shutdown circumstances .....                 | 9-9  |
| Starting an SCO OpenServer System .....            | 9-10 |
| Autoboot to multiuser mode .....                   | 9-10 |
| Standard boot .....                                | 9-11 |
| Switching Between System Modes.....                | 9-14 |
| Switching from multiuser to single-user mode ..... | 9-14 |

---

---

|                                                    |      |
|----------------------------------------------------|------|
| Switching from single-user to multiuser mode ..... | 9-14 |
| Lesson Summary .....                               | 9-15 |
| Lab: Abnormal System Startup.....                  | 9-16 |
| Overview .....                                     | 9-16 |
| Procedure .....                                    | 9-16 |
| Relevant Commands .....                            | 9-17 |
| Answers to Review Questions .....                  | 9-18 |

---

## **Appendix A: Starting the Desktop**

**A-1**

---

|                                                    |     |
|----------------------------------------------------|-----|
| Starting the Desktop.....                          | A-4 |
| Exiting the Desktop .....                          | A-4 |
| Using Desktop features .....                       | A-4 |
| Using the mouse.....                               | A-6 |
| Pressing onscreen buttons .....                    | A-6 |
| Using windows .....                                | A-7 |
| Scrolling.....                                     | A-7 |
| Using menus .....                                  | A-8 |
| Using icons .....                                  | A-8 |
| An overview of the SCO Panner window manager ..... | A-9 |

---

# ***1***

## ***Course Introduction***



**Lesson 1**

## **Course Introduction**

### **1.1 Introduction**

---

This *SCO OpenServer Release 5 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 an SCO OpenServer 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 first 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.

## 1.2 Student Materials

---

---

The contents of the box containing your student materials are yours to keep and write notes in as you see fit. 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 *Student Guide* contains:

- Outline of presentation
- Note-taking space
- 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(C)** commands and their functions.

### 1.2.3 SCO documentation

---

This course also includes references to the **SCO OpenServer System Administration Guide**. This guide provides step-by-step procedures an administrator needs to perform to ensure smooth and efficient operation of all services on a SCO OpenServer system. You should have access to this guide during the course.



## 1.3 Using *scoadmin*(ADM)

---

Many procedures in this course require you to start a **SCOadmin** manager such as the **Filesystem Manager**.

SCO OpenServer Release 5 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*(ADM) utilities.

For example, to run the **Filesystem Manager**, a tool that allows you to manage filesystems:

- From the **System Administration** folder, select ⇒ **Filesystems** ⇒ **Filesystem Manager**.
- From a UNIX window, enter **scoadmin**. Select ⇒ **Filesystems** ⇒ **Filesystem Manager**.
- From a UNIX window, enter **scoadmin filesystem**.

Be sure that you are logged in as **root** when invoking these utilities.

## 1.4 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. What is the maximum EAFS filesystem size?
  - A. 2GB
  - B. 256GB
  - B. 512GB
  - C. 1TB
2. Which security profile meets only the minimum requirements for the C2 level of trust?
  - A. High
  - B. Improved
  - C. Traditional
  - D. Low
3. Which file contains a log of device initialization messages:
  - A. */usr/adm/syslog*
  - B. */usr/adm/messages*
  - C. */usr/adm/hwconfig*
  - D. */usr/adm/install.log*

4. Which file contains a list of the filesystems to be checked when you invoke **fsck**(ADM) without arguments?
  - A. `/etc/bcheckrc`
  - B. `/etc/checklist`
  - C. `/etc/ncheck`
  - D. `/etc/default/checklist`
5. During operating system installation, which hard disk setup option is available only if your system has an active UNIX partition with a clean root filesystem and a valid `/etc/default/filesys` file?
  - A. Preserve
  - B. Use whole disk for UNIX
  - C. Customize
  - D. Interactive fdisk/divvy

### Answers to sample exam items

---

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

## 1.5 Typographical Conventions

---

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

|                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lp</b> or <b>lp(C)</b>                                                                                                                                                                                                                                   | 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)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>root</b>                                                                                                                                                                                                                                                 | System 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 superuser from the <b>root</b> 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)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

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



---

# 2

## *Using SCO Administration Tools*

AV 2-1

***Using SCO Administration Tools***

- **Use scoadmin(ADM)**
- **Locate topics in SCO documentation**
- **Identify other sources of information**
- **Describe the importance of the superuser account**
- **Maintain a system log**

sa1-0101

©The Santa Cruz Operation, Inc.

1-1



**Lesson 2**

## **Using SCO Administration Tools**

### **Introduction**

---

A system administrator may be responsible for performing a wide variety of tasks. This course focuses on the most common tasks involved in the routine administration of an SCO OpenServer system.

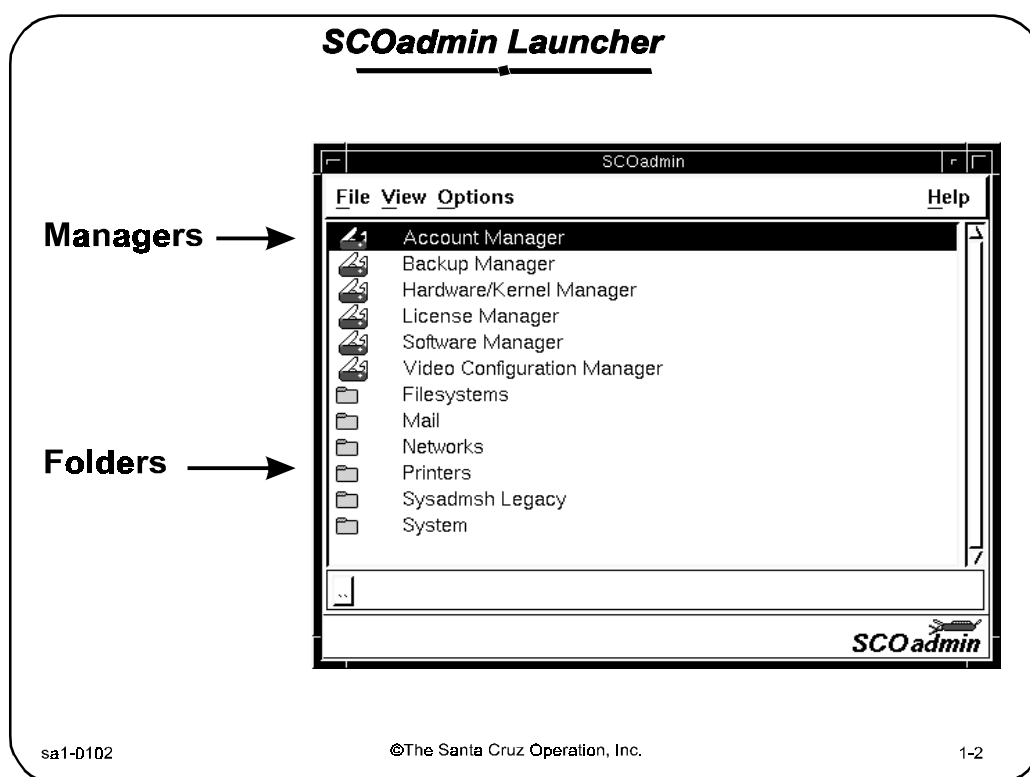
### **Objectives**

---

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**(ADM)
- Locate topics in SCO documentation
- Identify other sources of information
- Describe the importance of the superuser account
- Maintain a system log

AV 2-2



## 2.1 Using **scoadmin**(ADM)

---

Most of the system administration tasks described in this course can be accomplished using **scoadmin**(ADM), SCO's system administration and configuration tool. This tool consists of a series of managers that support both a graphical and a character interface so that you can perform system administration from any terminal or console. All of the functionality of **scoadmin** is available in either interface, but the methods of navigation differ.

Invoke **scoadmin** from a UNIX prompt to start the main program:

**scoadmin**

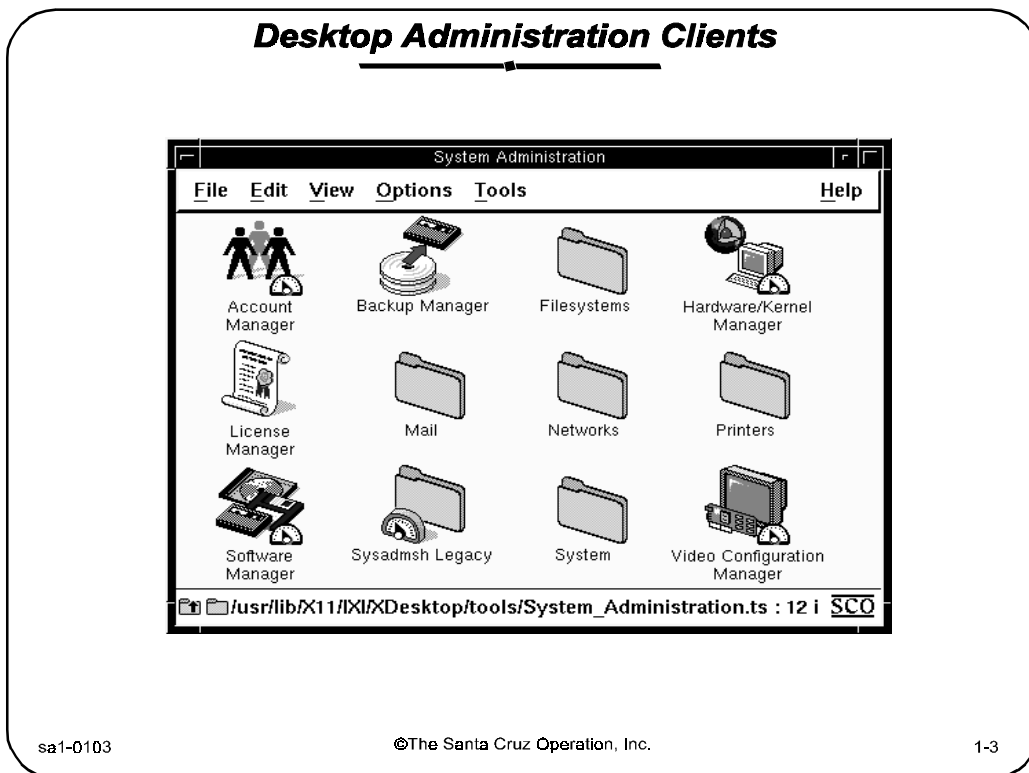
This brings up the launcher, a hierarchical menu to access the individual managers. Most of the managers are nested in subdirectories, or folders.

### **Exercise: Running **scoadmin**(ADM)**

---

Run **scoadmin**(ADM). Open the **System** folder and note the available managers. Close the folder by selecting the double-dot ( . . ) option at the bottom of the screen.

AV 2-3

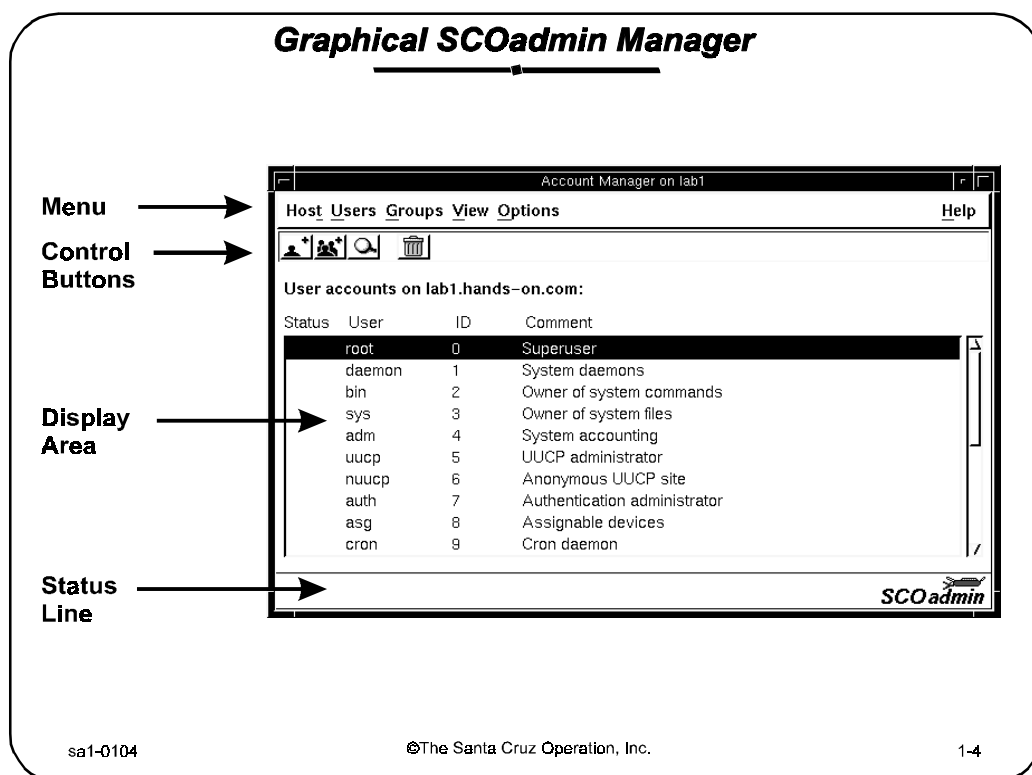


### 2.1.1 scoadmin(ADM) clients

---

If you are using the SCO Desktop, you can also access the various managers from Desktop icons. When the system is freshly installed, you can find all of the managers in the **System Administration** folder. You can move these icons directly to the Desktop for easier access.

## AV 2-4



## 2.1.2 Screen areas

---

In each **scoadmin**(ADM) manager, there are four distinct areas of the window.

### 2.1.2.1 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 allows you to select a remote system to control and the **Help** menu allows you to access context-sensitive online help.

### 2.1.2.2 Display area

---

This section contains the system elements that the manager supports. For example, the display area of the **Account Manager** lists user accounts, and the display area of the **Backup Manager** lists supported filesystems for backup.

### 2.1.2.3 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.

### 2.1.2.4 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.



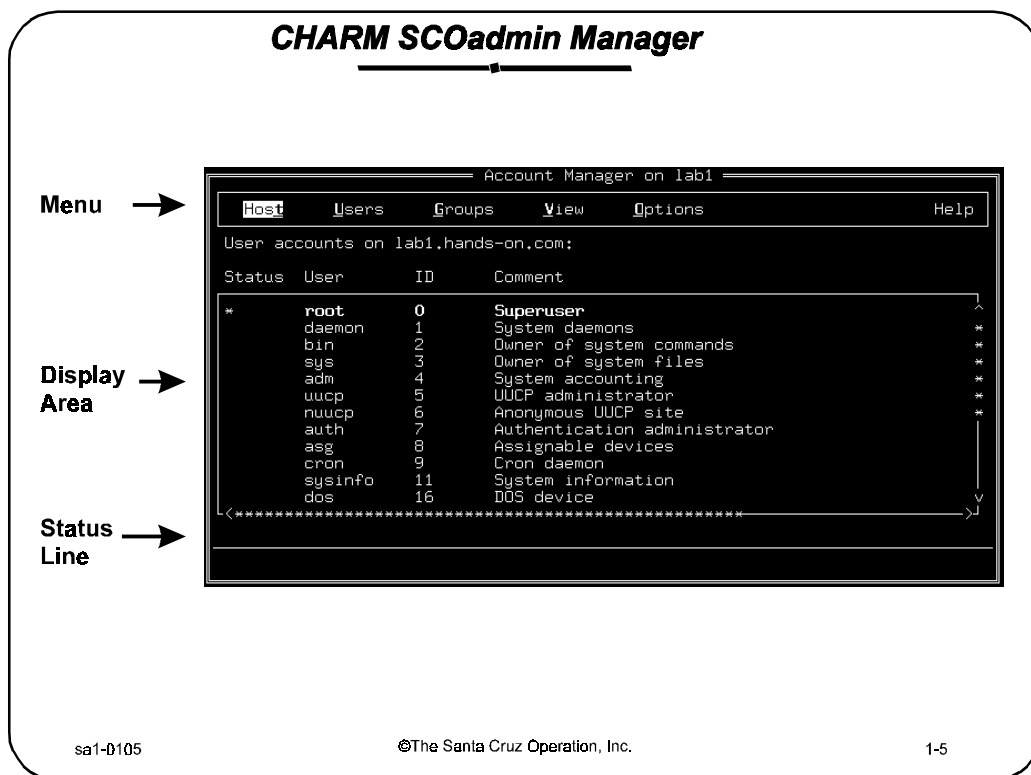
### 2.1.3 Graphical mode

---

The following 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.
- 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

AV 2-5



---

## 2.1.4 Character mode

---

The character mode version of **scoadmin**(ADM) is based upon the Character Motif (CHARM) interface. It executes the same managers as the graphical version, so the layout of the data and menu options are identical. Instead of using a mouse, you can do the following 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 .

### Exercise: Using *scoadmin*(ADM)

---

The file */etc/motd* is a “message of the day” that displays every time a user logs into the system. It is a way for the system administrator to communicate with users about the system. You can modify the message using the **MOTD Manager**:

- |         |                                                                         |
|---------|-------------------------------------------------------------------------|
| Step 1. | Log in as <b>root</b> .                                                 |
| Step 2. | Run <b>scoadmin</b> (ADM). Select <b>System</b> ⇨ <b>MOTD Manager</b> . |
| Step 3. | Edit the message.                                                       |
| Step 4. | Log out, then log in again and confirm the changes to the message.      |

## 2.2 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 and additionally can be purchased as a hard copy package. This section provides an overview of this documentation so that you can easily locate topics to find the answers to your questions.

### 2.2.1 Overview of documentation

---

The major reference books include the following:

- ***SCO OpenServer Handbook***

Introduces the product, covers installation and some basic use of the system, including the Desktop, online help, email, starting and stopping the system, configuring hardware, and installing software. In addition to being available online, this book is always included as hard copy in every SCO OpenServer package.

- ***SCO OpenServer Operating System Administration Guide***

Describes the configuration and maintenance of the base operating system, including account, filesystem, printer, backup, security, UUCP, and virtual disk management.

- ***SCO OpenServer Operating System Administrator's Reference***

Contains the manual pages for system administration commands and utilities (ADM), system file formats (F), hardware-specific information (HW), miscellaneous commands (M), and TCL commands (TCL).

- ***SCO OpenServer Operating System User's Guide***

Provides an introduction to UNIX command-line utilities, the SCO Shell utilities, working with files and directories, editing files with the **vi**(C) editor, transferring files to disk and tape, using DOS disks and files in the UNIX environment, managing processes, shell programming, regular expressions, **awk**(C), and **sed**(C).

- ***SCO OpenServer Operating System User's Reference***

Contains the manual pages for user-accessible operating system commands and utilities (C).

## 2.2.2 Using online help

---

SCO OpenServer systems provide help to both graphical- and character-based users. Graphical **scohelp**(XC) is a complete library of the documentation available for a particular system package.

Character-based help is available to users of the character-based versions of **scoadmin**(ADM). Reference pages for specific commands are available using the **man**(C) command.

Regardless of the tool, online help accesses the same text files located in */usr/lib/scohelp*.

Refer to the *SCO OpenServer Handbook*, “Getting Help.”

### 2.2.2.1 Using the man(C) command

---

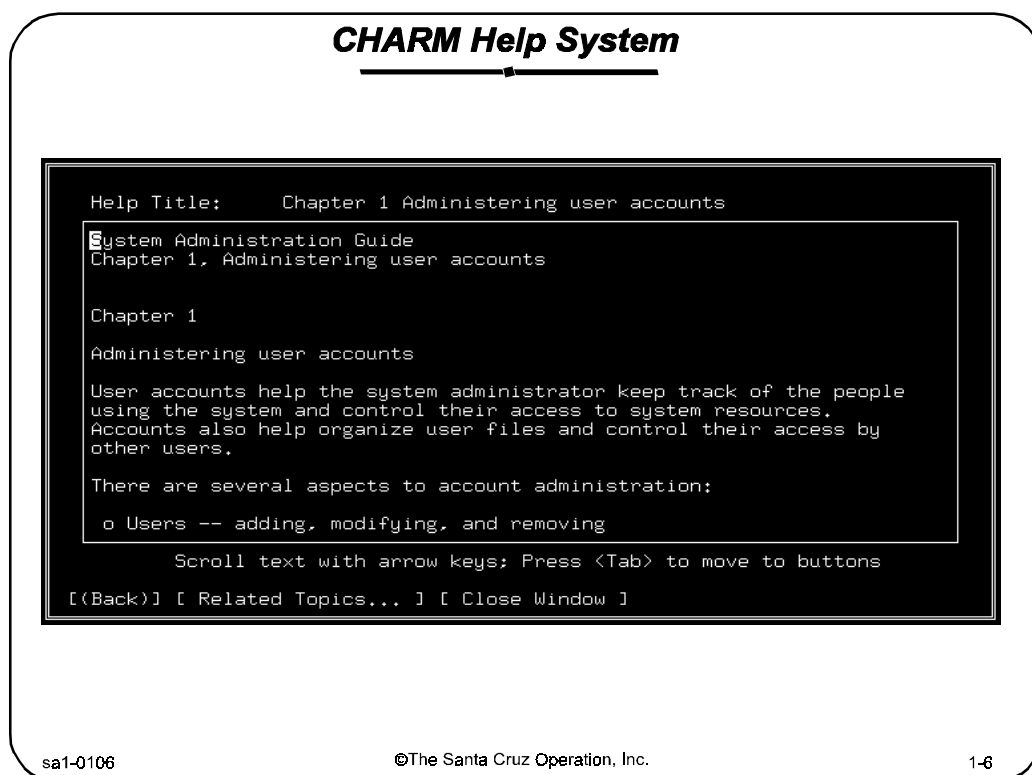
Use the **man**(C) command to access a reference page about a specific command. The file */etc/default/man* contains the default settings for the use of **man**.

#### **Exercise: Using man(C)**

---

Use the **man**(C) command to find information on **man**. Read about */etc/default/man*. Next, view */etc/default/man*.

AV 2-6



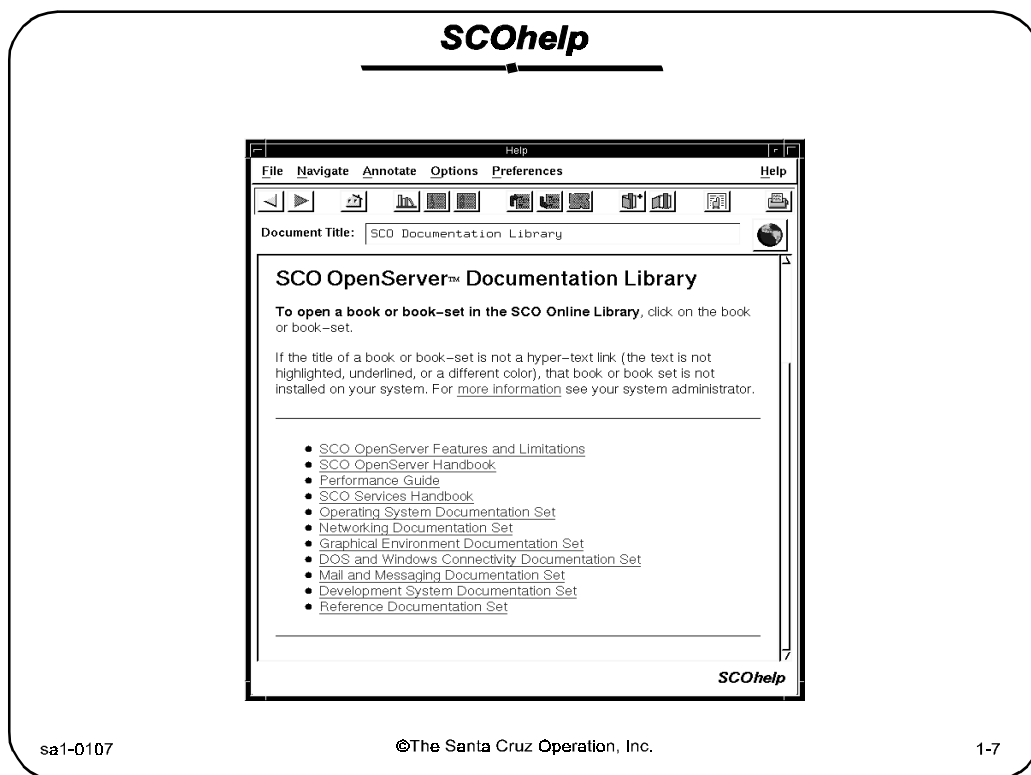
## 2.2.2.2 Using help in a character environment

---

In addition to **man**(C), you can access context-sensitive help while using any of the **scoadmin**(ADM) managers.

Select **Help** from any menu within **scoadmin**(ADM). You can access the relevant portions of the *SCO OpenServer Handbook* and the *SCO OpenServer System Administration Guide*, depending upon which part of **scoadmin**(ADM) you are using.

AV 2-7



sa1-0107

©The Santa Cruz Operation, Inc.

1-7



### 2.2.2.3 Using help in a graphical environment

---

You can access the online documentation as follows:

- From the Desktop, double-click on the **Help** icon or select **Help** ⇒ **On Help**
- From most SCO graphical tools, place your cursor on the element on which you want help, then press  or select the **Help** option from a button or menu

Once the help system is running, you can access any documentation available on your system. This is a hypertext system; clicking on a link takes you immediately to related documentation. There is also a toolbar located at the top of the window with the following buttons:

- Backward and forward arrows move you back and forth across selected hypertext links
- The library button displays a list of available manuals
- The table of contents button displays the table of contents for the current manual
- The index button displays the index of the current manual
- Bookmark buttons allow you to quickly access previously marked topics
- The search button allows you to search for a single key word in the current page, a specified document set, or the entire library
- The print button allows you to print the current page
- The scroll bar allows you to see more of the current page

You can add your comments to any help page using the menu option:  
**Annotate** ⇒ **Annotate**.

## 2.2.3 Newsgroups

---

If you have access to the Internet, you can find many technical newsgroups where users share tips and information. By communicating with a wide range of users, you can often find someone who has encountered and solved a problem similar to yours. SCO-specific newsgroups include:

|                          |                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| comp.unix.sco.announce   | Product, service, and business announcements of reasonable interest to the SCO community of developers, distributors, resellers, consultants, administrators, and end-users |
| comp.unix.sco.misc       | Questions, answers, comments, and discussions about past, present, and future SCO and related third party products and services                                             |
| comp.unix.sco.programmer | Questions, answers, comments, and discussion about past, present, and future SCO development system products and related software and issues                                |

## 2.2.4 Other resource sites

---

In addition to newsgroups, SCO also sponsors the following:

|                                 |                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Home page on the World Wide Web | Provides a graphical interface to browse SCO's technical scripts and to download patches. It is at the following address: <a href="http://www.sco.com/">http://www.sco.com/</a> .                                                                                                                                |
| FTP sites                       | Available on the Internet are two sites for downloading patches via File Transfer Protocol (FTP). If you do not have a Web browser, you can download patches from these sites. These sites are at the following addresses: <a href="ftp.sco.com">ftp.sco.com</a> and <a href="sosco.sco.com">sosco.sco.com</a> . |
| CompuServe                      | SCOFORUM                                                                                                                                                                                                                                                                                                         |

## **2.2.5 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 may encounter while administering the system.

## 2.3 Using the Superuser Account

---

Every UNIX system has a superuser account for system administration. Also known as the **root** account, this account:

- 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.

## **2.4 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

## 2.5 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. Using the CHARM interface, list the steps necessary to change the message of the day.
2. Which manual would you reference to find information about shell programming?
3. Which resource(s) allows you to direct questions to other users of SCO OpenServer systems?
4. Why should you avoid logging in as the superuser unless necessary?
5. Should the system log be kept online? Why or why not?

## 2.6 Relevant Commands and Files

---

The following commands and files were presented in this lesson.

### Relevant commands

---

|                      |                                                                          |
|----------------------|--------------------------------------------------------------------------|
| <b>man(C)</b>        | Displays manual pages                                                    |
| <b>scoadmin(ADM)</b> | Invokes SCOadmin applications (in this lesson, the <b>MOTD Manager</b> ) |
| <b>scohelp(XC)</b>   | Accesses the SCO documentation library                                   |

### Relevant files

---

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| <i>/etc/default/man</i> | Default configuration file for the use of <b>man(C)</b>         |
| <i>/usr/lib/scohelp</i> | Directory containing all of the <b>scohelp(XC)</b> manual pages |

## 2.7 Answers to Review Questions

---

---

This section provides suggested answers to the review questions.

1. To change the message of the day using the CHARM interface, do the following: run **scoadmin**(ADM), select **System** ⇨ **MOTD Manager**, and edit the message.
2. You would reference the *SCO OpenServer Operating System User's Guide* to find information about shell programming.
3. The Internet Newsgroups allow you to direct questions to other users of SCO OpenServer systems.
4. You should avoid logging in as superuser to minimize the danger of unintentionally deleting key files.
5. The system log should not be kept online. If the system crashes to the point where you cannot boot it, you need to be able to access a hard copy log.



---

# 3

## *Administering User Accounts*

AV 3-1

### **Administering User Accounts**

- **Analyze user account requirements**
- **Create, remove, and retire user accounts**
- **Modify individual accounts**
- **Manage user groups**
- **Set, change, and remove login restrictions**
- **Create account and login activity reports**
- **Troubleshoot user accounts**

sa1-0201

©The Santa Cruz Operation, Inc.

2-1

**Lesson 3**

## **Administering User Accounts**

### **Introduction**

---

The main task of any system administrator is to support the use of computer resources by users. Before a user can utilize an SCO OpenServer system, that 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, remove, and retire user accounts
- Modify individual accounts
- Manage user groups
- Set, change, and remove login restrictions
- Create account and login activity reports
- Troubleshoot user accounts

## **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 may have special needs. Setting up system-wide account defaults saves time when it actually comes to creating and maintaining accounts.

This section addresses issues to consider before creating user accounts.

### 3.1.1 User ID

---

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 for individual accounts is 200. The suggested maximum UID is 60000.

Use the same UID to identify a specific person on all systems that person accesses.

### 3.1.2 Login

---

The login is the account name typed in at the `login:` prompt. It must be unique for each user on the system. The login name:

- Can be between 1-8 characters, although the suggested length is between 3-8 characters for compatibility with other UNIX platforms
- 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

**/etc/default/passwd**

```
# PASSLENGTH
# Minimum acceptable password length (unless the user is authorized
# to not have a password). If it is not set, or set to a star (*)
# then the minimum password length is computed based on the
# password lifetime, delay between login attempts and other values.
PASSLENGTH=3

# MINWEEKS
# Minimum number of weeks which must elapse between changes
# of password
MINWEEKS=0

# MAXWEEKS
# Number of weeks before a password must be changed.
MAXWEEKS=0
.
.
.
```

sa1-0202

©The Santa Cruz Operation, Inc.

2-2

### 3.1.3 Password

---

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 them for an individual user.

No one can access the system without a valid account name and password. You can modify password restrictions to make it easier or harder for someone to gain unauthorized access. Some of the restrictions you can set include the following:

|                         |                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimum password length | What is the shortest password a user can have?                                                                                                                                                                                                                                                                                       |
| Password expiration     | If security is important, you want the users to periodically change their passwords. You can set how much time elapses before users are forced to change their passwords. In addition, to prevent them from immediately switching back to a previous password, you can set a minimum time that must elapse between password changes. |

Refer to the *SCO OpenServer System Administration Guide*, “Security Profiles,” for a list of default parameters set according to the security profile.

#### 3.1.3.1 Setting the minimum password length

---

The minimum password length can only be set for the entire system. Change the minimum password length for the system by editing the `PASSLENGTH` field in `/etc/default/passwd`.

AV 3-3

**Modify User Defaults**

tab1: Modify User Defaults

|                           |                                    |                                            |
|---------------------------|------------------------------------|--------------------------------------------|
| Minimum User ID:          | <input type="text" value="200"/>   |                                            |
| Maximum User ID:          | <input type="text" value="60000"/> |                                            |
| Login Shell:              | <input type="text" value="/sh"/>   | <a href="#">Change Login Shell...</a>      |
| Distributed Via:          | <input type="text" value=""/>      | <a href="#">Change Distribution...</a>     |
| Home Directory Base Path: | <input type="text" value="/usr"/>  | <a href="#">Home Directory Options...</a>  |
| Login Group:              | <input type="text" value="group"/> | <a href="#">Change Group Membership...</a> |

sa1-0203©The Santa Cruz Operation, Inc.2-3



### 3.1.3.2 Controlling password expiration

---

Password expiration defaults are set originally when the security profile for the system is selected. The following system-wide defaults can be modified in */etc/default/passwd*:

|          |                                                                                                                                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MINWEEKS | The minimum number of weeks that must elapse between password changes. This prevents a user from circumventing password changes. When forced to change passwords, the user could immediately switch back to the original password if this value is set to zero. |
| MAXWEEKS | The maximum number of weeks that can elapse before the password must be changed. The user must change the password before the login is allowed.                                                                                                                 |

The *login shell* is the command shell the user sees immediately after login. The default shell is the Bourne shell (sh), but the default also can be set to any of the following shells: Korn, C, Restricted Bourne, Restricted Korn, SCO shell, or DOS. Note that the system must have SCO Merge installed before you can select DOS as a shell.

The following steps describe how to view and modify the defaults for account creation:

- Step 1. Run **scoadmin**(ADM)
- Step 2. Select **Account Manager**.
- Step 3. Select **Options** ⇨ **User Defaults**.  
  
Note the User ID range, login shell, home directory, and login group.
- Step 4. Select **Change Login Shell**, select the new login shell, then select **OK** to return to the main defaults window.
- Step 5. Select **OK** to exit the **User Defaults** window.
- Step 6. Select **Host** ⇨ **Exit** to exit the **Account Manager**.

Any defaults changed affect only the creation of new user accounts. Existing accounts are not affected. Note that many account defaults are saved in */etc/default/accounts*.

AV 3-4

### **Group Permissions**

#### **Directory:**

```
drwxrwx--- 2 david sales 688 Jan 1993 reports
```

#### **File:**

```
-rw-r----- 1 david sales 234 Jan 1993 sales.dat
```

```
-rw-rw---- 1 sue market 1256 Mar 1993 forecast
```

#### **Groups:**

```
sales: john, sue, david
```

```
account: peter, mary, donna
```

```
market: john, sue, phil
```

sa1-0204

©The Santa Cruz Operation, Inc.

2-4

### 3.1.4 Home directory

---

#### **Exercise: Setting account defaults**

---

View `/etc/default/accounts` and note how the `SHELL` variable is set. Use the **Account Manager** to change the default login shell to the SCOshell (`scosh(C)`). Now, view `/etc/default/accounts` again. What is the value of `SHELL`?

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 `/usr/login_name`. Many systems have a separate filesystem for user account directories. The default should then create home directories in this separate filesystem, for example `/u/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.

### 3.1.5 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.

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.

#### **Exercise: Reviewing group permissions**

---

Refer to the first graphic on the previous page. Who can read the file *sales.dat*? Who can write to it? Who can read the file *forecast*? Who can write to it?

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

AV 3-5

### **Adding a New Group**

Group Name: 
Group ID:

Distributed Via: 
[Change Distribution...](#)

**Users In Group**

Search for:

Remove >>

<< Add

**Other Users**

adm  
 asg  
 audit  
 auth  
 backup  
 bin

Search for:

sa1-0205
©The Santa Cruz Operation, Inc.
2-5

### 3.1.5.1 Creating a group

---

The following steps describe how to create a new group:

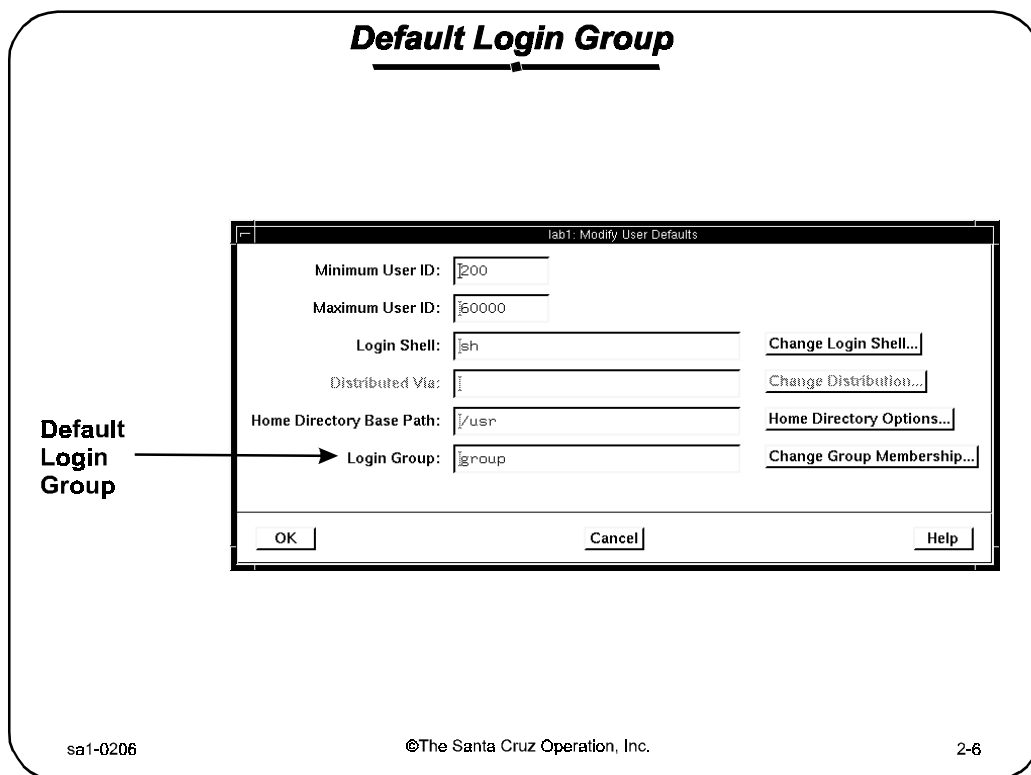
- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager** ⇒ **Groups** ⇒ **Add New Group**.
- Step 3. Enter a group name of 3-8 characters.
- Step 4. Accept the default Group ID or enter a new one.
- Step 5. Add users to the group by selecting them from the **Other Users** list and selecting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

#### **Exercise: Creating a group**

---

Create a new group called *class*.

AV 3-6



### 3.1.5.2 Changing the default login group

---

If the majority of users will belong to a specific group, you may want to set that group to be the default login group. On a freshly installed system, “group” is the default login group.

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

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager** ⇒ **Options** ⇒ **User Defaults**.
- Step 3. Select **Change Group Membership**.
- Step 4. Select the login group.
- Step 5. Select **OK** to accept changes.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

#### **Exercise: Modifying the default login group**

---

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

AV 3-7

### 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(C):

**\$ chmod 644 filename**



### 3.1.6 Reviewing permissions

---

Each file and directory has permissions for the following 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 **chmod**(C) command. This command has the following 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, if you entered the following command to set the permissions for the `/usr/pub/ascii` file:

**chmod 664 /usr/pub/ascii**

The permissions would for the file would look like:

`-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 3-8

**Default Discretionary Access Control**

|                                |                                  |
|--------------------------------|----------------------------------|
| <b>Directories:</b>            | (7) (7) (7)                      |
| Unrestricted permissions:      | <b>drwxrwxrwx</b>                |
| — umask 022                    | 0 2 2                            |
| Permissions of new directories | <b>drwxr-xr-x</b><br>(7) (5) (5) |

|                           |                                  |
|---------------------------|----------------------------------|
| <b>Ordinary files:</b>    | (7) (7) (7)                      |
| Unrestricted permissions: | <b>-rwxrwxrwx</b>                |
| — umask 022               | 0 2 2                            |
| — No execute permission   | <b>---x---x---x</b>              |
| Permissions of new files  | <b>-rw-r--r--</b><br>(6) (4) (4) |

sa1-0208

©The Santa Cruz Operation, Inc.

2-8

### 3.1.7 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 may want to change the default permissions for users within that group. For example, you may want the default permissions to grant write permissions to all members within the group.

#### 3.1.7.1 Review of `umask(C)`

---

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

For example, to set the following default permissions:

Owner              All permissions (none excluded)

Group              All permissions (none excluded)

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

You use the following command:

**`umask 002`**

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

#### 3.1.7.2 Modifying system-wide `umask(C)` 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`. The default **`umask`** in these files is determined by the security profile of the system:

Low and Traditional              022

Improved                          027

High

077

You can modify this setting by editing the appropriate environment file.

---

**Exercise: Setting umasks**

---

**Situation 1:** Set up the Bourne 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 **umask**.

---

### 3.1.8 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

Refer to the ***SCO OpenServer System Administration Guide***, Appendix D, "Sample shell startup files," for a detailed explanation of these files.

### 3.1.8.1 Default account startup files

---

You can find the default files that are copied to the home directories in */usr/lib/mkuser*. There is a subdirectory for each of the shells. Listed below are the shells and the names of their respective startup files:

|              |                                                                         |
|--------------|-------------------------------------------------------------------------|
| Bourne shell | <i>/usr/lib/mkuser/sh/profile</i>                                       |
| C shell      | <i>/usr/lib/mkuser/csh/cshrc</i> and <i>/usr/lib/mkuser/csh/login</i>   |
| Korn shell   | <i>/usr/lib/mkuser/ksh/kshrc</i> and <i>/usr/lib/mkuser/ksh/profile</i> |

These files contain default environment settings:

- Terminal type
- Search path
- Mail folder

### 3.1.8.2 System environment files

---

In addition to these default account files, the following 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 set up by default to do the following:

- Set up the user's umask
- Display the “message of the day” file, */etc/motd*, when the user first logs into the system
- Inform the user if there is unread mail waiting in the mailbox

## **3.2 Creating, Removing, and Retiring User Accounts**

---

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. At this point you would also set the password for the new account to avoid unauthorized access.

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

AV 3-9

## Adding a New User

tab1: Add New User

Login:

User ID:

Comment:

Password:

☒ Set password now
 ☐ Set password later

---

Login Shell:

Distributed Via:

Home Directory:

Login Group:

[Change Login Shell...](#)

[Change Distribution...](#)

[Change Home Directory...](#)

[Change Group Membership...](#)

sa1-0209
©The Santa Cruz Operation, Inc.
2-9



### 3.2.1 Creating a default account

---

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

Step 1. Run **scoadmin**(ADM).

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

Step 3. Enter the login name. Either accept or assign a UID. In the **Comment** field, you can enter information about this user, such as full name, department, and extension.

All of the other fields are set according to defaults.

Step 4. Select **Set password now**.

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

Step 5. Select **OK** to continue.

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

Step 6. Do one of the following:

- Set the password; the system will prompt you to enter the password twice
- Select **Generate password** to have the system select a password. The system displays the generated password. Write it down so that you can give it to the user.
- Select **Set password to blank** (if the security profile allows)

Step 7. Select whether or not you want to force the user to change the password at the first login.

Step 8. Select **OK**. The system creates the user account.

Step 9. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

### 3.2.2 Creating an account using modified defaults

---

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

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager** ⇒ **Users** ⇒ **Add New User**.
- Step 3. Enter the login name. In the **Comment** field, you can enter information about this user, such as the full name, department, and extension. You can also enter a different **User ID**, if desired.
- Step 4. Select **Set password now**.
- Note that, if you select **Set password later**, the user cannot log in until you set the initial password.
- Step 5. Change the default values for additional fields as follows:
- To change the login shell: select **Change Login Shell**, select the appropriate shell, then select **Add Shell Environment Files to Home Directory** to set up the default user environment for that shell. Select **OK** to continue.
  - To change the home directory or its permissions: select **Change Home Directory**, enter the new directory location, and set the permissions for the home directory. Select **OK** to continue.
  - To change group membership: select **Change Group Membership** and set the login group. You see a list of groups and a list of groups to which the account belongs. **Add** and **Remove** groups between those two lists. Select **OK** to continue.
- Step 6. Select **OK** to create the account.
- Step 7. Set the password for this account.
- Step 8. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

**Exercise: Creating a user account**

---

Create an additional user account for yourself. Select your login name. Add *adm* to your group membership, and set your login shell to the Korn shell (*ksh*).

### 3.2.3 Retiring and removing user accounts

---

When a user leaves the company, you should disable that user's account to prevent any unauthorized access. Depending upon the security profile of the system, you can disable a user account as follows:

- Remove the account so that the login name can be reused. This option is not available to systems using the high security profile.
- Retire the account. No one would be able to log into the system using the login name, and the login name is unavailable for reuse. This is available at all security settings.

#### 3.2.3.1 Managing user files

---

In addition to disabling the user account, you must decide what to do with the user's files and directories. Leaving the files unchanged could mean that disk space is used unnecessarily. Also, any files that belong to that user may be restricted to access only by the **root** account.

You have the following two options:

- Back up the files and directories, then delete any files or directories owned by the user. This would free up disk space, but could 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 could then decide which files to keep and which to remove.

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

### **Exercise: Locating user files**

---

Use **find(C)** to locate any files owned by your new user account. For example, if the new user login is **sysadm1**, enter the following:

```
find / -user sysadm1 -print | more
```

### **3.2.3.2 Removing a user**

---

The following steps describe how to remove a user account:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Account Manager**.
- Step 3. Select the user account.
- Step 4. Select **Users** ⇒ **Delete**.
- Step 5. Select **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.
- Step 7. Move any important files to another location.
- Step 8. Remove the user's home directory. The following command assumes the directory is in */usr*:

```
rm -r /usr/login_name
```

Once the home directory has been removed, the account name can be used again.

If you do not remove the home directory, you can still reuse the account name and ID if you specify a different home directory.

You can also use the **rmuser(ADM)** command to remove a user:

```
rmuser username
```

**Exercise: Removing a user account**

---

Remove the **sysadm2** account and delete the home directory. Try to log in as **sysadm2**. Now, create the **sysadm2** account and try to log in again.

### 3.2.3.3 Retiring a user

---

If the user account is to be temporarily out of use, you can retire that user. Both the login name and the user ID are then not available for reassignment. In high security systems, you must retire a user account to disable it.

The following steps describe how to retire a user account:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Account Manager**.
- Step 3. Select the account.
- Step 4. Select **Users** ⇒ **Retire**.
- Step 5. Select **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

**Exercise: Retiring a user account**

---

Retire the **sysadm2** account. Try to log into the system as **sysadm2**. Now try to create a new **sysadm2** account. What happens?

### 3.2.3.4 Unretiring a user

---

Use the **unretire(ADM)** command to reactivate a retired user account:

**unretire login\_name**

You must change the password after using **unretire**. Note that you cannot unretire an account when the system is set to the high (C2) security mode.

### **Exercise: Reactivating a user account**

---

Unretire the **sysadm2** account:

```
unretire sysadm2
```

### 3.3 Modifying Individual Accounts

---

You can make changes to individual accounts. For example, you can modify individual account information, an individual account environment, or the **umask** of a single account. In addition, you can change user passwords and control password expiration and selection.

#### 3.3.1 Modifying individual account information

---

When modifying a user account, you can change any of the values except the login name and user ID. The following steps describe how to modify an existing account:

Step 1. Run **scoadmin**(ADM).

Step 2. Select **Account Manager**.

Step 3. Select the account you want to modify.

Step 4. Select **Users** ⇒ **Modify**.

Note that the screen is the same as the screen to create a new user.

Step 5. Select the desired **Change** option(s) and make the changes. For example, to change the login shell, select **Change Login Shell**.

Step 6. Select **OK** after each change.

Step 7. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

#### **Exercise: Modifying a user account**

---

Modify your **sysadm1** user account so that the **Comment** field states the date and name of this course.

### 3.3.2 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> |

#### **Exercise: Setting a user's search path**

---

If only one group of users access a specific application, you may want to add that application's directory to their individual search paths.

Add */usr/bin/X11* to the search path for your account.



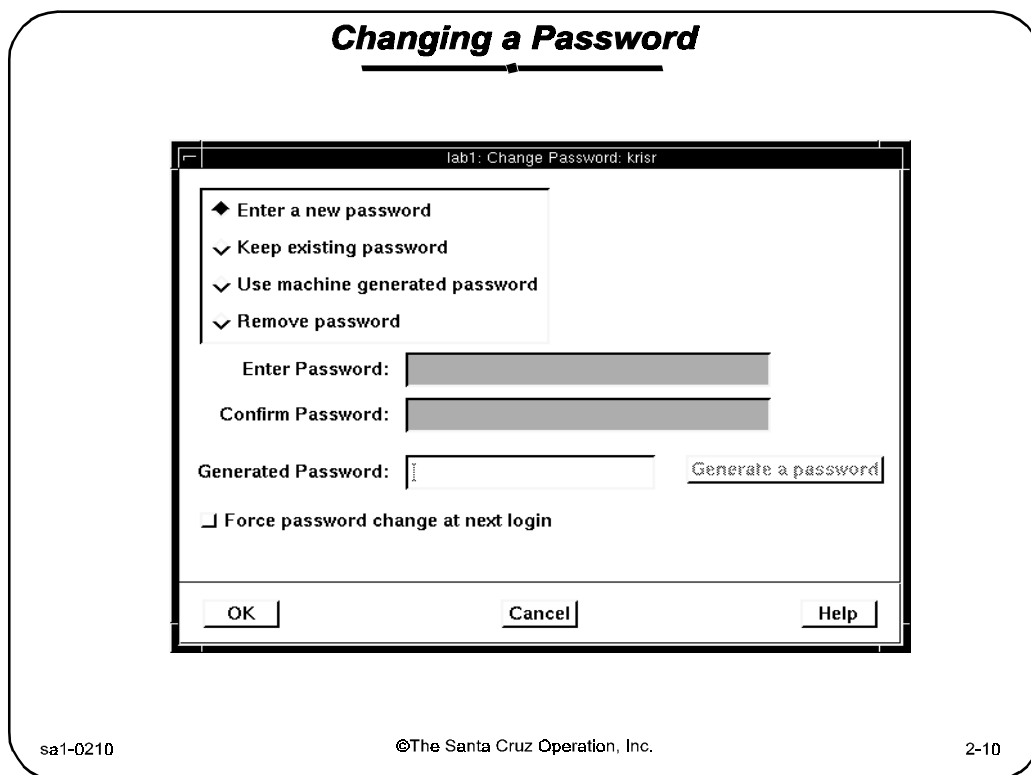
### 3.3.3 Modifying the umask of a single account

---

You can set up a user's environment to use a specific default by including a **umask(C)** 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 hole since the permissions on all new files will differ from the system defaults.

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

AV 3-10



### 3.3.4 Modifying user passwords

---

The following steps describe how to modify a user password:

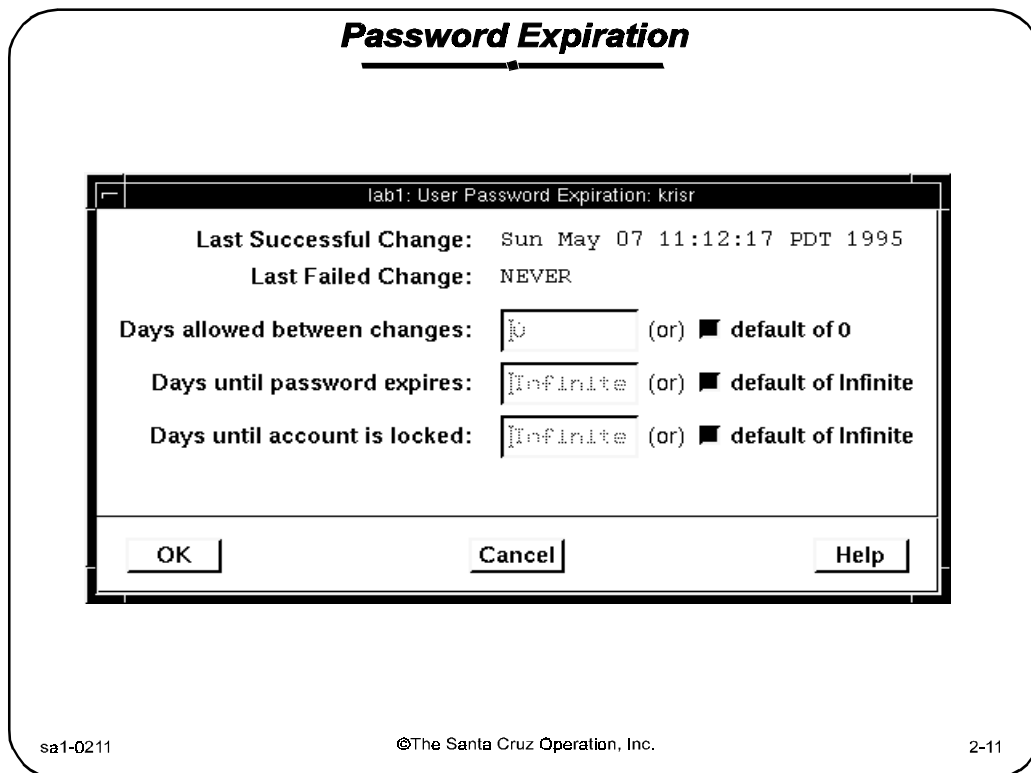
- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select the user.
- Step 4. Select **Users** ⇒ **Change Password**.
- Step 5. Set the password.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

#### **Exercise: Modifying the password for sysadm2**

---

Change the password for **sysadm2**.

AV 3-11



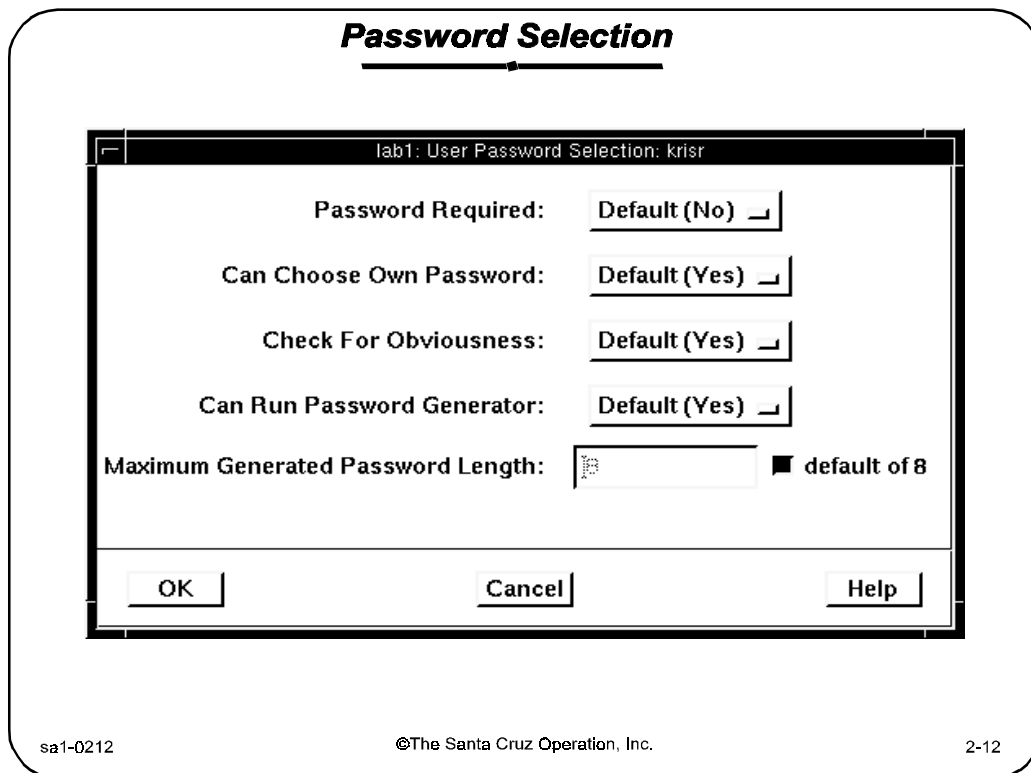
### 3.3.5 Controlling password expiration

---

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

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select the user.
- Step 4. Select **Users** ⇨ **Password Restrictions** ⇨ **Expiration**.
- Step 5. Select the desired values for the following:
  - **Days allowed between changes** is the number of days that must elapse between changes. Deselect the default value and enter a new value.
  - **Days until password expires** is the maximum number of days that can elapse before the password must be changed. Deselect the default value and enter a new value. This number must be larger than the number of days allowed between changes.
  - **Days until account is locked** sets the number of days that must elapse before the account is locked if the user does not change the password. This number should be larger than the number of days until the password expires.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇨ **Exit** to exit the **Account Manager**.

AV 3-12



### 3.3.6 Controlling password selection

---

The following steps describe how to modify the rules regarding an individual user's password selection:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select the user.
- Step 4. Select **Users** ⇒ **Password Restrictions** ⇒ **Selection**.
- Step 5. Set whether a password is required for this account. This does not delete an existing password. You must delete the password.  
  
WARNING! If an account does not have a password, anyone can access the system through this account.
- Step 6. Set whether or not the user can select the password. If set to **No**, the user must let the system generate a password.
- Step 7. Set whether the system should check a user-supplied password for obviousness. This helps users to select passwords that are more difficult to guess.
- Step 8. Set whether the user can generate a password. If the user can generate a password, set the maximum generated password length.
- Step 9. Select **OK**.
- Step 10. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

#### **Exercise: Controlling password selection for sysadm2**

---

Modify the **sysadm2** account so that the user cannot generate a password.

Log in as **sysadm2** and try to change the password by allowing the system to generate it.

## 3.4 Managing User Groups

---

---

You may need to add and remove users from groups, as well as remove groups, as personnel in your company changes.

### 3.4.1 Modifying group membership

---

The following steps describe how to modify a group's membership:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select **View** ⇨ **By Groups**.
- Step 4. Select the appropriate group.
- Step 5. Select **Groups** ⇨ **Modify**.
- Step 6. Add and remove users as desired.
- Step 7. Select **OK**.
- Step 8. Select **Host** ⇨ **Exit** to exit the **Account Manager**.



### 3.4.2 Removing a group

---

The following steps describe how to delete a group:

- Step 1.       Run **scoadmin**(ADM).
- Step 2.       Select **Account Manager**.
- Step 3.       Select **View** ⇒ **By Groups**.
- Step 4.       Select the appropriate group.
- Step 5.       Select **Groups** ⇒ **Delete**.
- Step 6.       Select **OK**.
- Step 7.       Select **Host** ⇒ **Exit** to exit the **Account Manager**.

Once 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**(C) command to modify files still assigned to the deleted group



## **3.5 Locking and Unlocking Accounts**

---

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 will be locked. In that case, you will have to unlock accounts and terminals so that those users can access the system again.

AV 3-13

**Login Restrictions**

lab1: User Login Controls: krisr

|                        | Location       | Time                                |
|------------------------|----------------|-------------------------------------|
| Last Successful Login: | <b>UNKNOWN</b> | <b>Sun May 07 11:12:17 PDT 1995</b> |
| Last Failed Login:     | <b>UNKNOWN</b> | <b>NEVER</b>                        |
| Last Logout:           | <b>UNKNOWN</b> | <b>UNKNOWN</b>                      |

Failed login attempts since last successful login:

**NONE**

Failed login attempts allowed before account is locked:

100

☒ default of 99

Current Account Lock Status:

**Locked**

☐ Unlock Account

Reason:

**Account locked by Administrator**

OK

Cancel

Help

sa1-0213
©The Santa Cruz Operation, Inc.
2-13

### 3.5.1 Setting login restrictions on user accounts

---

Depending upon the security profile of the system, there is a default limit on unsuccessful login attempts. If a particular user account is sensitive or at risk, you can modify the limit.

The following steps describe how to modify the limit for a specific user account:

- Step 1.       Run **scoadmin**(ADM).
- Step 2.       Select **Account Manager**.
- Step 3.       Select the user.
- Step 4.       Select **Users** ⇨ **Login Controls**.  
  
                The window displays the last successful login, the last failed login, the last logout, and the number of failed login attempts since the last successful login.
- Step 5.       Deselect the default limit and enter a new limit.
- Step 6.       Select **OK**.
- Step 7.       Select **Host** ⇨ **Exit** to exit the **Account Manager**.

### 3.5.2 Locking and unlocking a user account

---

If a user accidentally locks his or her account, you must unlock it before it can be used. If a user is going to be away for an extended period of time, you can lock the account to prevent unauthorized logins.

The following steps describe how to lock or unlock an account:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select the user account.
- Step 4. Select **Users** ⇒ **Login Controls**.
  - To unlock a locked account, select **Unlock Account**
  - To lock an unlocked account, select **Lock Account**
- Step 5. Select **OK**. A locked account symbol appears next to the account.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

You can also use **passwd -l** to lock an account:

**passwd -l username**

Use **passwd -u** to unlock an account:

**passwd -u username**

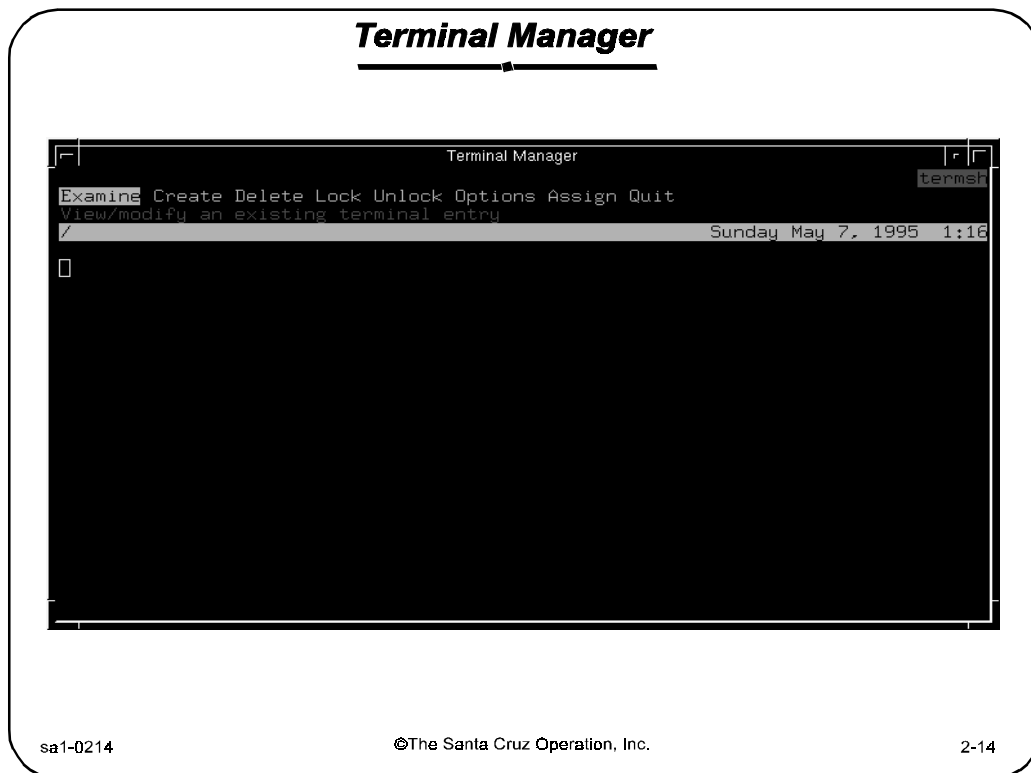
### **Exercise: Locking sysadm2**

---

---

Lock the **sysadm2** account then try to log into the system as **sysadm2**.

AV 3-14





### 3.5.3 Setting login restrictions on terminals

---

The following steps describe how to set login restrictions on terminals:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **System** ⇒ **Terminal Manager**.
- Step 3. Select **Examine**.
- Step 4. Enter the appropriate terminal device file, or press  for a list and select the device.

The window displays the last successful login, the last failed login, the last logout, and the number of failed login attempts since the last successful login.

- Step 5. Select **Specify** for **Consecutive unsuccessful logins**. Enter the desired limit. You can also specify a delay between login attempts and a timeout value for a login attempt.
- Step 6. Select **Quit** ⇒ **Yes** to exit the **Terminal Manager**.

### 3.5.4 Locking and unlocking a terminal

---

The following steps describe how to lock or unlock a terminal:

**WARNING!** Do not lock terminals that are labelled with a *ttyp*. These are pseudo terminals used for networking.

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **System** ⇒ **Terminal Manager**.

- Step 3. Lock or unlock a terminal as follows:

- To lock a terminal, select **Lock**. Enter the appropriate terminal device file, or press **F3** for a list and select the appropriate device. Select **Yes** to confirm the change.
- To unlock a terminal, select **Unlock**. Enter the appropriate terminal device file, or press **F3** for a list and select the appropriate device. Select **Yes** to confirm the change.

Step 4. Select **Quit** ⇒ **Yes** to exit the **Terminal Manager**.

You can also use the **ttymlock**(ADM) and **ttymunlock**(ADM) commands to lock and unlock a terminal. For example:

- To lock *tty05*:

**ttymlock tty05**

- To unlock *tty05*:

**ttymunlock tty05**

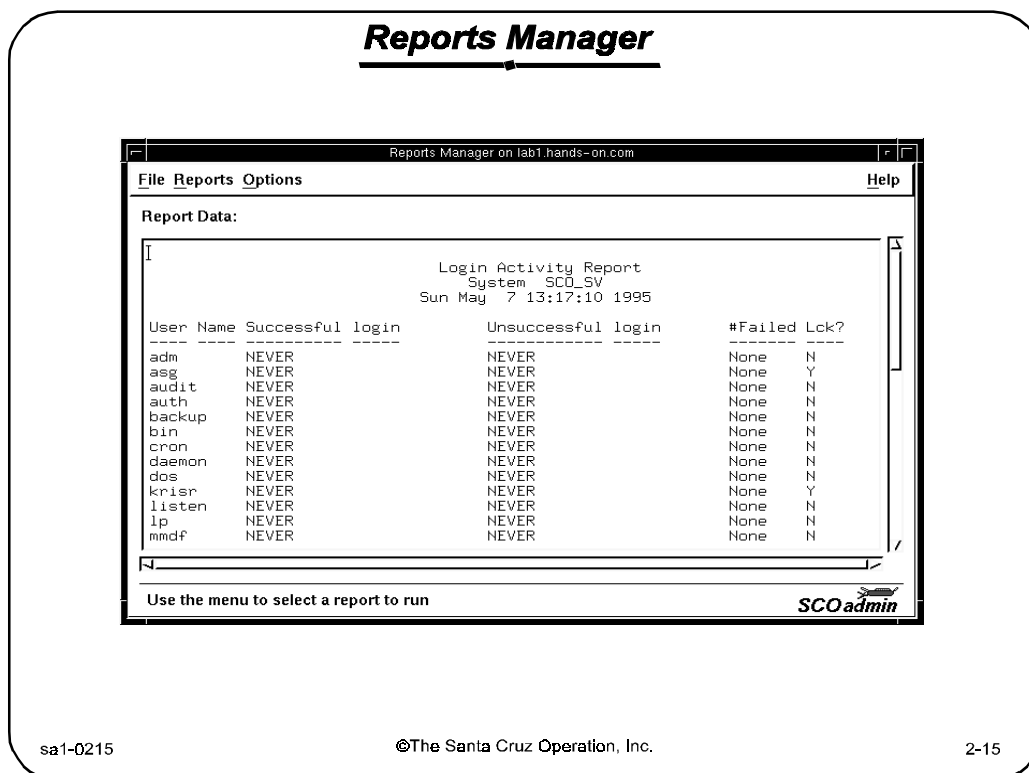
### **Exercise: Locking *tty05***

---

---

Lock the *tty05* multiscreen. Try to log in on that screen.

AV 3-15



## 3.6 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. SCO OpenServer systems provide a **Reports Manager** that generates system-wide reports for account, password, and terminal status.

### 3.6.1 Reporting password status

---

You can run the following three types of password status reports:

- A report that lists all accounts with passwords soon to expire
- A report that lists all accounts with expired passwords
- A report that lists all accounts locked due to expired passwords

The following steps describe how to run a password status report:

- Step 1.        Run **scoadmin(ADM)**.
- Step 2.        Select **System** ⇒ **Security** ⇒ **Reports Manager**.
- Step 3.        Select **Reports** ⇒ **Password Status**.
- Step 4.        Select the report you want to run.
- Step 5.        Select **OK**.
- Step 6.        Select **File** ⇒ **Exit** to exit the **Reports Manager**.

#### **Exercise: Running the password status report**

---

Use the **Reports Manager** to list all accounts with expired passwords.

AV 3-16

### ***Terminal Access Reports***

Terminal Access Status

Select Report to run:

◆ Report on a single terminal

✓ Report on a range of terminals

✓ Report on all terminals on the system

Enter terminal name:

Enter last terminal in range:

OK

Cancel

Help

sa1-0216

©The Santa Cruz Operation, Inc.

2 -16

### 3.6.2 Reporting terminal status

---

The terminal status report can address a single terminal, a range of terminals, or all terminals on the system. The report provides the following information:

- Terminal
- Whether the terminal is locked
- What type of login delay is in effect
- How many unsuccessful login attempts have occurred
- The limit on unsuccessful login attempts for this terminal

The following steps describe how to generate a terminal status report:

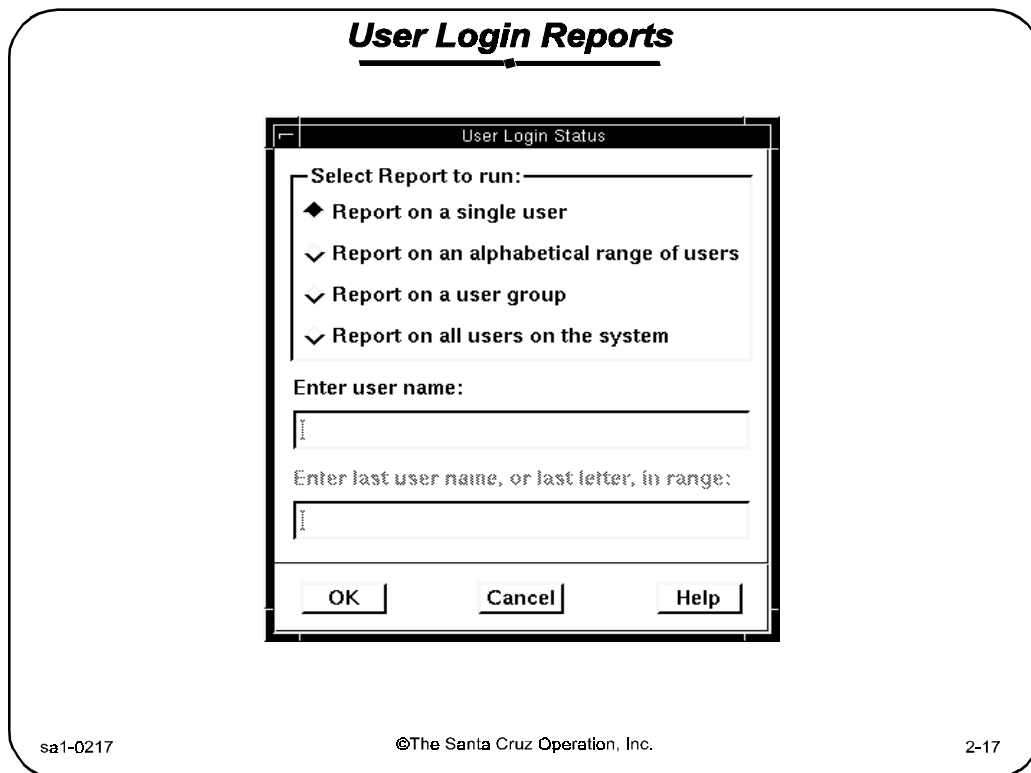
- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **System** ⇒ **Security** ⇒ **Reports Manager**.
- Step 3. Select **Reports** ⇒ **Terminal Access Status**.
- Step 4. Enter the terminal or range of terminals you want to examine.
- Step 5. Select **OK**.
- Step 6. Select **File** ⇒ **Exit** to exit the **Reports Manager**.

#### **Exercise: Running the terminal status report**

---

Use the **Reports Manager** to report on the status of *tty05*. Unlock *tty05* then run the status report again.

AV 3-17





### 3.6.3 Reporting login activity

---

The user login status report can address a single user, a range of users, a specific user group, or all users on the system. The report provides the following information:

- Login name
- Last successful login
- Last unsuccessful login
- Number of failed login attempts
- Lock status

The following steps describe how to generate a login activity report:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **System** ⇒ **Security** ⇒ **Reports Manager**.
- Step 3. Select **Reports** ⇒ **User Login Status**.
- Step 4. Enter the user or range of users you want to examine.
- Step 5. Select **OK**.
- Step 6. Select **File** ⇒ **Exit** to exit the **Reports Manager**.

#### **Exercise: Running the Login Activity report**

---

Use **Report Manager** to report on the status of the **sysadm2** account. Unlock the account, then run the status report again.

## 3.7 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 take to correct them.

### 3.7.1 Fixing forgotten or compromised passwords

---

The following 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.        Unlock the terminal, if necessary.
- Step 4.        Change the password. Force the password to be changed at the next login.
- Step 5.        Remind the user to keep the password private.

### 3.7.2 Fixing an incorrect terminal type

---

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

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

```
TERM=terminal_type  
export TERM
```

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

```
setenv TERM terminal_type
```

## 3.8 Lesson Summary

---

Before users can access a system, they must have 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. What **umask** value grants the owner and members of the group full access, but denies any access to other users?
2. What determines whether you can remove or unretire a user account?
3. What file sets an individual account environment using the Bourne shell?
4. List the steps necessary to remove a user group.
5. Why should you not lock terminals that are labelled with a *ttyp*?
6. List the three types of password status reports that can be generated.
7. Why do you want to confirm a user's identity before unlocking the account?

## 3.9 Lab: Creating Groups

---

---

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

### 3.9.1 Overview

---

Create three new groups: **admin**, **sales**, and **managers**.

### 3.9.2 Procedure

---

First, create the admin group and assign members.

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Account Manager**.
- Step 3. Select **Groups** ⇒ **Add New Group**.
- Step 4. Enter **admin** as the **Group Name**.
- Step 5. Select **OK**.
- Step 6. Repeat Steps 3 through 5 to create the **sales** and **managers** groups (enter the appropriate **Group Name** in Step 4).
- Step 7. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

## 3.10 Lab: Creating New Users

---

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

### 3.10.1 Overview

---

Create user accounts for five individuals. Your instructor will give you a new user password to assign to each of the accounts. Modify the default settings according to the individual's requirements:

|                |                                                                             |
|----------------|-----------------------------------------------------------------------------|
| <b>sales1</b>  | Uses the SCOshell                                                           |
| <b>sales2</b>  | Uses the Korn shell                                                         |
| <b>sysadm3</b> | Uses the Korn shell; also belongs to group backup                           |
| <b>sysadm4</b> | Uses the Korn shell; should log in as a member of the group <b>sysadmin</b> |
| <b>mgr1</b>    | Uses the SCOshell                                                           |

The **sysadm3** and **sysadm4** accounts should both belong to the **admin** group. The **sales1** and **sales2** accounts should both log in as members of the **sales** group. The **mgr1** account should belong to both the **sales** and the **managers** groups.

### 3.10.2 Procedure

---

The following steps describe how to set up and modify user accounts:

- Step 1. Run **scoadmin(ADM)**.
  - Step 2. Select the **Account Manager**.
- Perform the following steps for each account.
- Step 3. Select **Users** ⇨ **Add New User**.
  - Step 4. Enter the login name.
  - Step 5. Enter a comment to describe the account.
  - Step 6. Select **Set password now**.

- Step 7. Select **Change Login Shell**.
- Step 8. Select the correct shell for the user, then select **Add Shell Environment Files to Home Directory**.
- Step 9. Select **OK** to set the login shell.
- Step 10. Select **Change Group Membership**.
- Step 11. Select the group to add from the **Other Groups** list (either **backup** or **sysadmin**), then select **Add**.
- Step 12. Change the login group for the **sysadm4** account to **sysadmin**.
- Step 13. Assign other group memberships as defined above.
- Step 14. Select **OK** to set group membership.

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

- Step 15. Select **OK** from the **Add New User** screen to create the user account. The system sets up the account, including the populated home directory.
- Step 16. Type in the initial the password (provided by your instructor) when prompted in both the **Enter Password** and **Confirm Password** fields.
- Step 17. Select **Force password change at login**, then select **OK** to set the password.
- Step 18. Select **Host** ⇒ **Exit** to exit the **Account Manager**.

### 3.11 Relevant Commands and Files

---

The following commands and files were presented in this lesson.

#### Relevant commands

---

|                        |                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>passwd</b> (C)      | Sets a password. Also locks and unlocks user accounts.                                                                                     |
| <b>setenv</b> (C)      | Sets environment for command execution in the C shell                                                                                      |
| <b>ttylock</b> (ADM)   | Locks terminals                                                                                                                            |
| <b>ttyunlock</b> (ADM) | Unlocks terminals                                                                                                                          |
| <b>scoadmin</b> (ADM)  | Invokes SCOadmin applications (in this lesson, the <b>Account Manager</b> , the <b>Reports Manager</b> , and the <b>Terminal Manager</b> ) |
| <b>umask</b> (C)       | Displays or sets file-creation mode mask                                                                                                   |
| <b>unretire</b> (ADM)  | Unretires a previously retired user                                                                                                        |

#### Relevant files

---

|                                  |                                                      |
|----------------------------------|------------------------------------------------------|
| <i>/etc/cshrc</i>                | System environment file for the C shell              |
| <i>/etc/profile</i>              | System environment file for the Bourne or Korn shell |
| <i>/etc/default/accounts</i>     | File specifying default user account information     |
| <i>/etc/default/passwd</i>       | File specifying default password information         |
| <i>/usr/lib/mkuser/csh/cshrc</i> | Default account environment file for the C shell     |
| <i>/usr/lib/mkuser/csh/login</i> | Default account environment file for the C shell     |
| <i>/usr/lib/mkuser/ksh/kshrc</i> | Default account environment file for the Korn shell  |

|                                    |                                                       |
|------------------------------------|-------------------------------------------------------|
| <i>/usr/lib/mkuser/ksh/profile</i> | Default account environment file for the Korn shell   |
| <i>/usr/lib/mkuser/sh/profile</i>  | Default account environment file for the Bourne shell |
| <i>\$HOME/.chsrc</i>               | Account environment file for the C shell              |
| <i>\$HOME/.login</i>               | Account environment file for the C shell              |
| <i>\$HOME/.kshrc</i>               | Account environment file for the Korn shell           |
| <i>\$HOME/.profile</i>             | Account environment file for the Bourne or Korn shell |



## 3.12 Answers to Exercises and Review Questions

---

This section provides suggested answers to the exercises and review questions.

### Exercise: Setting account defaults

---

The value of SHELL is *scosh*.

### 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: Modifying the default login group

---

Changing the default login group will not affect existing 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: Retiring an account

---

The system does not allow you to re-use the **admin2** account name. Instead, you see the following error message:

Unable to create new user account: admin2

## Answers to review questions

---

1. The umask value 007 grants the owner and members of the group full access, but denies any access to other users.
2. The security profile of the system determines whether you can remove or unretire an account.
3. The *\$HOME/.profile* file sets an individual account environment using the Bourne shell.
4. To remove a user group: run **scoadmin(ADM)**, select the **Account Manager**, select **View** ⇨ **By Groups**, select the appropriate group, select **Groups** ⇨ **Delete**, and select **OK**.
5. You should not lock terminals that are labelled with a *ttyp* because they are *pseudo-terminals* that are used by the network. If you lock the pseudo-terminals, the network loses functionality.
6. The three types of password status reports are: all accounts with passwords soon to expire, all accounts with expired passwords, and all accounts locked due to expired passwords.
7. You should confirm a user's identity before unlocking the account to maintain system security.

---

# 4

## *Managing Processes*

AV 4-1

**Managing Processes**

- **Describe a process**
- **Terminate processes**
- **Schedule jobs**

sa1-0301

©The Santa Cruz Operation, Inc.

3-1

**Lesson 4**

## **Managing Processes**

### **Introduction**

---

Every program that runs on an SCO OpenServer system runs as a process. As the system administrator, you support your users by ensuring that processes are running correctly and by fixing hung processes.

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
- Schedule jobs

## 4.1 Describing a Process

---

Every event that occurs on an SCO OpenServer 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 to best fix them.

### 4.1.1 Definitions

---

A program is a file in the filesystem that contains instructions, or code, to accomplish a task. A process is an instance of a program which is presently executing.

SCO OpenServer 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

---

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

---

To view processes currently in the table, use the **ps(C)** command. 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

### Exercise: Viewing user processes

---

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

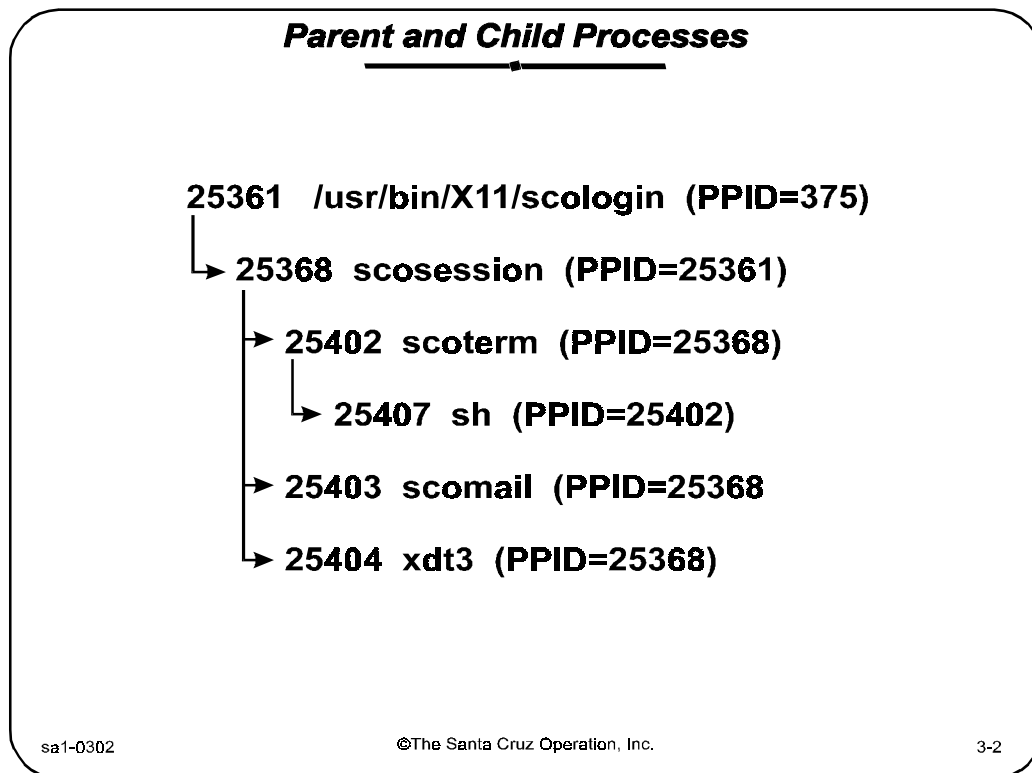
Use **ps -f** to view more information about the processes associated with your current login.

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

Use **ps -ft tty01** to view information about all processes associated with the console.

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

AV 4-2





#### 4.1.4 Process genealogy

---

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

The shell will take most commands and create 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* since 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

---

Daemon processes are processes not associated with a particular terminal or user. They perform system tasks on a periodic basis, and sleep between those tasks.

The **ps(C)** 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**(M) inherits and removes it.

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

## **4.2 Terminating Processes**

---

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

You may 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 will continue to use system time and memory until you terminate them.

### 4.2.1 The kill(C) command

---

You can terminate processes using the **kill(C)** 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 you want to terminate. Non-root users can kill only their own processes.

## 4.2.2 Using the kill(C) command

---

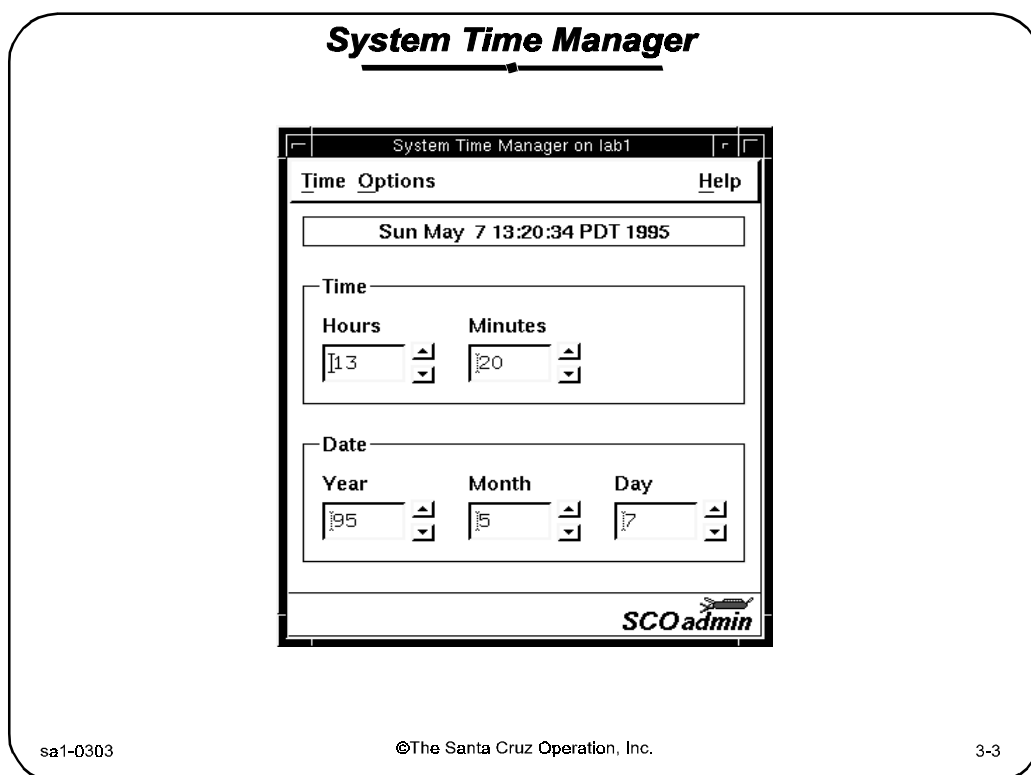
You send various signals to a process when using the **kill(C)** command. Send them in the following order until the process terminates:

- 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 will trap this signal, terminate child processes, and clean up any temporary files before quitting.
- Run **kill PID** on the parent process.

If none of the above signals work, run **kill -9 PID**. Processes cannot trap or ignore this signal. Since 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.

AV 4-3



## 4.3 Scheduling Jobs

---

One way to make your job easier is to automate routine tasks. The **cron**(C) daemon will run these automated tasks at designated hours on designated days. You can schedule non-interactive jobs to run during off-hours when the system load is lighter.

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

### 4.3.1 Setting the system date and time

---

Before you schedule jobs, you should be sure that the system date and time are correct.

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

- Step 1.        Run **scoadmin**(ADM).
- Step 2.        Select **System** ⇨ **System Time Manager**.
- 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.        Select **Time** ⇨ **Set** to set the system clock to the specified date and time.

The following steps describe how to set the date and time using the **asktime**(ADM) command:

Step 1. Enter:

**asktime**

The following prompt appears:

```
Current System Time is Wed Nov 8 08:19:00 PST 1994
Enter new time ([YYMMDD]hhmm[ss]):
```

Step 2. Enter the date and time:

- YYMMDD is an optional date field that consists of year, month, day. For example, to set the clock to February 10, 1995, at 2:30 p.m., enter **9502101430**.
- hhmm is a required field that specifies hours and minutes. Hours should be represented in a 24-hour format. For example, to set the clock to 2:30 p.m., enter **1430**.
- SS is an optional seconds field. For example, to set the clock to 2:30 p.m. with 45 seconds, enter **143045**.

Step 3. Press  .



**Exercise: Setting today's date and time**

---

Set the system clock to the correct date and time.

## AV 4-4

**Format for crontab.eg****crontab.eg**

```

0,15,30,45 * * * 1-5 df -v >>/tmp/df.log
0          3 * * 2-6 cbackup 2 150000 /dev/rct0/dev/u
0          4 28 * *   lp /sales/month_report
30         4 1 1 *    tar cvf /arch/yr_report /sales/*

```

MINUTES    HOURS    MONTH    DAY OF MONTH    DAY OF WEEK    COMMAND

- Fields delimited by spaces or tabs
- The file must not have blank lines

sa1-0304

©The Santa Cruz Operation, Inc.

3-4

## AV 4-5

**crontab(C) Parameters**

| Field        | Allowable Values                            |
|--------------|---------------------------------------------|
| Minute       | 0 - 59                                      |
| Hour         | 0 - 23                                      |
| Day of month | 1 - 31                                      |
| Month        | 1 - 12                                      |
| Day of week  | 0 - 6 (0=Sunday)                            |
| Command      | Any non-interactive command or shell script |

- A field value can be a single value, range of values, or list of values separated by commas
- An asterisk selects all allowable values

sa1-0305

©The Santa Cruz Operation, Inc.

3-5

### 4.3.2 Specifying jobs and scheduled times

---

Jobs and their scheduled times are stored in a file. The file can have any name, but SCO recommends calling it *crontab.eg* because the name clearly states the file's purpose.

The *crontab.eg* file is an ASCII file that can be created with any text editor. Each user can submit only one request file, so the file can contain multiple job requests. A new submission overwrites previous submissions. Each request in the file must contain six fields, separated by spaces or tabs. The first five fields specify when the job should run, and the sixth is the command to run.

The file cannot have any blank lines or header lines. Be sure that you do not include a carriage return at the end of the last line in the file.

#### **Exercise: Specifying cron(C) jobs**

---

Create a **cron(C)** entry to mail the last 10 lines of */usr/adm/syslog* to **root** every Saturday at 11:30 pm.

### 4.3.3 Listing and modifying user cron(C) jobs

---

You can use the **crontab**(C) command to list and modify users' cron jobs. Each user's entry is stored in */usr/spool/cron/crontabs/user\_name*.

To list and modify scheduled jobs:

Step 1.       Enter:

**crontab -e -u user**

Step 2.       Edit the file to add or modify any job requests.

### 4.3.4 Removing cron(C) jobs

---

You can use **crontab -r** to cancel all **cron(C)** activities for a user:

**crontab -r**

WARNING! Running this command as **root** will delete all of the **cron(C)** jobs for **root** that assist in system maintenance.

AV 4-6



### 4.3.5 Authorizing a user to schedule jobs

---

The following files control which users can schedule **cron**(C) jobs:

|                                 |                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>/usr/lib/cron/cron.allow</i> | An explicit list of who can schedule <b>cron</b> (C) jobs. An empty file indicates that none of the users can schedule jobs.                                                       |
| <i>/usr/lib/cron/cron.deny</i>  | An explicit list of who cannot schedule <b>cron</b> (C) jobs. This file is used only if <i>cron.allow</i> does not exist. An empty list indicates that any user can schedule jobs. |

If neither of these files exist, any user can schedule **cron**(C) jobs. If both of these files exist, *cron.allow* takes precedence.

The following steps describe how to use authorize users to submit **cron**(C) requests:

- Step 1.       Run **scoadmin**(ADM).
- Step 2.       Select **System** ⇒ **Cron Manager**.
- Step 3.       Select **Scheduled** ⇒ **Default** to set the permissions for all users. Select **Allow** or **Deny** to permit or deny schedule requests.
- Step 4.       Select **Scheduled** ⇒ **User** to set the permissions for a specific user. Enter the user's name, or press **F3** for a list and select a name. Then select **Allow** or **Deny** to permit or deny schedule requests.
- Step 5.       Press **F2** to exit the **Cron Manager**.

## 4.4 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?
2. Why is it preferable to use **kill -15** instead of **kill -9**?
3. Why should you save your **cron** entries in a separate file such as *crontab.eg*?



## 4.5 Lab: Scheduling Processes

---

In this lab you will schedule tasks to run automatically.

### 4.5.1 Overview

---

Log in as **sysadm1**. View your current **cron(C)** file. Then create scheduled tasks to:

- Search for and remove any *core* files at 5:00pm each day
- Mail the last 50 lines of */usr/adm/messages* to **root** at 8:30am on Mondays

### 4.5.2 Procedure

---

Step 1. List the contents of the current **cron(C)** file:

```
crontab -l
```

Step 2. Use the **find(C)** command to write the **cron(C)** entry to search for core files and remove them:

```
find / -name core -exec rm {} \; 2>/dev/null
```

Step 3. Use the **tail(C)** command to write the **cron(C)** entry to mail the last 50 lines of */usr/adm/messages* to **root**:

```
tail -50 /usr/adm/messages | mail root
```

## 4.6 Relevant Commands and Files

---

---

The following commands and files were presented in this lesson.

### Relevant commands

---

|                      |                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------|
| <b>cron(C)</b>       | Executes commands scheduled by <b>crontab(C)</b>                                                            |
| <b>crontab(C)</b>    | Schedules commands to be executed at regular intervals                                                      |
| <b>kill(C)</b>       | Sends a kill signal to a process                                                                            |
| <b>ps(C)</b>         | Displays information about active processes                                                                 |
| <b>scoadmin(ADM)</b> | Invokes SCOadmin applications (in this lesson, the <b>Cron Manager</b> and the <b>System Time Manager</b> ) |

### Relevant files

---

|                                 |                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------|
| <i>\$HOME/crontab.eg</i>        | Suggested file containing a user's <b>cron(C)</b> requests                               |
| <i>/usr/lib/cron/cron.allow</i> | Contains a list of users allowed to submit <b>cron(C)</b> requests                       |
| <i>/usr/lib/cron/cron.deny</i>  | Contains a list of users explicitly denied the ability to submit <b>cron(C)</b> requests |

## 4.7 Answers to Exercises and Review Questions

---

This section provides suggested answers to the exercises and review questions.

### Exercise: Specifying cron(C) jobs

---

The **cron**(C) entry looks like:

```
30 23 * * 6 tail /usr/adm/syslog | mail root
```

### Review questions

---

1. The difference between a program and a process is that a program is an executable file in the filesystem, while a process is an instance of a program which 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. Signal 9 cannot be trapped, and any temporary files created would not be deleted.
3. You should save your **cron** entries in a separate file such as *crontab.eg* because, if you accidentally delete the **cron**(C) entry, you can resubmit it using the file *crontab.eg*.



---

# 5

## *Working with Filesystems*

AV 5-1

**Working with Filesystems**

- Understand 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

sa1-0401

©The Santa Cruz Operation, Inc.

4-1

**Lesson 5**

## **Working with Filesystems**

### **Introduction**

---

A filesystem is a structure that allows UNIX to store and access files and directories. Unless you make a filesystem available to your users, they cannot access any of the information stored on it. If a filesystem becomes damaged, you will be unable to access any of its data until it has been repaired. If a filesystem fills up, performance degrades and users may not be able to save their work. Maintaining filesystems ensures that users can access the programs and data needed for their jobs.

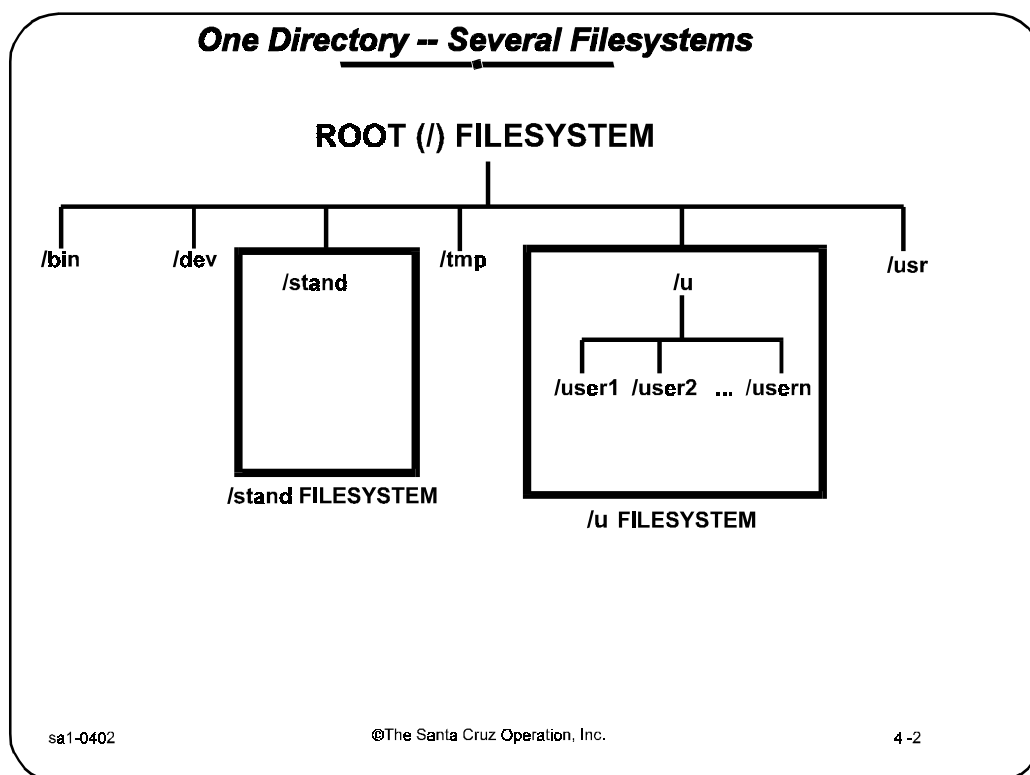
### **Objectives**

---

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

- Understand 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 5-2





## 5.1 Understanding Filesystem Basics

---

Understanding what a filesystem is will help you manage user data effectively. Filesystems must be handled properly to prevent data corruption, and different types of filesystems have different capabilities.

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

A UNIX filesystem is a data structure which 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 once a filesystem is full, it cannot hold any more data.

Permanent filesystems can reside on hard disks, floppy disks, and CD-ROMS. 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.



## **5.2 Using Different Filesystem Types**

---

Different types of filesystems have different capabilities, which may affect how you use them. In most cases, you control the types of filesystems used; the one exception is CD-ROMs. Knowing the types of filesystems supported will allow you to determine whether the system can use a particular CD-ROM.

AV 5-3

**Filesystem Types**

|                      | HTFS | DTFS | EAFS | AFS | S51K |
|----------------------|------|------|------|-----|------|
| Increased Throughput | ✓    |      |      |     |      |
| Data Compression     |      | ✓    |      |     |      |
| Checkpointing        | ✓    | ✓    | ✓    | ✓   | ✓    |
| Logging              | ✓    | ✓    | ✓    | ✓   |      |
| Versioning           | ✓    | ✓    |      |     |      |
| Long Filenames       | ✓    | ✓    | ✓    |     |      |
| Symbolic Links       | ✓    | ✓    | ✓    |     |      |

sa1-0403

©The Santa Cruz Operation, Inc.

4-3

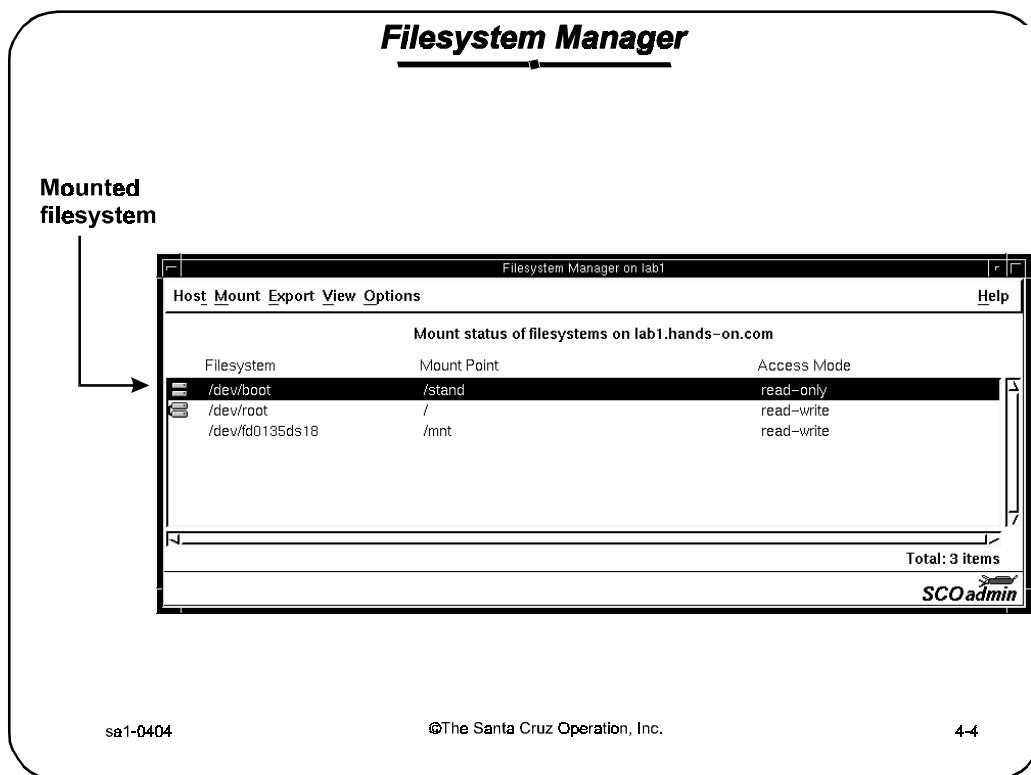
### **5.2.1 Disk filesystems**

---

Following is a list of features available in the various disk filesystems:

|                      |                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Increased throughput | Caching techniques increase the data throughput of your computer                                                                                                                                                                                                                                                  |
| Data compression     | Allows you to store more data in a filesystem. Compression occurs real-time and is transparent to users.                                                                                                                                                                                                          |
| Checkpointing        | Updates the disk from the buffer cache. If your system experiences a system error, checkpointing will reduce the likelihood that the filesystem will need to be checked and repaired when rebooting the system.                                                                                                   |
| Logging              | Reduces the system downtime normally incurred when cleaning a large filesystem. All filesystem activity is logged so in the event of an abnormal shutdown, the log is used to track areas of the disk which need to be cleaned. This reduces time spent on checking and cleaning the filesystem to a few seconds. |
| Versioning           | Allows users to undelete a file                                                                                                                                                                                                                                                                                   |
| Long filename        | Older filesystem types supported filenames up to 14 characters in length. Newer filesystem types support longer file names                                                                                                                                                                                        |
| Symbolic links       | Allow you to link directories and files across different filesystems. Older filesystem types do not support symbolic links.                                                                                                                                                                                       |

AV 5-4



## 5.2.2 DOS filesystems

---

Any MS-DOS® primary partition or disk is also a filesystem recognized by an SCO OpenServer system. These DOS structures can be mounted into the hierarchical directory structure like any other filesystem. Note that you cannot mount a compressed DOS partition.

## 5.2.3 Viewing filesystem information

---

The following steps describe how to view the filesystem types:

Step 1. Run **scoadmin**(ADM).

Step 2. Select **Filesystems** ⇒ **Filesystem Manager**.

A list of known filesystems appears. Note which ones are mounted.

Step 3. Select **View** ⇒ **Filesystem Type**.

Step 4. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

You can also use the **fstyp**(ADM) command to view the filesystem type of a specified filesystem:

**fstyp /dev/root**

As **root**, use the **mount**(ADM) command to identify mounted filesystems:

**mount**

### **Exercise: Viewing the current filesystems**

---

---

View the current filesystems. What type is each?





## 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 want to make a CD-ROM available to users, the filesystem on it will appear within the existing directory structure. The user will not even be able to distinguish between data on the CD-ROM and data on the hard disk.

Before a user can access data in a filesystem, it must be incorporated into the existing directory structure. This process is known as *mounting* a filesystem.

### 5.3.1 Mounting a 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 the following two pieces of information:

- The device file associated with the filesystem
- The existing directory to which you will mount the filesystem, known as the *mount point*

#### 5.3.1.1 Filesystem device files

---

Each filesystem has an associated device file. Some of the common filesystems are listed below with their respective device files:

|                            |                        |
|----------------------------|------------------------|
| root filesystem            | <code>/dev/root</code> |
| <code>/u</code> filesystem | <code>/dev/u</code>    |
| Primary floppy disk        | <code>/dev/fd0</code>  |
| Primary CD-ROM             | <code>dev/cd0</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.

If the mount point directory contains any files, you will not be able to access those files as long as a filesystem is mounted to that point. Specify the mount point as an absolute pathname. Ideally, the mount point should always be an empty directory.

The following steps describe how to mount a filesystem:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Filesystems** ⇒ **Filesystem Manager**.
- Step 3. Select the filesystem you want to mount.
- Step 4. Select **Mount** ⇒ **Mount**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

You can also use the **mount**(ADM) command to mount a filesystem:

**mount /dev/filesystem\_device mount\_point**

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 to the */mnt* directory, you would use the following command:

**mount -r /dev/cd0 /mnt**

#### **Exercise: Mounting a floppy disk filesystem**

---

Mount the floppy disk filesystem to the */mnt* directory.

### **5.3.1.3 Why mounting may fail**

---

If a mount operation fails, check for the following 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 or using a file in the mount directory?  
Use **fuser**(ADM) to determine if anyone is using the directory:

**fuser -u /mount\_point**

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.

### 5.3.2 Unmounting a filesystem

---

To unmount a filesystem, no one can be using it. That means that user, including the root account, should have the mount point directory or any of its subdirectories as the 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**

The following steps describe how to unmount a filesystem:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Filesystems** ⇒ **Filesystem Manager**.
- Step 3. Select the filesystem you want to unmount.
- Step 4. Select **Mount** ⇒ **Unmount**.
- Step 5. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

To unmount a filesystem from the command line, use one of the following **umount(ADM)** commands:

**umount /dev/filesystem\_device**

or

**umount mount\_point**

#### **Exercise: Unmounting a floppy disk filesystem**

---

Unmount the floppy disk filesystem, then mount it again to 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. If the filesystem mounts during startup, the system normally is configured to check and repair it before mounting it. You would need to 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
- Power failure
- Improper shutdowns

The last two are the most common causes of filesystem corruption.

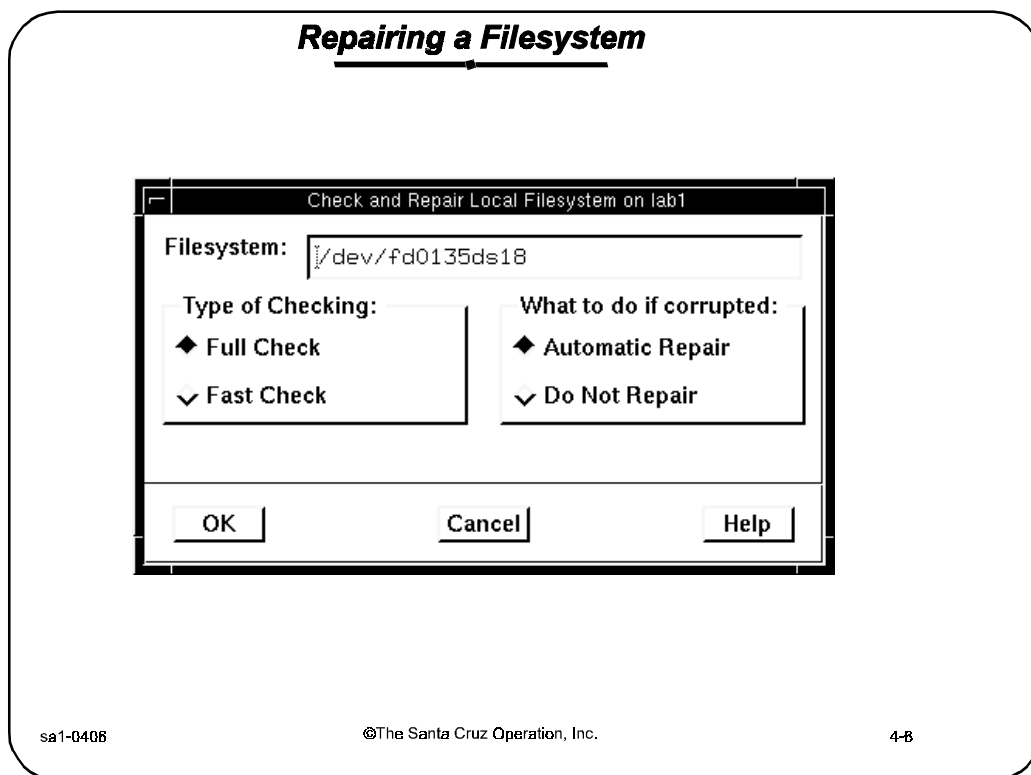
### 5.4.2 The *lost+found* directory

---

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.



AV 5-6



### 5.4.3 Repairing a non-root filesystem manually

---

WARNING! Do not perform this procedure on the root filesystem.

The following basic steps must occur to manually repair a filesystem:

Step 1. Unmount the filesystem.

Step 2. Repair the filesystem.

Step 3. Mount the filesystem.

If the filesystem is already mounted, you can use the **Filesystem Manager** to unmount the filesystem, repair it, and mount it again. Perform the following steps:

Step 1. Run **scoadmin(ADM)**.

Step 2. Select **Filesystems** ⇒ **Filesystem Manager**.

Step 3. Select the filesystem that you want to repair.

Step 4. Select **Mount** ⇒ **Check and Repair** ⇒ **Selected Filesystem**.

Note: If you want to check a filesystem not listed, select **Check and Repair** ⇒ **Other Local Filesystem**. Then, enter the filesystem device file.

Step 5. Select either **Full** or **Fast** checking.

Step 6. Do one of the following:

- Select **Automatic Repair** if you want the system to automatically repair any filesystem problems
- Select **Do Not Repair** if you do not want the system to automatically repair any filesystem problems

Step 7. Select **OK** to start the check. An **Fsck Status** window appears to report progress.

Step 8. Select **Close** when complete to exit the **Fsck Status** window.

Step 9. Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.

If the filesystem was mounted prior to checking, the system will unmount the filesystem, check and repair it, and mount it again. If the filesystem was not mounted prior to checking, the system will simply check it. You must mount it to make the data available.

Use the **fsck**(ADM) command to check and repair the filesystem from the command line. Cleaning the filesystem may not fix everything. Save the output in case it is needed later for analysis.

**umount /dev/filesystem\_name**

**fsck -y /dev/filesystem\_name 2> log\_file**

**mount /dev/filesystem\_name /mount\_point**



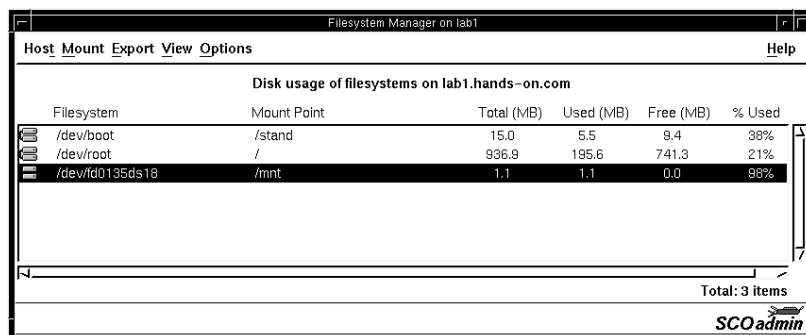
**Exercise: Repairing a floppy disk filesystem**

---

Check and repair the floppy filesystem.

AV 5-7

### ***Filesystem Free Space***



The screenshot shows a window titled "Filesystem Manager on lab1". It has a menu bar with "Host", "Mount", "Export", "View", "Options", and "Help". Below the menu bar is a table titled "Disk usage of filesystems on lab1.hands-on.com". The table has six columns: "Filesystem", "Mount Point", "Total (MB)", "Used (MB)", "Free (MB)", and "% Used". There are three rows of data. The first row is for "/dev/boot" with a total of 15.0 MB, 5.5 MB used, 9.4 MB free, and 38% used. The second row is for "/dev/root" with a total of 936.9 MB, 195.6 MB used, 741.3 MB free, and 21% used. The third row is for "/dev/d0135ds18" with a total of 1.1 MB, 1.1 MB used, 0.0 MB free, and 98% used. The third row is highlighted. At the bottom right of the table area, it says "Total: 3 items". The "SCOadmin" logo is in the bottom right corner of the window.

| Filesystem     | Mount Point | Total (MB) | Used (MB) | Free (MB) | % Used |
|----------------|-------------|------------|-----------|-----------|--------|
| /dev/boot      | /stand      | 15.0       | 5.5       | 9.4       | 38%    |
| /dev/root      | /           | 936.9      | 195.6     | 741.3     | 21%    |
| /dev/d0135ds18 | /mnt        | 1.1        | 1.1       | 0.0       | 98%    |

Total: 3 items

SCOadmin

sa1-0407

©The Santa Cruz Operation, Inc.

4-7

## 5.5 Monitoring Filesystems

---

When a filesystem comes close to being full, performance will start to suffer. If the filesystem actually fills up, users and programs will not be able to save any data to that filesystem. You should never allow a filesystem to completely fill up. Before that occurs, you should either increase the size of the filesystem or delete unnecessary data. As the system administrator, it is your responsibility to keep track of filesystem usage for proper planning.

### 5.5.1 Determining filesystem free space

---

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

- Step 1.        Run **scoadmin**(ADM).
- Step 2.        Select **Filesystems** ⇨ **Filesystem Manager**.
- Step 3.        Select **View** ⇨ **Disk Usage**.  
  
                  Note that the list displays the total size of each filesystem, the number of megabytes used, the number of megabytes free, and the percentage of filesystem used.
- Step 4.        Select **Host** ⇨ **Exit** to exit the **Filesystem Manager**.

To check the free space from the command line, use the **df**(C) command:

**df -kv**

The **-k** option displays size in 1KB blocks. The **-v** option reports the percent of used blocks as well as the number of used and free blocks.

SCO OpenServer filesystem performance will begin to degrade when filesystem free space drops below 15%.

AV 5-8

### **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**

sa1-0408

©The Santa Cruz Operation, Inc.

4-8

**Exercise: Determining free space on a filesystem**

---

Determine how much free space is on each of the filesystems.

## 5.5.2 Determining the size of a directory

---

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

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

```
du / | sort -nr | head
```

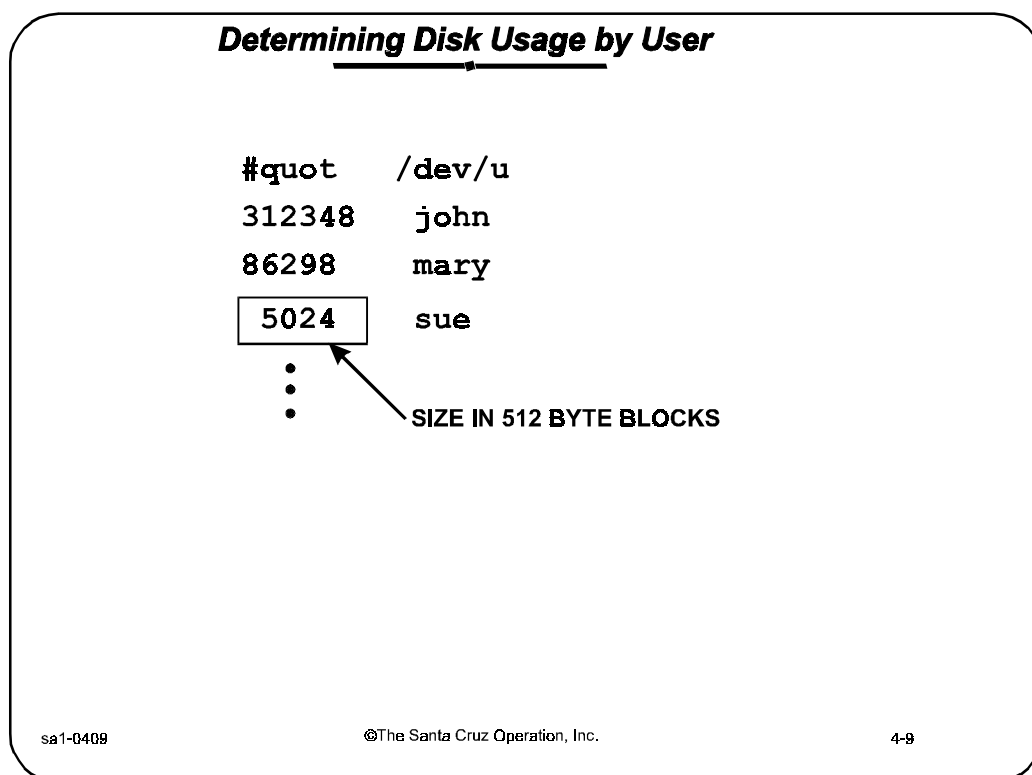
The **-n** option sorts by numeric value. The **-r** option reverses the order of the sort.

**Exercise: Identifying the largest directories**

---

Determine the ten largest subdirectories on the system.

AV 5-9



sa1-0409

©The Santa Cruz Operation, Inc.

4-9

### 5.5.3 Determining disk usage by user

---

If a filesystem is close to full, you may want to 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**(ADM) command to determine space used by each user:

**quot /dev/*filesystem\_name***

#### **Exercise: Determining disk usage**

---

---

Determine disk usage by user for the `/u` filesystem:

**quot /dev/u**

## 5.6 Locating and Managing User Files

---

Throughout normal operation, both users and programs will save files to a filesystem. Most of these files are normal data files, but some may be *core* files, created when a program failed. You can 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 may use valuable free space.

You also may want to 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, you may need to adjust your filesystem organization to compensate for usage.

In any of these situations, the **find(C)** 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 -print
```

### 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 -print
```

### 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*, and it contains a copy of the terminated program.

You can find and automatically delete core files using the **find(C)** command:

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

Use the **-ok** 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(C)** command:

```
sort /etc/termcap
```

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

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

## 5.7 Managing System Log Files and Temporary Directories

---

The SCO OpenServer 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, you should 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 may be left behind if a program encountered an error or a user stopped 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

---

You may want to print or archive a log before clearing it. Do not delete a log file because the file ownership and permissions may change when it is recreated. Also, deleting the file only removes the symbolic link, not the actual data. Instead, do the following:

**> *log\_filename***

Some of the main system-wide log files that grow quickly are:

|                                       |                     |
|---------------------------------------|---------------------|
| <i>/etc/wtmp</i>                      | Account records     |
| <i>/usr/adm/messages</i>              | System messages log |
| <i>/usr/adm/syslog</i>                | System events log   |
| <i>/usr/spool/lp/admins/lp/logs/*</i> | Printer logs        |

## 5.7.2 Clearing key temporary directories

---

The main system-wide temporary files are:

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

Check these directories periodically and remove older files.

## 5.8 Lesson Summary

---

---

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

Finally, monitoring and managing disk space assures that the system can continue to support your users' work. Upgrade the disk space before it fills to capacity.

### Review questions

---

1. What must occur before a user can access the files on a filesystem?
2. Which filesystems support long filenames?
3. List three situations that might cause a mount command to fail.
4. If the system is cleaning the `/u` filesystem, in what directory will recovered files be stored?
5. Which command will show how much space each user is utilizing on a filesystem?
6. How would you find every file on the system that is larger than 3MB?
7. What happens when you delete a log file?

## 5.9 Lab: Working with a Floppy Disk Filesystem

---

This lab emphasizes the difference in a directory when a filesystem is mounted to it.

### 5.9.1 Overview

---

If the floppy filesystem is still mounted, unmount it. Copy `/usr/pub/ascii` to `/mnt` and write down the contents of `/mnt`. Mount a floppy disk filesystem to `/mnt`. Copy `/etc/motd` 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 the following procedure, you will unmount the floppy disk filesystem (if it is mounted), copy a file to `/mnt`, and record the original contents of that directory. Next, you will mount the floppy disk filesystem, copy a different file to `/mnt`, and record the contents. Then, you will unmount the floppy disk filesystem, examine the contents of `/mnt`, and compare the directory listings.

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

```
umount /mnt
```

Step 2. Copy `/usr/pub/ascii` to `/mnt`:

```
cp /usr/pub/ascii /mnt
```

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

```
l /mnt
```

Step 4. Run **scoadmin**(ADM).

Step 5. Select **Filesystems** ⇨ **Filesystem Manager**.

Step 6. Select **Mount** ⇨ **Add Mount Configuration** ⇨ **Local**.

Step 7. Enter `/dev/fd0` for **Device File**, `/mnt` for **Mount Point**, and select **Now** for **When to Mount**.

Step 8. Verify that **At System Startup** is *not* selected for **When to Mount**.

- Step 9.       Select **OK**.
- Step 10.      Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.
- Step 11.      Copy `/etc/motd` to the floppy disk filesystem:
- cp /etc/motd /mnt**
- Step 12.      Obtain a directory listing of `/mnt` and record the output:
- l /mnt**
- Step 13.      Run **scoadmin**(ADM).
- Step 14.      Select **Filesystems** ⇒ **Filesystem Manager**.
- Step 15.      Select the `/dev/fd0` filesystem.
- Step 16.      Select **Unmount**.
- Step 17.      Select **Yes** to verify the operation.
- Step 18.      Select **Host** ⇒ **Exit** to exit the **Filesystem Manager**.
- Step 19.      Obtain a directory listing of `/mnt` and record the output:
- l /mnt**
- Step 20.      Compare the directory listings from Step 3, Step 12, and Step 19.

## 5.10 Relevant Commands, Files, and Syntax

---

The following commands and files were presented in this lesson.

### Relevant commands

---

|                       |                                                                                |
|-----------------------|--------------------------------------------------------------------------------|
| <b>df</b> (C)         | Reports number of free disk blocks                                             |
| <b>du</b> (C)         | Summarizes disk usage                                                          |
| <b>find</b> (C)       | Find files                                                                     |
| <b>fsck</b> (ADM)     | Checks and repairs filesystems                                                 |
| <b>fstyp</b> (ADM)    | Determines filesystem type                                                     |
| <b>fuser</b> (ADM)    | Identify processes using a filesystem or directory                             |
| <b>mount</b> (ADM)    | Mounts a filesystem                                                            |
| <b>quot</b> (ADM)     | Summarizes filesystem ownership                                                |
| <b>scoadmin</b> (ADM) | Invokes SCOadmin applications (in this lesson, the <b>Filesystem Manager</b> ) |
| <b>umount</b> (ADM)   | Unmounts a filesystem                                                          |

### Relevant files

---

|                          |                          |
|--------------------------|--------------------------|
| <i>/etc/wtmp</i>         | Accounts record file     |
| <i>/usr/adm/messages</i> | System messages log file |
| <i>/usr/adm/syslog</i>   | System events log        |

## 5.11 Answers to Review Questions

---

This section provides suggested answers to review questions.

### Review questions

---

1. Before a user can access the files on a filesystem, the filesystem must be mounted.
2. The HTFS, DTFS, EAfs filesystems support long filenames.
3. Three situations that would cause a mount command 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 */u* filesystem, recovered files will be stored in */u/lost+found*.
5. The **quot(ADM)** command shows how much space each user is utilizing on a filesystem.
6. To find every file on the system that is larger than 3MB, enter:  
  
**find / -size +6144 -print**
7. When you delete a log file, you delete the symbolic link to the file. The information is still in the filesystem.



---

# 6

## *Working with Disks and Tapes*

AV 6-1

**Working with Disks and Tapes**

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

sa1-0501

©The Santa Cruz Operation, Inc.

5-1

**Lesson 6**

## **Working with Disks and Tapes**

### **Introduction**

---

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

There are also times when you may want to duplicate one or more directories on another system. If the amount of data is large, it may require a large number of diskettes. An easier way to accomplish this would be to transfer the data by tape.

### **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(C)** and **cpio(C)** commands
- Transfer files to and from a DOS disk

AV 6-2

### **Floppy Disk Device Names**

|                |                |                  |
|----------------|----------------|------------------|
| <b>48ds9</b>   | <b>360 KB</b>  | <b>5.25-inch</b> |
| <b>96ds15</b>  | <b>1.2 MB</b>  | <b>5.25-inch</b> |
| <b>135ds9</b>  | <b>720 KB</b>  | <b>3.5-inch</b>  |
| <b>135ds18</b> | <b>1.44 MB</b> | <b>3.5-inch</b>  |
| <b>135ds36</b> | <b>2.88 MB</b> | <b>3.5-inch</b>  |

#### **Examples:**

**Floppy Disk 0** 3.5-inch 1.44 MB /dev/rfd0**135ds18**  
**Floppy Disk 1** 5.25-inch 1.2 MB /dev/rfd1**96ds15**

sa1-0502

©The Santa Cruz Operation, Inc.

5-2

## 6.1 Working with Floppy Disks

---

To transfer data using floppy disks, follow these guidelines:

- You must know the correct device file to use for a specific floppy disk
- If you receive a floppy disk with data, you must know how the data was transferred to the disk
- If you are going to transfer data to a floppy disk, you must format the disk before using it

### 6.1.1 Identifying floppy device names

---

The standard UNIX data transfer commands use device files. Each type of floppy disk uses a different device file:

|                             |                                             |
|-----------------------------|---------------------------------------------|
| 5¼-inch 1.2MB floppy disks  | <i>/dev/rfd096ds15 or /dev/rfd196ds15</i>   |
| 3½-inch 1.44MB floppy disks | <i>/dev/rfd0135ds18 or /dev/rfd1135ds18</i> |
| 3½-inch 2.88MB floppy disks | <i>/dev/rfd0135ds36 or /dev/rfd1135ds36</i> |

AV 6-3

**Determining the Type of Floppy Disk**

```
# dtype    /dev/rfd0  
  
/dev/rfd0  : tar format
```

sa1-0503

©The Santa Cruz Operation, Inc.

5-3

## 6.1.2 Determining a disk media type

---

Use the **dtype(C)** command to determine what type of data a floppy disk contains:

**dtype** *device\_name*

This command recognizes any of the following data types:

- UNIX filesystems
- DOS diskettes
- **tar(C)** archive
- **cpio(C)** archive
- **backup(ADM)** archive

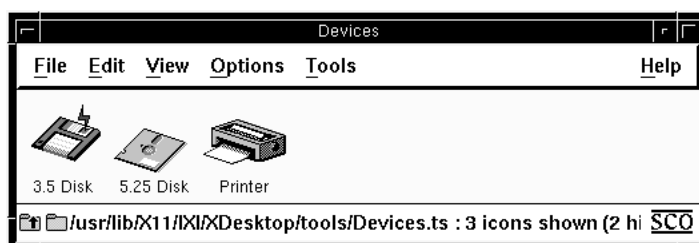
### **Exercise: Examining a floppy disk**

---

Determine the type of data stored on the floppy disk(s) provided by the instructor.

AV 6-4

### **Formatting a Floppy Disk**



sa1-0504

©The Santa Cruz Operation, Inc.

5-4



### 6.1.3 Formatting a floppy disk

---

You must format a new floppy disk before you can use it. The following steps describe how to format a floppy disk from the SCO Desktop:

- Step 1.       Select **Tools** ⇨ **Toolsheds** ⇨ **Devices**.
- Step 2.       Click and hold on the appropriate disk (use the right mouse button if your mouse is configured as a right-hand mouse; use the left mouse button if your mouse is configured as a left-hand mouse).
- Step 3.       Select **Format**.
- Step 4.       Insert the floppy disk when prompted.
- Step 5.       Press  .
- Step 6.       Press  again when complete.

You can also format a floppy disk from the command line using the **format(C)** command. For example, to format a 1.44MB disk in the primary floppy drive, enter:

**format /dev/rfd0135ds18**

#### **Exercise: Formatting a floppy disk**

---

Format a floppy disk. How does **dtype(C)** identify the disk?

AV 6-5

### **Types of Tape Drives**

#### **DEVICE**

**/dev/xct0**

**/dev/erct0**

**/dev/nrct0**

**/dev/rct0**

**/dev/rStp0**

**/dev/rctmini**

**/dev/rft0**

#### **TYPE**

**Cartridge tape controller**

**Error correcting cartridge tape**

**No rewind cartridge tape**

**Cartridge tape**

**SCSI tape**

**Mini cartridge tape**

**QIC 40 floppy tape**

sa1-0505

©The Santa Cruz Operation, Inc.

5-5

## 6.2 Working with Tape Drives

---

To transfer data using tapes, follow these guidelines:

- You must know the correct device file to use for a specific tape drive
- If you receive a tape with data, you must know how the data was transferred to it

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 may need a way to erase the data from tapes.

This section addresses these preparatory steps.

### 6.2.1 Identifying tape device names

---

Before you can use a tape drive, you must know the proper device file to use. The common tape drives and their respective device files are listed below:

|                       |                                                  |
|-----------------------|--------------------------------------------------|
| Cartridge             | <i>/dev/rct0, /dev/nrct0, /dev/xct0</i>          |
| SCSI Cartridge or DAT | <i>/dev/rStp0, /dev/nrStp0, /dev/xStp0</i>       |
| Mini Cartridge        | <i>/dev/rctmini, /dev/nrctmini, /dev/xctmini</i> |

For each type of tape drive, notice the three device files. Each of the three are described below:

|                |                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------|
| <i>/dev/r</i>  | Character device file that rewinds upon closing. This is the most commonly used file.                                     |
| <i>/dev/nr</i> | Character device file that does not rewind upon closing. This is the device used to append data to a tape.                |
| <i>/dev/x</i>  | Control file used by <b>tape(C)</b> . Data cannot be transferred using this file. This file accesses the tape controller. |

## 6.2.2 Working with tapes

---

You can retention, rewind, or erase tapes using the **tape(C)** command. Depending upon the type of tape drive you have, there are also some other options available. To find out which options are available, enter the following command:

### **tape**

You can use the **tape** command with any tape device. The default tape device is stored in */etc/default/tape*.

#### **Exercise: Viewing */etc/default/tape***

---

Determine the default tape drive:

```
more /etc/default/tape
```

Use the **tape** command as follows:

- To retention a tape using the default tape drive, enter:

```
tape reten
```

- To rewind a tape using the default tape drive, enter:

```
tape rewind
```

- To erase a tape using the default tape drive, enter:

```
tape erase
```

- To use a tape drive other than the default, specify the appropriate device file at the end of the command. For example, to retention a tape using a cartridge tape drive, enter:

```
tape reten /dev/rct0
```

## 6.3 Transferring Data to Tape or Disk

---

The two major transfer utilities are **tar**(C) and **cpio**(C). Both commands can copy files and directories. Both 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 by 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, you 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 you archive */usr/pub/ascii*, you can create the archive from within any directory. You can also restore the file from any directory, and the file is placed in */usr/pub*.

You can override absolute pathnames during a restore.

#### 6.3.1.2 Relative pathnames

---

When using relative pathnames, you 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 */usr/pub*. To specify a relative backup, use *./ascii* to designate the file. If you restore the file while in the */tmp* directory, the file *ascii* is restored in */tmp*.

### 6.3.2 Transferring symbolically linked files

---

SCO OpenServer systems use a large number of symbolic links in the root filesystem. When backing up an entire filesystem, this does not affect the procedure. However, consider the following when backing up a single directory containing symbolic links:

- If you just back up the directory containing the link, the default behavior is to back up the link only, not the data
- With both **cpio**(C) and **tar**(C), 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 6-6

**/etc/default/tar**

| #         | DEVICE           | BLOCK | SIZE | TAPE |
|-----------|------------------|-------|------|------|
| archive0= | /dev/rfd048ds9   | 18    | 360  | n    |
| archive1= | /dev/rfd148ds9   | 18    | 360  | n    |
| archive2= | /dev/rfd096ds15  | 10    | 1200 | n    |
| :         |                  |       |      |      |
| :         |                  |       |      |      |
| archive6= | /dev/rfd0135ds18 | 18    | 1440 | n    |
| :         |                  |       |      |      |
| :         |                  |       |      |      |
| archive8= | /dev/rStp0       | 20    | 0    | y    |
| :         |                  |       |      |      |
| :         |                  |       |      |      |
| archive=  | /dev/rfd0135ds18 | 18    | 1440 | n    |

← **DEFAULT tar DEVICE**

sa1-0508                      ©The Santa Cruz Operation, Inc.                      5-8



### 6.3.3 The tar(C) command

---

The **tar**(C) command can archive only subdirectories that are within 17 levels of subnesting.

This command has the following advantages:

- 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 was created using absolute pathnames.

This command also has the following limitations:

- It cannot be used to transfer special device files or empty directories
- It does not support filename expansion for extracting data
- Data archives created with **tar**(C) may be difficult to transfer to computer platforms other than SCO OpenServer systems

Use **tar** unless you must transfer special device files or empty directories.

The default device used by **tar** is specified in */etc/default/tar*. This file also contains references to other devices **tar** can access. For example, **archive8** points to the primary SCSI tape drive.

#### **Exercise: Modifying the default tar(C) device**

---

Edit */etc/default/tar* so that the default device is the tape drive in your system.

AV 6-7

**tar(C) Options**

| OPTION   | DESCRIPTION                                          |
|----------|------------------------------------------------------|
| <b>v</b> | <b>Verbose (display output)</b>                      |
| <b>L</b> | <b>Follow symbolic links</b>                         |
| <b>c</b> | <b>Create archive</b>                                |
| <b>r</b> | <b>Append to archive</b>                             |
| <b>t</b> | <b>Table of contents</b>                             |
| <b>x</b> | <b>Extract from archive</b>                          |
| <b>#</b> | <b>Archive device in<br/><i>/etc/default/tar</i></b> |

sa1-0507

©The Santa Cruz Operation, Inc.

5-7

### 6.3.3.1 Copying data

---

Listed below are several examples of creating archives using **tar(C)**:

- Create an archive of */usr/pub* using absolute pathnames. Store the archive on the default device:

```
tar cv /usr/pub
```

- Create an archive of */usr/pub* using relative pathnames. Store the archive on the primary floppy disk, identified as *archive6* in */etc/default/tar*:

```
cd /usr/pub
```

```
tar cv6 ./*
```

- Create an archive of */usr/pub*. Store the archive in */tmp/tarfile*:

```
tar cvf /tmp/tarfile /usr/pub
```

- Using relative pathnames, append the data in */etc/motd*, a symbolically linked file, to the archive on the floppy disk:

```
cd /etc
```

```
tar rvL6 ./motd
```

### 6.3.3.2 Viewing the contents of a tar(C) 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(C) archive

---

Listed below are several examples of extracting data from a **tar(C)** archive.

- Restore the entire archive from the primary floppy disk to */tmp*:

```
cd /tmp
```

```
tar xv6
```

- Restore just *./motd* from the primary floppy disk to */usr/pub*:

```
cd /usr/pub
```

```
tar xv6 ./motd
```

- Restore */usr/pub/ascii* from */tmp/tarfile*. Override the absolute pathname and restore it to */tmp*:

```
cd /tmp
```

```
tar xvAf /tmp/tarfile usr/pub/ascii
```

AV 6-8

### **cpio(C) Options**

#### **Creating an Archive: (vocBL)**

|          |                                                                |
|----------|----------------------------------------------------------------|
| <b>v</b> | <b>Verbose</b>                                                 |
| <b>o</b> | <b>Write archive out</b>                                       |
| <b>c</b> | <b>ASCII header (for moving to different types of systems)</b> |
| <b>B</b> | <b>Blocking factor set to 5KB</b>                              |
| <b>L</b> | <b>Follow symbolic links</b>                                   |

#### **Extracting an Archive (vicdumB)**

|          |                                           |
|----------|-------------------------------------------|
| <b>v</b> | <b>Verbose</b>                            |
| <b>i</b> | <b>Read archive in</b>                    |
| <b>c</b> | <b>ASCII header</b>                       |
| <b>d</b> | <b>Create directories as required</b>     |
| <b>u</b> | <b>Copy unconditionally</b>               |
| <b>m</b> | <b>Retain previous modification times</b> |
| <b>B</b> | <b>Blocking factor set to 5 KB</b>        |

sa1-0508

©The Santa Cruz Operation, Inc.

5-8

### 6.3.4 The **cpio(C)** command

---

The **cpio(C)** command has the following advantages:

- It copies device files and empty directories
- 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 was created using absolute pathnames.

#### 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(C)** command. Use **find -depth** so that **cpio** restores files located in write protected directories.

Listed below are several examples of creating archives with **cpio**:

- Create an archive of the current directory. Store the archive on the primary floppy drive:

```
find . -depth -print | cpio -vocBL -O /dev/rfd0
```

- Create an archive of */usr/pub* using absolute pathnames. Store the archive on the primary floppy drive:

```
find /usr/pub -depth -print | cpio -vocBL -O /dev/rfd0
```

- Create an archive of the */u* filesystem. Store the archive on tape:

```
cd /u
```

```
find . -depth -mount -print | cpio -vocBL -O /dev/rct0
```

### 6.3.4.2 Viewing the contents of a cpio file

---

Use the following command to display a table of contents for a **cpio(C)** archive:

```
cpio -Bitcv -I/dev/device_name
```

For example, use the following command to display the contents of a **cpio** archive on the primary tape drive:

```
cpio -Bitcv -I/dev/rct0
```



### 6.3.4.3 Extracting data from a cpio file

---

Listed below are examples of extracting files from a **cpio** archive:

- To extract all files from an archive created with absolute pathnames, enter:

```
cpio -vicdumB -I /dev/rfd0
```

- To extract a single file archived with a relative pathname, enter:

```
cd /usr/pub
```

```
cpio -vicdumB -I /dev/rfd0 ascii
```

AV 6-9

**/etc/default/msdos**

**A = /dev/install  
B = /dev/install1  
C = /dev/hd0d  
D = /dev/hd1d  
X = /dev/install  
Y = /dev/install1**

sa1-0509

©The Santa Cruz Operation, Inc.

5-9

## 6.4 Transferring Data to and from a DOS Disk

---

SCO OpenServer systems also provide a variety of commands that allow you to manipulate files on DOS diskettes without mounting the disks. If you are performing a few quick tasks on the disk, you may find these commands quicker to use than mounting the disk or running DOS Services.

### 6.4.1 DOS disk designations

---

You can use these DOS utilities by either specifying the UNIX device file or standard DOS disk designations. You can find the DOS disk designations defined in */etc/default/msdos*.

#### **Exercise: Viewing DOS disk designations**

---

View */etc/default/msdos*. Note that the primary floppy disk is identified as the A drive.

### 6.4.2 DOS utilities

---

Listed below are the various DOS utilities and their functions.

|                  |                                                            |
|------------------|------------------------------------------------------------|
| <b>doscatt</b>   | List the contents of a DOS file                            |
| <b>doscp</b>     | Copy a file to or from a DOS disk                          |
| <b>dosdir</b>    | List DOS directories in the DOS <b>DIR</b> style           |
| <b>dosformat</b> | Format a DOS floppy                                        |
| <b>dosls</b>     | List DOS directories in the UNIX system <b>ls(C)</b> style |
| <b>dosmkdir</b>  | Make a directory on a DOS disk                             |
| <b>dosrm</b>     | Remove files from a DOS disk                               |
| <b>dosrmdir</b>  | Remove directories from a DOS disk                         |

Refer to the **doscmd(C)** manual page for additional information.

### **Exercise: Copying a file to a DOS diskette**

---

Copy **/etc/motd** to a DOS diskette in the primary floppy disk drive:

**doscp /etc/motd a:**

Confirm that the file has been copied:

**dosdir a:**

### **6.4.3 Copying data to DOS filesystems**

---

SCO OpenServer systems enable you to integrate DOS applications and files. Although DOS filesystems have a different structure than UNIX filesystems, you can mount them to the UNIX directory structure as with any other UNIX filesystem. This provides two main benefits:

- You can copy, move, rename, and delete files using the same commands as for UNIX files, eliminating the need to learn special commands
- You can back up the files in the DOS filesystems using the same tools used to back up UNIX filesystems

Listed below are two types of DOS filesystems and their respective device files:

- Existing DOS partitions on a hard disk—**/dev/hd0d**
- DOS formatted floppy disks—**/dev/fd0**

Mounting and unmounting DOS filesystems is the same as for UNIX filesystems.

There are two restrictions to using mounted DOS filesystems:

- You cannot execute DOS files and applications from a mounted DOS filesystem; to do this, you must run SCO Merge or boot DOS off the DOS partition
- You cannot use DOS utilities on a mounted DOS filesystem

**Exercise: Using a DOS filesystem**

---

Mount a DOS floppy filesystem to */mnt*. Copy */etc/motd* to the DOS floppy.

## 6.5 Lesson Summary

---

---

SCO OpenServer 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 device name for a 3.5-inch, 720KB diskette drive if it is the second diskette drive in the system?
2. What type of tape device is `/dev/rStp0`?
3. What happens if you use the **L** option with the **tar(C)** command?
4. What are the benefits to mounting a DOS filesystem?

## 6.6 Lab: Creating an Archive and Extracting Selected Files

---

In this lab, you use the **cpio(C)** and **tar(C)** commands to create archives and extract selected files from them.

### 6.6.1 Overview

---

Create a relative backup of the */usr/pub* directory to either tape or disk. Rename */usr/pub/ascii*, then restore */usr/pub/ascii* from the archive.

Create a backup of the */dev* directory. Rename */dev/tty05*, then restore */dev/tty05* from the archive.

### 6.6.2 Procedure

---

The following steps describe how to create an archive and extract selected files:

Step 1. Move to the */usr/pub* directory:

```
cd /usr/pub
```

Step 2. Use the **tar(C)** command to create a relative backup of the directory:

- For a floppy disk, enter:

```
tar cvf /dev/rfd0 ./*
```

- For a cartridge tape, enter:

```
tar cvf /dev/rct0 ./*
```

Step 3. Rename */usr/pub/ascii*:

```
mv ascii ascii.bak
```

Step 4. View the **tar(C)** archive:

- For a floppy disk, enter:

```
tar tvf /dev/rfd0
```

- For a cartridge tape, enter:

```
tar tvf /dev/rct0
```

Step 5. Use the **tar(C)** command to extract */usr/pub/ascii*:

- From a floppy disk, enter:

```
tar xvf /dev/rfd0 ./ascii
```

- From a cartridge tape, enter:

```
tar xvf /dev/rct0 ./ascii
```

Step 6. Move back to the root (/) directory.

```
cd /
```

Step 7. Using **cpio(C)**, create an archive of the */dev* directory:

- For a disk, enter:

```
find /dev -depth -print | cpio -ov -0 /dev/rfd0
```

- For a tape, enter:

```
find /dev -depth -print | cpio -ov -0 /dev/rct0
```

Step 8. Disable and rename */dev/tty05*:

```
disable tty05
```

```
mv /dev/tty05 /dev/tty05.bak
```

Step 9. View the **cpio(C)** archive:

- For a disk, enter:

```
cpio -Bitvc -I /dev/rfd0
```

- For a tape, enter:

```
cpio -Bitvc -I /dev/rct0
```



Step 10. Using **cpio**(C), restore */dev/tty05*:

- From a disk, enter:

```
cpio -ivmu /dev/tty05 -I /dev/rfd0
```

- From tape, enter:

```
cpio -ivmu /dev/tty05 -I /dev/rct0
```

## 6.7 Relevant Commands and Files

---

The following commands and files were presented in this lesson.

### Relevant commands

---

|                 |                                         |
|-----------------|-----------------------------------------|
| <b>cpio(C)</b>  | Copies archives                         |
| <b>doscp</b>    | Copies a file to a DOS diskette         |
| <b>dosdir</b>   | Displays the contents of a DOS diskette |
| <b>dtype(C)</b> | Determines the format of data           |
| <b>find(C)</b>  | Locates files                           |
| <b>tape(C)</b>  | Maintains tapes                         |
| <b>tar(C)</b>   | Copies archives                         |

### Relevant files

---

|                           |                                         |
|---------------------------|-----------------------------------------|
| <i>/etc/default/msdos</i> | DOS command configuration file          |
| <i>/etc/default/tape</i>  | Default <b>tape(C)</b> device           |
| <i>/etc/default/tar</i>   | <b>tar(C)</b> device configuration file |

## 6.8 Answers to Exercises and Review Questions

---

This section provides suggested answers to the exercises and review questions.

### Exercise: Formatting a floppy disk

---

The command **dtype(C)** identifies the newly formatted disk as *unrecognized data*.

### Exercise: Scheduling an unattended backup

---

The **cron(C)** entry would be as follows:

```
30 17 * * 2,4 /usr/lib/sysadmin/cbackup 0 150000 /dev/rct0 \  
/dev/boot
```

### Review questions

---

1. The device name for a 3.5-inch, 720KB diskette drive, if it is the second diskette drive in the system, is */dev/rfd1135ds9*.
2. The tape device */dev/rStp0* is the first SCSI tape drive in the system. Using this device will cause the drive to rewind the tape upon completion of the task.
3. The **tar(C)** command will back up the actual data associated with a symbolic link if the **L** option is used.
4. Mounting a DOS filesystem has the following benefits: you can copy, move, rename, and delete files using the same commands as for UNIX files, eliminating the need to learn special commands; you can back up the files in the DOS filesystems using the same tools used to back up UNIX filesystems.



---

# 7

## *Filesystem Backups*

AV 7-1

### **Filesystem Backups**

- **Organize and maintain filesystem backups**
- **Manage backup schedules**
- **Back up filesystems**
- **Schedule unattended backups**
- **Verify a filesystem backup**
- **Restore files**
- **Restore non-root filesystems**

sa1-0601

©The Santa Cruz Operation, Inc.

6-1

**Lesson 7**

## **Filesystem Backups**

### **Introduction**

---

The most expensive component of any system is the data stored on it. Unlike hardware, lost data is often irreplaceable. To protect this business critical information, routine backups are essential. Maintaining systematic backups and restoring lost data is an important and common task for system administrators.

### **Objectives**

---

This lesson shows how to maintain backups that enable the restoration of a filesystem or critical files. By the end of this lesson, you will be able to:

- Organize and maintain filesystem backups
- Manage backup schedules
- Back up filesystems
- Schedule unattended backups
- Verify a filesystem backup
- Restore files
- Restore non-root filesystems

## 7.1 Organizing and Maintaining Filesystem Backups

---

Filesystem backups are a copy of one or more filesystems saved on tape or diskette. Files and filesystems can become damaged, resulting in data loss. Maintaining backups give you the best chance of recovering data. Sometimes you may want to restore an older version of a file, so you should retain more than the most current backup. To restore the correct data, you must keep accurate records of the backups you create. This section addresses some of the basic administrative details associated with maintaining good system backups.

### 7.1.1 Using different backup levels

---

Although there are a large number of user files that change on a daily basis, programs and most system files tend to remain static. One way to save tape space and time spent performing backups is to use incremental backups. The **Backup Manager** supports three levels of backups:

|         |                                                                                  |
|---------|----------------------------------------------------------------------------------|
| Level 0 | Backs up every file in the filesystem                                            |
| Level 1 | Backs up every file created or modified since the last level 0 backup            |
| Level 2 | Backs up every file created or modified since the last level 1 or level 0 backup |

### 7.1.2 Using a backup schedule

---

The best protection against data loss is a systematic backup routine. The **Backup Manager** allows you to create a schedule in which you designate how often the system should perform each backup level. For example, you can choose to perform a level 0 backup every two weeks. You may then decide to perform a level 1 backup weekly and a level 2 backup daily. A backup schedule provides the following benefits:

- Backups take as little time as possible
- Files that change regularly are backed up on a daily basis while more static information is backed up less often
- Lost files can be recovered as quickly as possible



### 7.1.3 Deciding when to back up filesystems

---

Back up a filesystem when the fewest number of users are logged into the system. This provides the following benefits:

- The backup does not affect system performance during peak times of system use
- You have a better chance of avoiding problems caused by backing up the system while users are modifying files. In fact, you may want to bring the system down to single-user mode while performing a complete system backup.

### 7.1.4 Storing backup media

---

After creating your backups, store them in a secure, fireproof place so that you can use them to restore your data in the event of a hardware failure or other system problem that causes data loss. Consider archiving older tapes off-site for additional protection against any disaster that could destroy the building, such as fire.

**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, you should label the backups with the following type of information:

- System name
- Filesystem name
- Backup date
- Who performed the backup
- Backup method—list what utility was used to create the backup
- Specify the sequence on the volumes if the backup required multiple volumes. For example, specify “1 of 3” to identify the first tape of a backup that required 3 tapes.
- Backup level
- Rotation date—the date that the tape can be reused

## 7.1.5 Maintaining backup logs

---

Maintaining a written backup log book for each computer also helps you to keep your backups organized. Your system maintains a backup history for scheduled backups; however, if the online history is unavailable, you can use the written records to construct a backup set from which to restore the system.

For each backup of the system, record the following:

- Filesystem name
- Backup date
- Who performed the backup
- Number of volumes required for the backup
- Backup level
- Any problems that occurred during the backup

## **7.2 Managing Backup Schedules**

---

---

A backup schedule helps you to perform systematic, routine backups. This section describes how to maintain backup schedules.

AV 7-2

### Adding a Backup Schedule

Add Filesystem Backup Schedule on lab1

Backup Schedule for lab1 /dev/root Filesystem

Perform Complete backup every  days

Select days to perform Incremental backups:

|                                           |           |
|-------------------------------------------|-----------|
| <input checked="" type="checkbox"/> Day 1 | Complete  |
| <input type="checkbox"/> Day 2            | No Backup |
| <input type="checkbox"/> Day 3            | No Backup |
| <input type="checkbox"/> Day 4            | No Backup |
| <input type="checkbox"/> Day 5            | No Backup |
| <input type="checkbox"/> Day 6            | No Backup |
| <input type="checkbox"/> Day 7            | No Backup |

Incremental Backup Types:

Level 1 (files changed since last Complete backup)

Level 2 (files changed since last Incremental backup)

Today is Day

[Backup Options...](#)

OK Cancel Help

sa1-0602

©The Santa Cruz Operation, Inc.

6-2

---

### 7.2.1 Creating or modifying a schedule

---

The following steps describe how to create a backup schedule:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select the desired filesystem.
- Step 4. Do one of the following:
  - Select **Schedule** ⇒ **Add Filesystem Schedule** if there is no existing schedule
  - Select **Schedule** ⇒ **Modify Filesystem Schedule** if a schedule exists
- Step 5. Enter how often the system should perform a complete backup (level 0). The maximum interval is 35 days.
- Step 6. Click on a day in the **Select days to perform incremental backups** list until you see the desired backup option. You see a list showing all of the days between complete backups.
- Step 7. Enter **1** in the **Today is Day** field to begin your backup cycle with a complete backup of the filesystem.
- Step 8. Select **Backup Options**. Select the desired option for whether or not the filesystem should be mounted.
- Step 9. Select **Save Backup Contents Lists** to maintain a history of all scheduled backups. This history includes:
  - The filesystem name
  - The names of all files and directories backed up
  - The backup date
  - The backup level
- Step 10. Select **OK** to leave the options menu.
- Step 11. Select **OK** to save the schedule.
- Step 12. Select **Host** ⇒ **Exit** to exit the **Backup Manager**.

### **Exercise: Creating a backup schedule for the boot (/stand) filesystem**

Create a backup schedule for the boot filesystem. Assume Monday is day 1. Perform a complete backup each Monday and a level 1 backup every Tuesday through Friday. Do not perform a backup on Saturday or Sunday. Select **Save Backup Contents Lists**.

## **7.2.2 Deleting a Schedule**

---

The following steps describe how to delete an existing filesystem schedule:

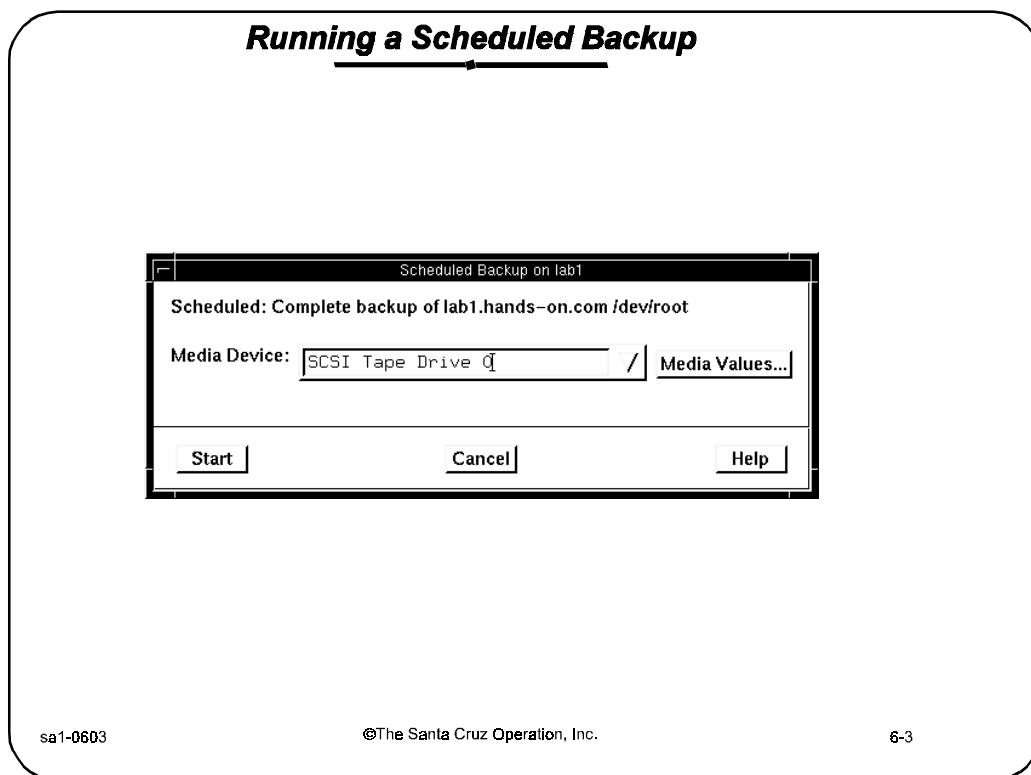
- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select the **Backup Manager**.
- Step 3. Select the desired filesystem.
- Step 4. Select **Schedule** ⇒ **Delete Filesystem Schedule**.
- Step 5. Select **OK** to delete the schedule when prompted.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Backup Manager**.

## **7.3 Backing up a Filesystem**

---

Even though a backup schedule has been created, you must still perform the backups. The schedule does not mean that the backup occurs automatically; it specifies what type of backup should run on any given day.

AV 7-3





### 7.3.1 Running a scheduled backup

---

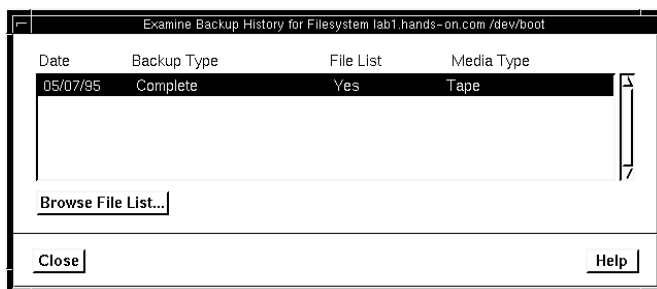
The following steps describe how to run a scheduled backup:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select the desired filesystem.
- Step 4. Select **Backup** ⇒ **Run Scheduled**.  
  
The system displays the default backup media device.
- Step 5. Select the appropriate device if you are using a media device other than the default.
- Step 6. Select on **Media Values** to set the block and volume size for the media.
- Step 7. Select **Start**.
- Step 8. Insert the appropriate media into the media device when prompted.
- Step 9. Select **OK** to begin the backup. If the backup requires more than one disk or tape, insert the next disk or tape when prompted and Select **OK**.  
  
When complete, the system prompts you to verify the backup. If you select **Yes**, the system prompts you to insert the disks.
- Step 10. Select **OK** when complete.
- Step 11. Select **Host** ⇒ **Exit** to exit the **Backup Manager**.

If you skip a scheduled backup, the **Backup Manager** performs the highest level backup that is due to run.

AV 7-4

### **Examining a Backup History**



sa1-0804

©The Santa Cruz Operation, Inc.

8-4

### 7.3.2 Examining the backup history

---

If you are using incremental backups, you may not know when a file was last archived. It may exist on one or more level 1 or level 2 backups. If you chose to maintain a backup history, you can browse through these online logs to locate a particular file.

The following steps describe how to examine the backup history:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select the desired filesystem.
- Step 4. Select **Examine** ⇨ **Backup History**.

A screen displays all of the backups with the backup date, backup level, whether or not a file list exists, and the backup media type.

- Step 5. Select a backup and select **Browse File List**.

You can see all of the files and directories that are on that backup. You can also search for a specific file.

- Step 6. Select **Close** to exit the file list.
- Step 7. Select **Close** to exit the backup history.
- Step 8. Select **Host** ⇨ **Exit** to exit the **Backup Manager**.

#### **Exercise: Backing up the boot filesystem**

---

Perform a scheduled backup of the boot filesystem. Start the backup without the media inserted. What error message do you get? Insert the media and perform the backup. Once the backup is complete, view the backup history for this filesystem.

### 7.3.3 Running an unscheduled backup

---

There are times when you may want to run an unscheduled, complete backup of a filesystem. Whenever you are going to make major changes to the system, you should back it up completely in case problems occur that result in data loss. Some examples of such changes include the following:

- Adding any hardware to the system
- Changing the size of a filesystem or partition
- Reorganizing filesystems

The following steps describe how to run an unscheduled backup:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select the desired filesystem.
- Step 4. Select **Backup** ⇒ **Run Unscheduled** ⇒ **Selected Filesystem**.
- Step 5. Select the appropriate device if you are using a media device other than the default.
- Step 6. Select on **Media Values** to set the block and volume size for the media.
- Step 7. Enter the starting directory (if desired) in the **From Directory** field.
- Step 8. Select **Start**.
- Step 9. Insert the appropriate media into the media device when prompted.
- Step 10. Select **OK** to begin the backup. If the backup requires more than one disk, insert the next disk when prompted and Select **OK**.
- Step 11. Select **Yes** when prompted to verify the backup.
- Step 12. Insert Volume 1 when prompted and select **OK**. Do the same if prompted for additional volumes.
- Step 13. Select **OK** when verification is complete.
- Step 14. Select **OK** again after you receive the message that the backup is complete.

Step 15. Select **Host** ⇒ **Exit** to exit the **Backup Manager**.

The backup history contains only the logs for scheduled backups. If you want to examine the contents of a specific tape, perform the following steps:

Step 1. Run **scoadmin**(ADM).

Step 2. Select the **Backup Manager**.

Step 3. Select **Examine** ⇒ **Media Contents**.

Step 4. Select the appropriate media device.

Step 5. Select **Start**. After reading the first volume of the backup, the system displays a list of files and directories that are on that backup. You can also search for a specific file.

Step 6. Select **Close** to exit the backup history.

Step 7. Select **Close** to exit the file list.

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

### **Exercise: Backing up the */etc/default* directory**

---

Perform an unscheduled backup of */etc/default* on the *root* filesystem. Verify the backup, then view its contents.

## 7.4 Scheduling an Unattended Backup

---

You can schedule automatic backups that occur during hours of low system use without requiring that someone be present. This provides several advantages:

- As long as there is a tape in the drive, a backup occurs. You do not have to worry about forgetting to back up the system.
- Since you can schedule the backup to occur during hours of low system use, the backup does not have to impact system performance when there are many users on the system
- Since the backup occurs automatically, someone does not have to spend the time monitoring the backup

Observe the following cautions when using unattended backups:

- For an unattended backup to succeed, a single day's backup must fit on a single tape
- Be careful to replace the tape each day, or the automatic backup overwrites the previous day's archive. This means that you will not have any previous versions of the backup; and if there is a disaster that destroys the system, it can also destroy your backup.
- The filesystem must be mounted before the backup occurs
- Only the **root** account can back up *all* files with the **cbackup**(ADM) command

Unattended backups are created using **cbackup**, which does the following:

- Bypasses the backup schedule for a particular filesystem
- Uses the **cpio**(C) command to create the backup
- Supports incremental backup levels

The syntax for **cbackup** is:

**/usr/lib/sysadmin/cbackup level vol\_size device filesystem**

Volume size is expressed in KB. For example, to create a complete (level 0) backup of the /u filesystem on a 150MB cartridge tape, you would use the following command:

**/usr/lib/sysadmin/cbackup 0 150000 /dev/rct0 /dev/u**

Use the **cron**(C) command to run the backup at specified times.

Refer to *SCO OpenServer System Administration Guide*, “Performing unattended backups.”

### **Exercise: Scheduling an unattended backup**

---

Before creating a **cron** job, you should always test the command first to make sure the syntax is correct.

Using the **cbackup**(ADM) command, perform a level 0 backup of the boot (*/dev/boot*) filesystem.

If this executes correctly, log in as the user **backup** and submit a **cron**(C) request to run this level 0 backup every Tuesday and Thursday at 5:30 p.m. Be careful that you do not overwrite any existing cron requests for this user. Refer to Lesson 3 for instructions on submitting a **cron** request.

## 7.5 Verifying a Filesystem Backup

---

You should verify the backups to ensure that the system can read the backup. Otherwise, you might not find out about a problem until you are unable to recover data from a particular backup. At the very least, periodically verify a backup upon completion and assume the others are also valid.

The following steps describe how to verify a backup:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select **Backup** ⇨ **Verification**.
- Step 4. Select the appropriate device if you are using a media device other than the default.
- Step 5. Insert the first volume when prompted and select **OK**. Do the same if prompted for additional volumes.  
  
The verification displays discrepancies (if any) or a message that the backup is OK.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇨ **Exit** to exit the **Backup Manager**.

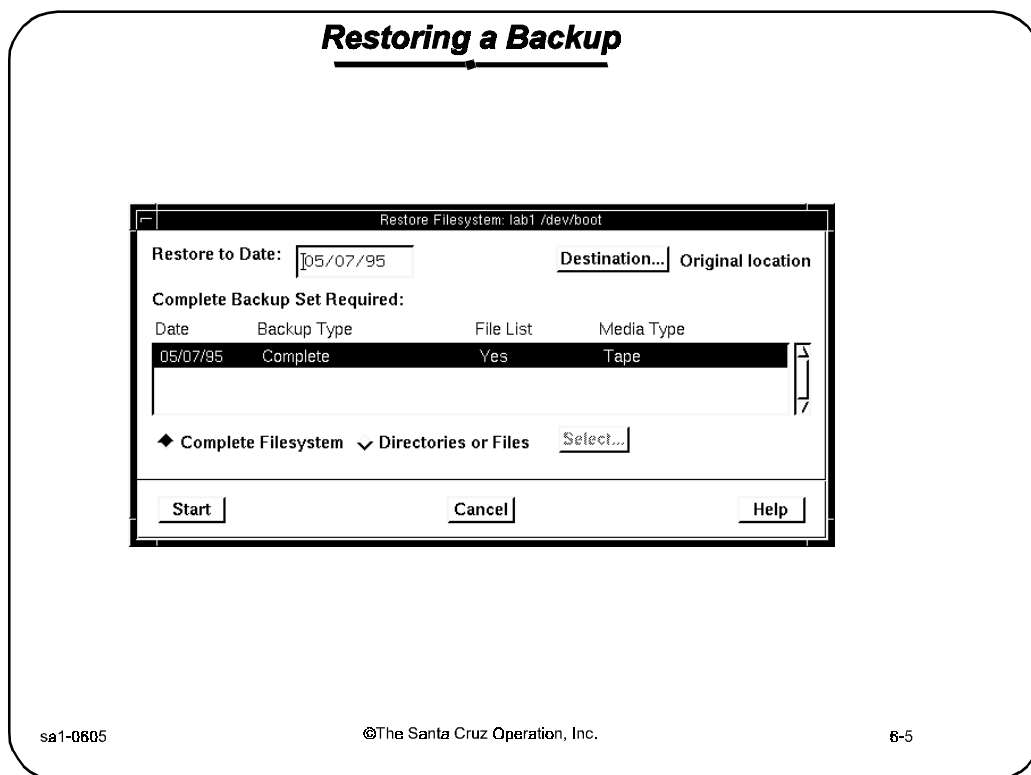


**Exercise: Verifying the last backup of the boot filesystem**

---

Verify the backup created with the **cbackup**(ADM) command.

AV 7-5



## 7.6 Restoring Selected Files

---

There are times when you need to restore only a few files from a specific backup. A file may have been accidentally erased or corrupted. Restoring the entire filesystem would overwrite some current files, so you want to select the files to be restored. The **Backup Manager** allows you to select the files to be restored and designate where to restore them.

The following steps describe how to restore selected files from a backup:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select **Restore** ⇨ **From Backup History** to restore files from a scheduled backup. Select **Restore** ⇨ **From Current Media** to restore from an unscheduled backup.
- Step 4. Select the appropriate media device.
- Step 5. Do one of the following:
  - **Select Specified Files** if you want to type in a short list of files to restore.
  - **Select Files Selected from Media List** to select the files from a list
- Step 6. Insert the first volume of the backup when prompted.
- Step 7. Select **OK**. A list of files appears.
- Step 8. Select the files you want to restore and select **Add**. The selected files appear in a list at the bottom of the window. If you want to remove a file from the selected list, highlight the file and select **Remove**. You also can search for specific files.
- Step 9. Select **OK** when you have completed the list of files to restore.
- Step 10. Specify the destination directory. If you want to restore files to their original directories, specify the root (/) directory.
- Step 11. Select **Start**. You can then verify the file list by selecting **View Selected Files**.
- Step 12. Verify the list and select **OK** to start the restoration.
- Step 13. Insert the first volume of the backup when prompted and select **OK**.

The system sequentially restores the files, and prompts you for other backup volumes, if necessary.

Step 14. Select **OK** when the restore is complete.

Step 15. Select **Host** ⇒ **Exit** to exit the **Backup Manager**.

### **Exercise: Restoring /etc/default/tar**

---

Restore */etc/default/tar* from the unscheduled backup of the directory */etc/default*.

Next, restore */unix* to the directory */tmp* from the backup of the *boot* filesystem.

## 7.7 Restoring a Non-root Filesystem

---

Although unlikely, sometimes a filesystem becomes so damaged that a complete restoration is required. Or, you may have added a new hard disk and have to move the filesystem to it. In either case, you must restore the entire filesystem.

The following steps describe how to restore a full filesystem:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Do one of the following:
  - Select **Restore** ⇨ **From Backup History** to restore files from a scheduled backup
  - Select **Restore** ⇨ **From Current Media** to restore from an unscheduled backup
- Step 4. Specify the appropriate media type.
- Step 5. Select **Complete Contents of Media** and designate the root (/) directory as the destination directory.
- Step 6. Select **Start**. A verification message appears.
- Step 7. Select **OK**.
- Step 8. Insert the first volume of the backup when prompted and select **OK**.  
  
The system restores the files and prompts you for other backup volumes, if necessary.
- Step 9. Select **OK** when the restore is complete.
- Step 10. Select **Host** ⇨ **Exit** to exit the **Backup Manager**.

## 7.8 Lesson Summary

---

---

Creating system backups is the only way to recover your system in case of either hardware failure or accidental loss of data. SCO OpenServer systems provide a backup tool that allows you to create complete as well as incremental backups. These backups allow you to restore either entire filesystems or selected files.

### Review questions

---

1. Why should you store backup tapes off-site from the location of the system?
2. How does saving the "Backup Contents Lists" benefit you?
3. Two days of scheduled backups were skipped, a level 1 and a level 2. Today's backup is a level 0. Which level backup will run today if you perform a scheduled backup?
4. What would be the **cbackup**(ADM) command to perform a level 1 backup of the root filesystem using the primary 250MB cartridge tape?
5. How often should you verify a backup?
6. List the steps to restore a single file from a scheduled backup.
7. List the steps to restore a complete non-root filesystem.

## 7.9 Lab: Creating a Default Backup Schedule

---

Create a backup schedule to back up the `/u` filesystem regularly.

### 7.9.1 Overview

---

Create a default backup schedule for the `/u` filesystem. Perform a complete backup every 14 days, a level 1 backup on days 2 and 8, and a level 2 backup on all other days. Make sure that you save the backup content lists.

### 7.9.2 Procedure

---

The following steps describe how to create a backup schedule to back up the `/u` filesystem regularly:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select the **Backup Manager**.
- Step 3. Select the `/u` filesystem.
- Step 4. Select **Schedule** ⇒ **Add Filesystem Schedule**.
- Step 5. Set **Perform Complete Backup** to 14 days.
- Step 6. Select once on **Day 2** and **Day 8** to perform a Level 1 Incremental backup.
- Step 7. Select twice on **Days 3-7** and **Days 9-14** to perform a Level 2 Incremental backup.
- Step 8. Select on **Backup Options**.
- Step 9. Select **Always Mount Filesystems** and **Save Backup Contents Lists**.
- Step 10. Select **OK** to close the “Backup Options” dialog box.
- Step 11. Select **OK** to save the backup schedule. Do not exit **Backup Manager**.

Given the above schedule, if the system were to crash on the morning following the Day 10 backup, from which backups would you have to restore to completely recover the system?

## 7.10 Lab: Backing up and restoring a filesystem

---

Run a scheduled backup of the `/u` filesystem. Restore the entire filesystem.

### 7.10.1 Overview

---

Verify that the default media device is the tape drive. Perform a scheduled backup of the `/u` filesystem.

### 7.10.2 Procedure

---

The following steps describe how to run a scheduled backup of the `/u` filesystem, then restore the entire filesystem:

- Step 1.       Select **Options** ⇨ **Set Default Device**.
- Step 2.       Set **Media Device** to **Tape**.
- Step 3.       Select the `/u` filesystem.
- Step 4.       Select **Backup** ⇨ **Run Scheduled**.
- Step 5.       Verify the Media Device and select **Start**.
- Step 6.       Select **Restore** ⇨ **From Backup History**.
- Step 7.       Specify the appropriate media type.
- Step 8.       Select **Complete Contents of Media** and designate `/u` as the destination directory.
- Step 9.       Start the restore process. Insert media as prompted.



## 7.11 Relevant Commands

---

The following commands were presented in this lesson.

|                       |                                                                            |
|-----------------------|----------------------------------------------------------------------------|
| <b>cbackup</b> (ADM)  | Performs unattended incremental backups                                    |
| <b>cron</b> (C)       | Executes scheduled commands                                                |
| <b>crontab</b> (C)    | Schedules <b>cron</b> (C) jobs                                             |
| <b>scoadmin</b> (ADM) | Invokes SCOadmin applications (in this lesson, the <b>Backup Manager</b> ) |

## 7.12 Answers to Exercises and Review Questions

---

This section provides suggested answers to the exercises and review questions.

### 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(C)** 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(C)** 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(C)** 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 the following 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, 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 would want to limit access to a printer when you want to reserve that printer for a highly specialized activity, such as printing forms or production-quality materials.
6. Check any of the following 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

## *Managing Printers*

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**

sa1-0701

©The Santa Cruz Operation, Inc.

7-1

**Lesson 8**

## **Managing Printers**

### **Introduction**

---

After data transfer, printing is one of the most common functions that users perform. Maintaining printers, print services, and print queues enables your users to 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 8-2

### **Checking Printer Status**

```
$ lpstat -t
```

```
scheduler is running  
system default destination: laser1  
device for laser1: /dev/lp0  
laser1 accepting requests since Fri Jan 13 17:22:45 1995  
printer laser1 is idle. enabled since Fri Jan 13 17:22:45 1995  
available.
```

sa1-0702

©The Santa Cruz Operation, Inc.

7-2



## 8.1 Managing the Print Service

---

You control print services through the **Printer Manager**, which is located in the **Printers** folder in **scoadmin**(ADM). The **Printer Manager** allows you to control the operation and configuration of specific printers and printer classes.

### 8.1.1 Defining the print service

---

The print service is responsible for performing the following tasks:

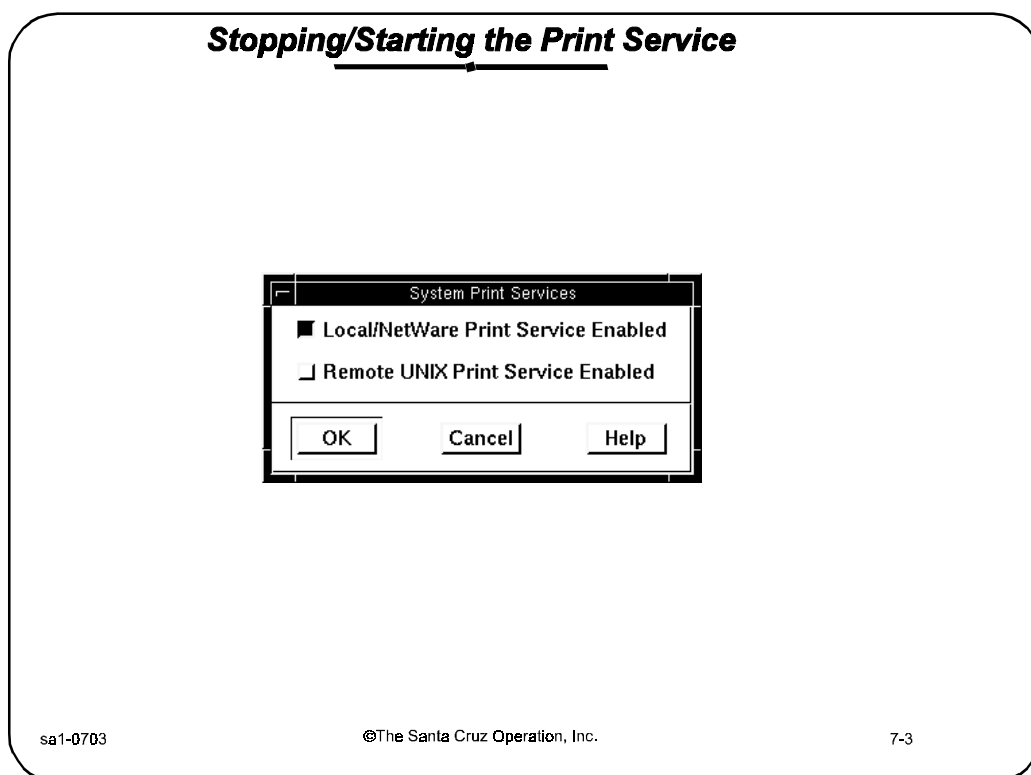
- Receiving files to be printed
- Scheduling the work of one or more printers
- Starting the programs that interface with specific printers
- Tracking the status of print jobs
- Alerting you to printer problems
- Issuing error messages when problems occur

When a user prints a file, a daemon process called the printer scheduler, **lpsched**(ADM), 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.

Use the **lpstat**(C) command to view the status of the various printers:

**lpstat -t | more**

AV 8-3



**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 multiuser mode. 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.

The following steps describe how to stop the print service manually without stopping the operating system:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select **System** ⇒ **Print Services**.
- Step 4. Deselect **Local print service enabled**. If your system supports remote printing, also deselect **Remote UNIX print service enabled**.
- Step 5. Select **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **lpshut**(ADM) command to stop the print service:

**/usr/lib/lpshut**

---

### 8.1.3 Starting the print service

---

The following steps describe how to restart the print service:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select **System** ⇒ **Print Services**.

- Step 4. Select **Local print service enabled**. If your system supports remote printing, also select **Remote UNIX print service enabled**.
- Step 5. Select **OK**.
- Step 6. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **lpsched**(ADM) command to start the print service:

**/usr/lib/lpsched**

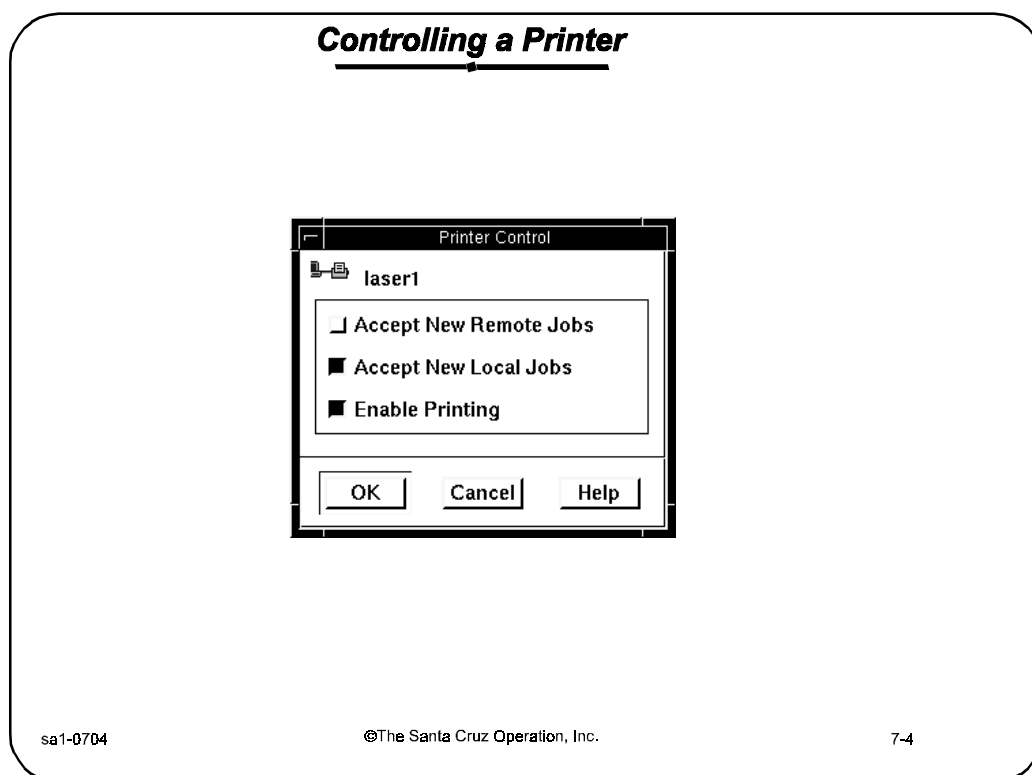
### **Exercise: Stopping the print service**

---

Shut down the print service, and try to print a file. What is the error message? Run **lpstat(C)**. What does it say?

Restart the print service. Run **lpstat(C)** to ensure that the print service is running.

AV 8-4



## 8.2 Accepting and Rejecting Print Jobs

---

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 such situations, you want the print queue to reject print jobs so that users will know to send requests to another printer.

### 8.2.1 Rejecting print jobs

---

The following steps describe how to stop a printer from accepting print jobs:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select the desired printer.
- Step 4. Select **Settings** ⇒ **Control**.
- Step 5. Deselect **Accept new local jobs**. If this printer accepts requests from remote systems, also deselect **Accept new remote jobs**.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **reject**(ADM) command to stop a printer from accepting print jobs:

**reject *printername***

Use the option **-r** to reject print jobs so that a reason will show up in an **lpstat**(C) report:

**reject -r"reason" *printername***

Note that users will not see this message unless they run **lpstat**(C).

### 8.2.2 Accepting print jobs

---

The following steps describe how to allow a printer to begin accepting print jobs:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.

- Step 3.        Select the desired printer.
- Step 4.        Select **Settings** ⇒ **Control**.
- Step 5.        Select **Accept new local jobs**. If this printer accepts requests from remote systems, also select **Accept new remote jobs**.
- Step 6.        Select **OK**.
- Step 7.        Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **accept(ADM)** command to allow a printer to begin accepting print jobs:

**accept printername**

### **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(C)**. What does it report? Try to send a print job to *laser1*. What message do you get?

Accept print jobs. Run **lpstat(C)** 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 enable it again.

If you disable the printer while it is in the middle of a print job, the printer restarts the job from the beginning once you enable it.

### 8.3.1 Disabling a printer

---

The following steps describe how to disable a printer:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select the desired printer.
- Step 4. Select **Settings** ⇒ **Control**.
- Step 5. Deselect **Enable printing**.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **disable**(ADM) command to disable a printer, or printers:

**disable *printername* ...**

Use the option **-r** to disable the printer so that a reason appears in an **lpstat**(C) report:

**disable -r"*reason*" *printername* ...**

### 8.3.2 Enabling a printer

---

The following steps describe how to enable a printer:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.

- Step 3.        Select the desired printer.
- Step 4.        Select **Settings** ⇒ **Control**.
- Step 5.        Select **Enable printing**.
- Step 6.        Select **OK**.
- Step 7.        Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

You can also use **enable**(ADM) to enable the printer, or printers:

**enable *printername* ...**

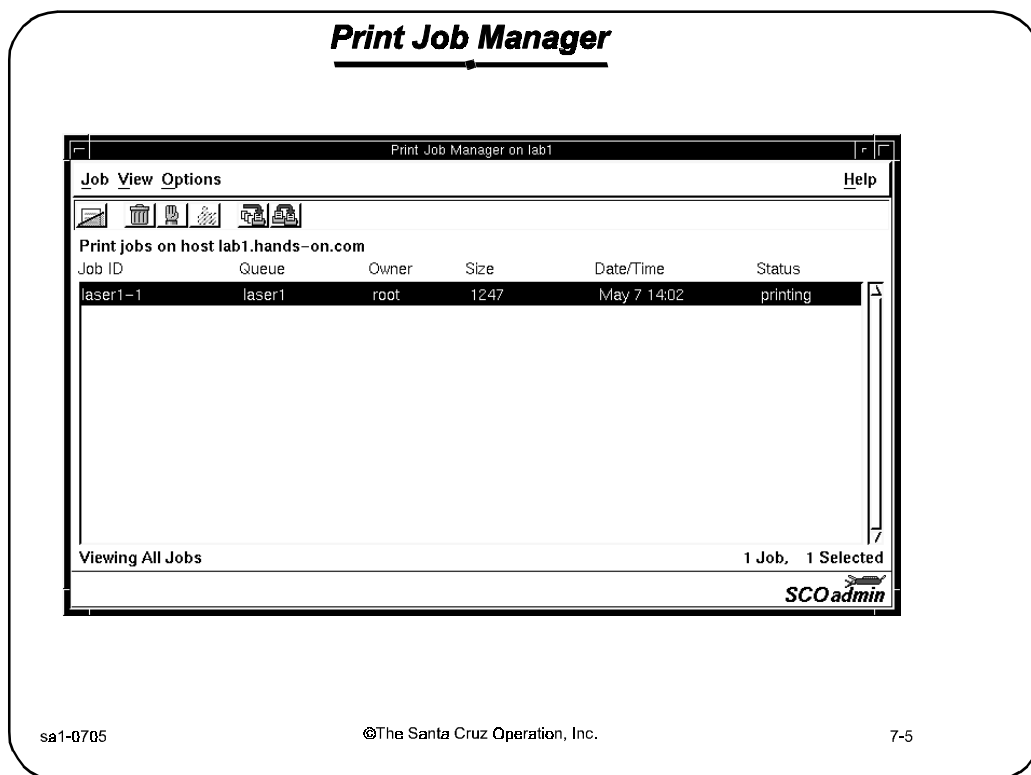
### **Exercise: Disabling a printer**

---

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(C)** again. What happens to the print job?

AV 8-5



## 8.4 Managing Print Jobs

---

What can you do if one of the following situations occurs?

- 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 timely report is sitting in a queue behind many time-consuming and less important print jobs

The **Print Job Manager** allows you to manipulate individual print requests and groups of print requests to keep the queues running smoothly.

### 8.4.1 Viewing print jobs

---

The following steps describe how to view print jobs:

Step 1. Run **scoadmin(ADM)**.

Step 2. Select **Printers** ⇒ **Print Job Manager**.

A list of print jobs that are still in the printer queues appear in the order in which they were submitted.

Step 3. Select **View** ⇒ **By Queue(s)**. Select the queues that you want to view.

Step 4. Select **View** ⇒ **By User(s)**. Select the users that you want to view.

Step 5. Select **Job** ⇒ **Exit** to exit the **Printer Job Manager**.

You can also use the **lpstat(C)** command to view print jobs as follows:

- 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 **sysadm1** and send several print jobs to each printer.

Now view the print requests. Sort the jobs by queue, then by user.

## **8.4.2 Canceling print jobs**

---

The following steps describe how to cancel print jobs:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Printers** ⇒ **Print Job Manager**.
- Step 3. Select the print job(s) you want to cancel.
- Step 4. Select **Job** ⇒ **Delete**.
- Step 5. Select **Job** ⇒ **Exit** to exit the **Printer 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(C)** command to cancel print jobs:

**cancel job\_id1 job\_id2 ...**

### **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 may want to 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 will continue to process other jobs in the queue until you resume the job.

The following steps describe how to hold a print job:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Print Job Manager**.
- Step 3. Select the print job(s) you want to place on hold.
- Step 4. Select **Job** ⇒ **Hold**.
- Step 5. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(C)** command to hold print jobs:

```
lp -i job_id -H hold
```

#### 8.4.3.1 Resuming print jobs

---

The following steps describe how to resume a print job:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Print Job Manager**.
- Step 3. Select the print job(s) you want to resume.
- Step 4. Select **Job** ⇒ **Resume**.
- Step 5. Select **Job** ⇒ **Exit** to exit the **Printer Manager**.

You can also use the **lp(C)** command to resume print jobs:

```
lp -i job_id -H resume
```

### **Exercise: Holding and resuming print jobs**

---

Disable *laser1* so that print jobs will 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 will print 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. If other jobs have already been promoted, the job moves to the end of the list of promoted jobs, unless you promote the job again.

The following steps describe how to promote a print job:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Printers** ⇒ **Print Job Manager**.
- Step 3. Select the desired print job(s), then select **Job** ⇒ **Promote**. The job or jobs move to the top of the queue.
- Step 4. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp(C)** command to promote a print job:

```
lp -i job_id -H immediate
```



**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

---

The following steps describe how to transfer print jobs between queues:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Print Job Manager**.
- Step 3. Select the job(s) to transfer.
- Step 4. Select **Job** ⇒ **Transfer**.
- Step 5. Select the destination queue, then select **OK**.
- Step 6. Select **OK** again when prompted to confirm the destination queue.
- Step 7. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.

You can also use the **lp**(C) command with the option **-d** to transfer print jobs between queues:

**lp -d job\_id -dprint\_queue**

### **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?

## 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

---

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.

The following steps describe how to set up a printer as the default printer:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select the desired printer.
- Step 4. Select **Printer** ⇒ **Set to default**.

The **Printer Manager** displays the name of the default printer in the lower right corner of the screen.

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

### 8.5.2 Setting a default printer for a user

---

You can specify default printers for individual users, overriding the system default.

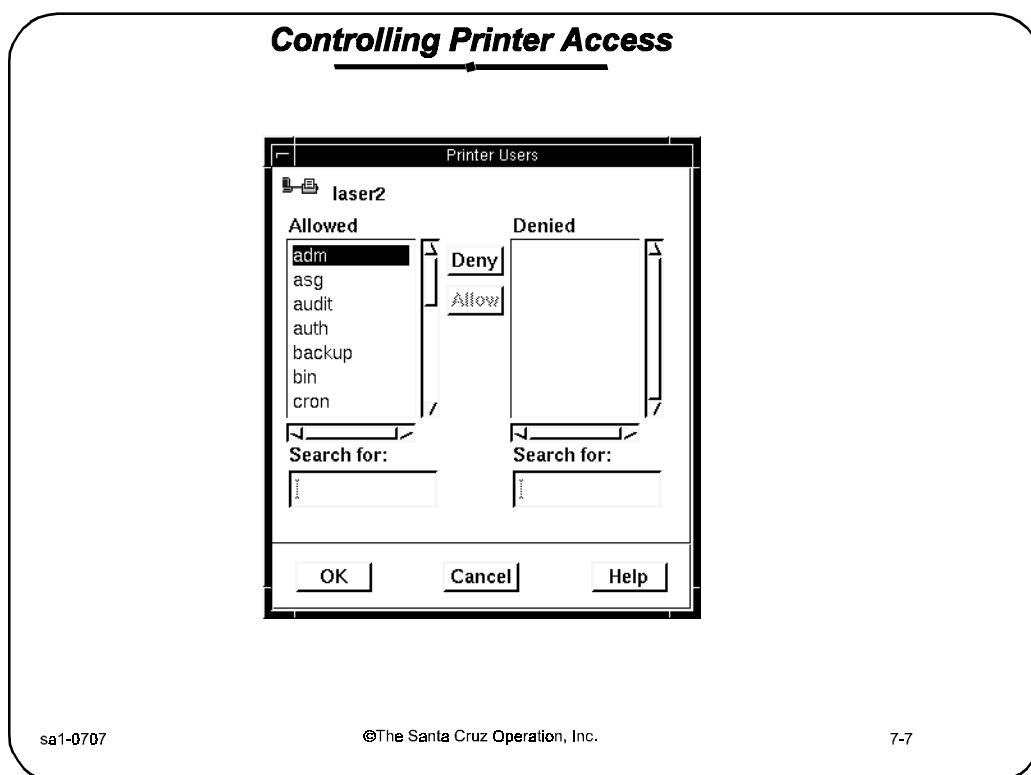
For Bourne and Korn shell users, edit the user's *.profile* and add the following two lines:

```
LPDEST=printername  
export LPDEST
```

For C shell users, edit the user's *.cshrc* and add the following line:

```
setenv LPDEST printername
```

AV 8-6



### 8.5.3 Controlling access to a printer

---

There are situations in which you may 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

The following steps describe how to restrict access to a printer:

Step 1. Run **scoadmin**(ADM).

Step 2. Select **Printers** ⇒ **Printer Manager**.

Step 3. Select the desired printer.

Step 4. Select **Settings** ⇒ **Advanced** ⇒ **Users**.

The “Printer Users” dialog box appears with an **Allowed** and a **Denied** list.

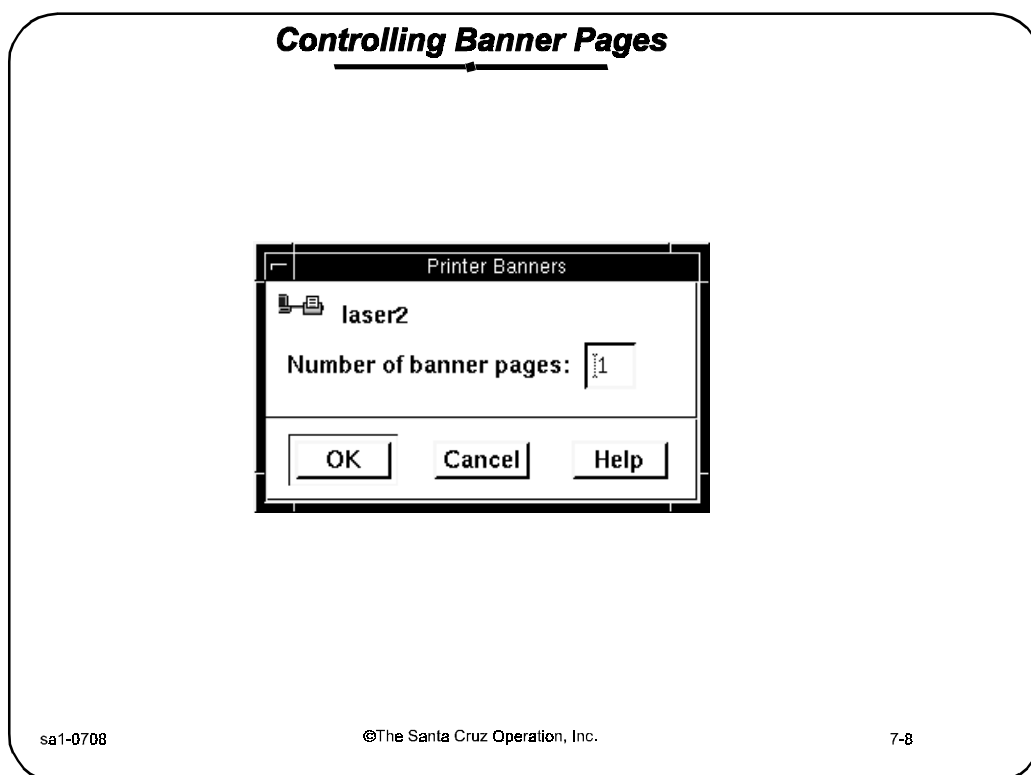
Step 5. Allow or deny access to the printer as follows:

- If a user is on the **Allowed** list, and you want to deny that user access to the printer, select the user ID, then select **Deny**. The user ID moves to the **Denied** list.
- If a user is on the **Denied** list, and you want to allow that user to access the printer, select the user ID, then select **Allow**. The user ID moves to the **Allowed** list.

Step 6. Select **OK**.

Step 7. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

AV 8-7



**Exercise: Controlling access to a printer**

---

Set up the *laser2* printer to deny access to **sysadm2**. Log in as **sysadm2** then try to print */etc/motd* to *laser2*. What error message do you see?

---

**8.5.4 Preventing banner pages**

---

If you have a printer dedicated to printing special forms, such as checks, you may want to disable banner pages so that the printer does not print a banner across the form.

To disable the banner for a specific printer, follow these steps:

- Step 1. Run **scoadmin(ADM)**.
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select the desired printer.
- Step 4. Select **Settings** ⇒ **Advanced** ⇒ **Banners**.
- Step 5. Enter **0** for no banner printing.
- Step 6. Select **OK**.
- Step 7. Select **Host** ⇒ **Exit** to exit the **Printer Manager**.

## 8.6 Troubleshooting Printer Problems

---

---

If a printer stops printing, try the following troubleshooting tips:

- 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 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(C)** to verify that **lpsched(ADM)** is not running. Restart the print service.

If none of the above work, shut down the system and restart it.

Refer to the *SCO OpenServer System Administration Guide*, “Troubleshooting the print system,” for a list of common problems and suggested solutions.

### **Exercise: Online help troubleshooting suggestions**

---

---

Use the online help system to find suggestions if the printer output is illegible.



## 8.7 Lesson Summary

---

---

The print service allows you to control how users access printers. You can temporarily disable a printer for quick maintenance, or you can reject all print jobs if a specific printer is to be down for a few days.

The print service also allows you to control individual print requests. Print jobs can be redirected to different printers, canceled, or moved ahead in the queue.

In addition, the print service allows you to 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 does the print service do?
2. When should you set up a printer to reject print requests?
3. When should you disable a printer?
4. What is the difference between transferring a print job and promoting it?
5. Why would you want to limit access to a specific printer?
6. List three things to check when a printer stops printing.

## 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

---

The following steps describe how shut to down *laser1* for repairs, reject any new print requests for that printer, and redirect any jobs in its queue to *laser2*.

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **Printers** ⇒ **Printer Manager**.
- Step 3. Select *laser1*, then select **Settings** ⇒ **Control**. Deselect **Enable Printing**.
- Step 4. Select *laser2*, then select **Settings** ⇒ **Control**. Deselect **Enable Printing**.
- Step 5. Open a **scoterm** window or multiscreen. Send several print requests to both printers. Some examples are listed below:  
  

```
lp -dlaser1 /etc/motd
lp -dlaser2 /etc/default/tar
```
- Step 6. Select *laser1*, then select **Settings** ⇒ **Control**.
- Step 7. Deselect **Accept new local jobs**.
- Step 8. Select **OK** to activate your choices.
- Step 9. Open a **scoterm** window or multiscreen. Try to send a print job to *laser1*:  
  

```
lp -dlaser1 /etc/motd
```
- Step 10. Run **scoadmin**(ADM).
- Step 11. Select **Printers** ⇒ **Print Job Manager**.

- Step 12. Select **View** ⇒ **By Queue(s)** to list all print jobs on *laser1*.
- Step 13. Select all print jobs currently on *laser1*, then select **Job** ⇒ **Transfer**. Transfer the jobs to *laser2*.
- Step 14. Select **OK**.
- Step 15. Select **OK** again when prompted to transfer the jobs to *laser2*.
- Step 16. Select **Job** ⇒ **Exit** to exit the **Print Job Manager**.
- Step 17. Go back to the **Printer Manager**. Select *laser2*, then select **Settings** ⇒ **Control**. Select **Enable Printing**.
- Step 18. Select **OK**.
- Step 19. 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

---

|                       |                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------|
| <b>accept</b> (ADM)   | Allows print requests to a printer or class of printers                                                      |
| <b>cancel</b> (C)     | Cancels print requests                                                                                       |
| <b>disable</b> (C)    | Turns off a printer or class of printers                                                                     |
| <b>enable</b> (C)     | Turns on a printer or class of printers                                                                      |
| <b>lp</b> (C)         | Sends requests to a printer                                                                                  |
| <b>lp sched</b> (ADM) | Starts the print service                                                                                     |
| <b>lpshut</b> (ADM)   | Stops the print service                                                                                      |
| <b>lpstat</b> (C)     | Prints information about the current status of the print service                                             |
| <b>lpusers</b> (ADM)  | Sets printing queue priorities                                                                               |
| <b>reject</b> (ADM)   | Prevents print requests to a printer or class of printers                                                    |
| <b>scoadmin</b> (ADM) | Invokes SCOadmin applications (in this lesson, the <b>Print Job Manager</b> and the <b>Printer Manager</b> ) |

### Relevant files

---

|                         |                                                                           |
|-------------------------|---------------------------------------------------------------------------|
| <i>\$HOME/.cshrc</i>    | User's C shell login file where a default printer may be set              |
| <i>\$Home/.profile</i>  | User's Bourne or Korn shell login file where a default printer may be set |
| <i>/etc/default/lpd</i> | Default print service options                                             |

## 8.10 Answers to Exercises and Review Questions

---

This section provides suggested answers to the review questions.

### Review questions

---

1. It is expedient to use the **haltsys**(ADM) command when the system is in single-user mode, the shutdown process fails, a hard disk crashes, or a security breach is detected.
2. In single-user, 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 multiuser mode, the system checks and repairs filesystems, if necessary, then mounts any non-root filesystems that have been 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 mode in 15 minutes, enter the following:

```
shutdown -g15 -i1 y -f"The system is coming down."
```



---

# 9

## *Stopping and Starting the System*

AV 9-1

**Stopping and Starting the System**

- **Stop an SCO OpenServer system**
- **Start an SCO OpenServer system**
- **Switch between system modes**

sa1-0801

©The Santa Cruz Operation, Inc.

B-1



**Lesson 9**

## **Stopping and Starting the System**

### **Introduction**

---

Starting and stopping an SCO OpenServer 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 to carry out system maintenance tasks. An improper shutdown can result in the loss of data and a corrupted system. This lesson demonstrates the necessary steps to ensure proper operation.

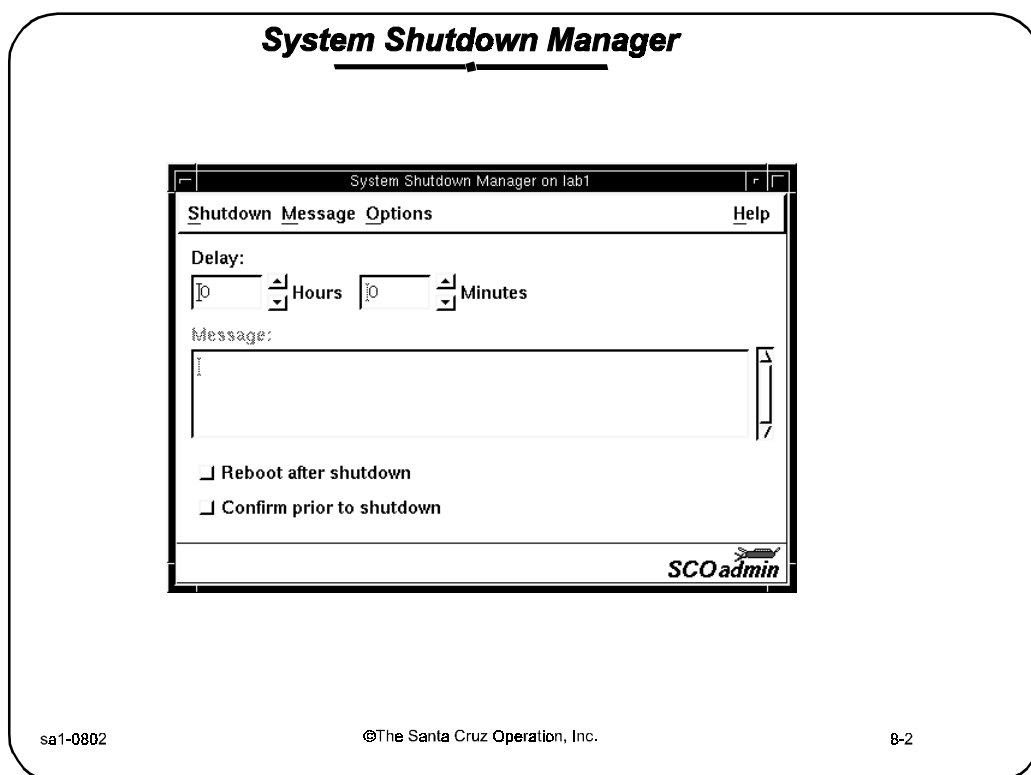
### **Objectives**

---

This lesson describes the proper way to shut down and start up an SCO OpenServer system. By the end of this lesson, you will be able to:

- Stop (shutdown) an SCO OpenServer system
- Start (boot) an SCO OpenServer system
- Switch between system modes

AV 9-2



## 9.1 Stopping an SCO OpenServer System

---

Occasionally, you may need to shut down the system to perform routine system maintenance, for example:

- To replace system hardware
- To clear up hung (defunct) processes or a hung system
- To upgrade system resources, such as processors, memory, or hard disks

Although the new SCO OpenServer filesystems are more robust than earlier releases, a proper shutdown is still the best way to protect filesystems and user data from corruption.

To execute a safe shutdown, the following precautions are necessary:

- 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** account or a user with shutdown privileges can shut down the system

### 9.1.1 Normal shutdown

---

The following steps describe how to perform a normal shutdown:

- Step 1. Run **scoadmin**(ADM).
- Step 2. Select **System** ⇨ **System Shutdown Manager**.
- Step 3. Deselect **Reboot after shutdown** if you do not want the system to automatically reboot.
- Step 4. Deselect **Confirm prior to shutdown** if you do not want to be prompted during the shutdown process.
- Step 5. Enter **15** in the **Minutes** field to give users time to save work and log off the system.
- Step 6. Enter a warning message in the **Message** box to alert users to save their work and log off the system.
- Step 7. Select **Shutdown** ⇨ **Begin Shutdown**.
- Step 8. Select **OK** to confirm the shutdown when prompted.

Note that you can also select **Cancel if you decide** to stop the shutdown.

You can also use the **shutdown**(ADM) command to execute a shutdown:

**shutdown -g15 -y -f"System to shutdown in 15 min."**

The following list describes the options used in this example:

- **-g** sets the number of minutes until the shutdown starts. Use *hh:mm* if you want to specify the number of hours and minutes to precede the shutdown. If you do not set this option, the shutdown starts in one minute.
- **-y** allows the shutdown to proceed without any further prompts
- **-f "mesg"** broadcasts the message to all terminals, warning users to save their work and log out of the system

AV 9-3

### **Shutting Down the System**

#### **shutdown(ADM)**

- polite, gradual
- allows programs warning (networks, windows)

#### **haltsys(ADM)**

- emergencies only
- from single user mode

#### **reboot(ADM)**

- from single user mode
- automatically starts up again

#### **Turn off computer**

- necessary for a "hung" system
- last resort

sa1-0803

©The Santa Cruz Operation, Inc.

8-3

### **Exercise: Shutting down the system**

---

Shut down the system so that the system warns users and then shuts down in 2 minutes.

## **9.1.2 Other shutdown 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 mode
- The shutdown process fails
- A hard disk crashes
- A security breach is detected

If the system is in multiuser mode and you need to bring it down quickly, use the **shutdown**(ADM) command without any delay:

**shutdown -g0 -y**

If the **shutdown** command is not working or the system is in single-user mode, use the **haltsys**(ADM) command:

**haltsys**

If you want to reboot the system immediately after shutdown, you can use the **reboot**(ADM) command:

**reboot**

**WARNING!** The commands **haltsys** and **reboot** can cause problems if used while there is network activity. They should only be used from single-user mode or in emergencies when **shutdown** does not work.

## 9.2 Starting an SCO OpenServer 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
- Repairing the *root* filesystem, if necessary, and mounting it
- Selecting the mode of system operation
- Setting the system date and time

At several points throughout this process, you have the option to accept the default startup or to modify the boot operation. Some examples include:

- Booting from an older kernel if there is a problem with the default
- Booting into single-user mode to perform system maintenance
- Correcting the system date and time

### 9.2.1 Autoboot to multiuser mode

---

Under normal circumstances, you can let the system automatically boot. If no one responds to the boot prompt within a specified time, typically 60 seconds, the system boots automatically. During an automatic boot, the system does the following:

- Loads the default kernel, */stand/unix*, from the primary hard disk
- Cleans the root filesystem, if necessary
- Boots to multiuser mode
- Pauses for 30 seconds so that you can set the date and time. If the system receives no input, it accepts the system-calculated date and time
- Cleans and mounts any other filesystems 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 operation without requiring intervention.

Refer to the **SCO OpenServer Handbook**, “Changing the system restart options,” for instructions on how to change the automatic boot default values.



## 9.2.2 Standard boot

---

If you need to start the system using values other than the default, you must respond to all of the prompts during startup. These are described below.

### 9.2.2.1 Boot prompt

---

The first prompt you see during startup determines which version of the operating system loads.

```
Boot
:
```

If you press **ENTER**, the system boots the default kernel.

If the default kernel does not load correctly, you can load the previous version of the kernel by entering **unix.old** at the prompt:

```
Boot
:unix.old
```

If you have a DOS partition, you can boot DOS by entering **dos** at the prompt:

```
Boot
:bootos dos
```

Once you respond to this prompt, the boot process loads the specified kernel.

### 9.2.2.2 Checking and repairing the root filesystem

---

Once the operating system is loaded, it displays information about the system configuration and verifies that the root filesystem is in order and not corrupted. If there is a problem with the files or directories in the root filesystem, the filesystem is *dirty* and you see the following message:

```
fsstat: root filesystem needs checking
OK to check the root filesystem (/dev/root) (y/n)?
```

You must clean the filesystem. If you choose not to clean it, the root filesystem may become even more corrupt, resulting in unpredictable behavior and eventual failure. Type **y** and press **ENTER**. At this point, the system runs **fsck(ADM)**. Record any error messages that report files with sizes larger than 0. You may need to restore these files.

If the filesystem is in good order, it is called *clean*, and the system mounts it for operation.

---

### 9.2.2.3 Selecting single-user or multiuser mode

---

Once the system mounts the root filesystem, the system is in single-user mode, also known as *run-level 1*. The system then prompts you to either log in to perform system maintenance or to enter multiuser mode. You see the following message:

```
INIT: SINGLE USER MODE
```

```
Type CONTROL-d to continue with normal startup,  
(or give the root password for system maintenance):
```

To bring the system up for full, normal operation, press **CTRL d**. This brings the system up in multiuser mode, also known as *run-level 2*. While the system is in multiuser mode:

- If necessary, the system checks and repairs, then mounts, any non-root filesystems that have been configured to mount during startup
- All system-generated processes are running
- Users can log into the system

Some forms of system maintenance require you to run the system in maintenance, or single-user, mode. For example, backing up the *root* filesystem in single-user mode ensures that users are not modifying files while the backup occurs.

Enter the **root** account password at this prompt to remain in maintenance mode. While in maintenance mode:

- Only the **root** account is logged into the system
- Many system services, such as printing and networking, are not operating
- The system only mounts the boot (*/stand*) and root filesystems

### 9.2.2.4 Setting the system time

---

If the system is booting to multiuser mode, the system prompts you for the correct time and date:

```
INIT: New run level: 2
```

```
Current System Time is Wed Nov 8 08:19:00 PST 1994
Enter new time ([YYMMDD]hhmm[ss]):
```

If the current date and time are correct, press . Otherwise, enter the correct values and press .

**YYMMDD** Optional date field which consists of year, month, day. For example, to set the clock to February 10, 1995, at 2:30 p.m., enter **9502101430**.

**hhmm** The required hours and minutes. Hours should be represented in a 24-hour format. For example, to set the clock to 2:30 p.m., enter **1430**.

**ss** The optional seconds field. For example, to set the clock to 2:30 p.m., 45 seconds, enter **143045**.

Once you set the date and time, the system completes the boot process, and the system is ready for normal operation.

Refer to the *SCO OpenServer Handbook*, “Setting the time and date at startup.”

#### **Exercise: Starting the system**

---

Manually start the system. Enter multiuser mode. If necessary, enter the correct date and time.

## 9.3 Switching Between System Modes

---

The cleanest way to back up your root filesystem is to back it up from single-user mode. You could reboot the system to switch between the two modes, but you can also switch between the modes without fully rebooting the system.

### 9.3.1 Switching from multiuser to single-user mode

---

Use **shutdown -i1** to bring the system from multiuser mode into single-user mode without rebooting the system:

```
shutdown -g15 -i1 -y -f"The system is coming down"
```

Run this command from the system console so that you can then log into system maintenance mode.

### 9.3.2 Switching from single-user to multiuser mode

---

After performing a system backup, you can switch back into multiuser mode without rebooting. To switch back to multiuser mode:

Step 1. Type **CTRL d** at a system prompt to exit single-user mode. You see the following message:

```
INIT: SINGLE USER MODE
```

```
Type CONTROL-d to continue with normal startup,  
(or give the root password for system maintenance):
```

Step 2. Type **CTRL d** again to enter multiuser mode.

#### **Exercise: Switching modes**

---

Bring the system to single-user mode, then back to multiuser mode.

## 9.4 Lesson Summary

---

Shutting down the system in an orderly fashion provides users with enough warning to save their work. However, in cases of emergencies, you can use the **haltsys**(ADM) or **reboot**(ADM) commands to bring the system down more quickly.

Left alone, the system can start up and enter multiuser mode automatically. You can also boot other operating systems, or bring the system into single-user mode for system maintenance.

### Review questions

---

1. When is it expedient to use the **haltsys**(ADM) command instead of the **shutdown**(ADM) command?
2. What is the difference between single-user and multiuser mode?
3. What command would you use to bring the system from multiuser to single-user mode in 15 minutes, and warn users that the system is coming down?

## 9.5 Lab: Abnormal System Startup

---

If you are not using a Uninterruptable Power Source (UPS) with your system, a power failure brings the system down, possibly corrupting the filesystem. You need to bring the system back up and clean any filesystem damage.

### 9.5.1 Overview

---

Turn off the power to the system while it is running in multiuser mode. Manually boot the system and clean all of the filesystems.

### 9.5.2 Procedure

---

The following steps describe how to bring up your system after an abnormal shutdown:

- Step 1. Turn off the system while it is still in multiuser mode.
- Step 2. Wait 10 seconds, then power up the system.
- Step 3. Enter **y** when prompted to check the root filesystem.
- Step 4. Enter **y** when prompted to correct any problems.
- Step 5. Write down any messages displayed before the filesystem was set to “OK.”
- Step 6. Press **CTRL d** when prompted to enter multiuser mode.
- Step 7. Enter **y** if you are prompted to clean the */u* filesystem.
- Step 8. Enter **y** when prompted to correct any problems.
- Step 9. Write down any messages displayed before the filesystem was set to “OK.”

## 9.6 Relevant Commands

---

The following commands were presented in this lesson.

|                       |                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------|
| <b>haltsys</b> (ADM)  | Shuts down the system                                                               |
| <b>reboot</b> (ADM)   | Shuts down the system and reboot                                                    |
| <b>scoadmin</b> (ADM) | Invokes SCOadmin applications (in this lesson, the <b>System Shutdown Manager</b> ) |
| <b>shutdown</b> (ADM) | Shuts down the system in an orderly fashion                                         |

## 9.7 Answers to Review Questions

---

---

This section provides suggested answers to review questions.

### Review questions

---

1. It is expedient to use the **haltsys**(ADM) command when the system is in single-user mode, the shutdown process fails, a hard disk crashes, or a security breach is detected.
2. In single-user, 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 multiuser mode, the system checks and repairs filesystems, if necessary, then mounts any non-root filesystems that have been 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 mode in 15 minutes, enter the following:

```
shutdown -g15 -i1 y -f"The system is coming down."
```



---

**A**

## ***Starting the Desktop***



**Appendix A**

## **Starting the Desktop**

### **Introduction**

---

For your reference, the following pages have been extracted from the ***SCO OpenServer Handbook***.

## A.0.1 Starting the Desktop

---

To start the Desktop, type your login name in the field, press the Enter key, type your password, then press Enter again. To keep your password confidential, it is not shown on the screen as you type it.

---

**NOTE** Users should log in with a non-*root* account to do their daily tasks. It is recommended that only system administrators log in as *root* on the Desktop.

---

If you do not have an account (login) name and password, see your system administrator or the *System Administration Guide*. If you have problems, make sure that the “login” field is highlighted (selected) before entering your name. To select the field, use the mouse to move the pointer into that field, then briefly press and release (click) the left mouse button (mouse button 1).

If your screen is blank, try pressing any key. If your screen is still blank, make sure your terminal is turned on.

If your screen is not blank, the absence of the login box means that the Desktop has been set up to start differently at your site. The most common alternative setup requires you to:

1. Enter your login name at a command-line prompt.
2. Enter your password.
3. At the prompt, enter: **startx**.

See your system administrator for instructions if the Desktop still fails to start.

## A.0.2 Exiting the Desktop

---

When you are ready to exit from the Desktop, open the File menu at the upper left corner of the Desktop by moving the mouse pointer onto the word File and clicking mouse button 1. Then move the mouse pointer to the word Exit and click mouse button 1.

When you are asked, click mouse button 1 on the OK button to confirm that you want to log out.

## A.0.3 Using Desktop features

---

As you work on the Desktop, you can communicate with your computer by pointing to graphic images (objects) on the screen. The objects that you’ll be using the most frequently are icons, windows, menus, and the mouse pointer:

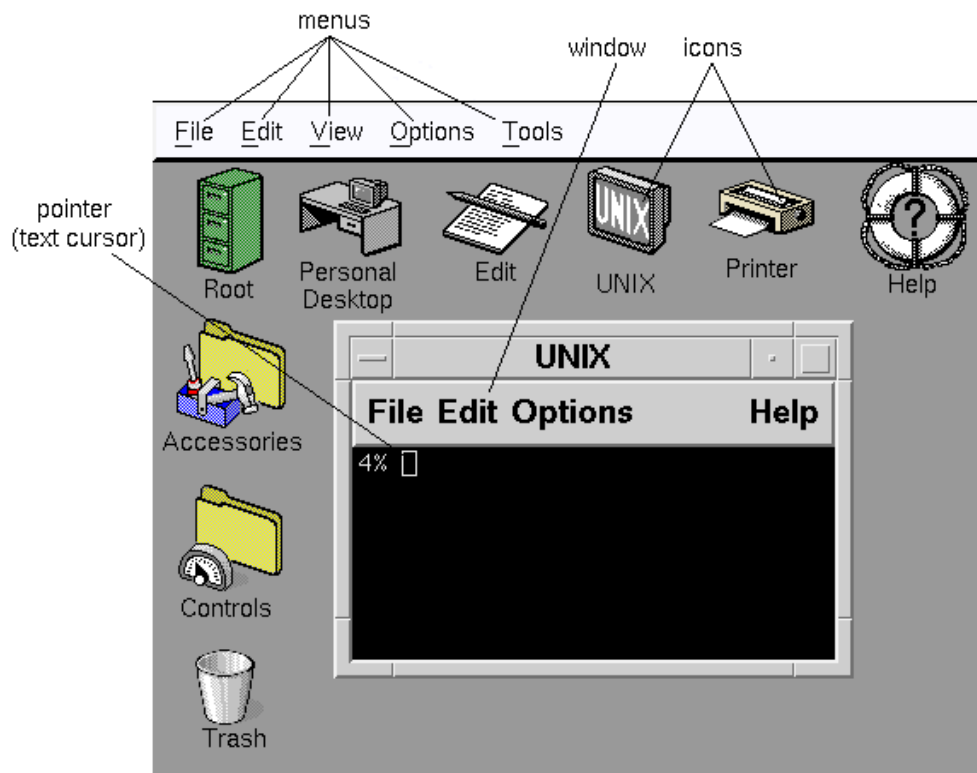


**Figure 1-1 Desktop Overview**

|                |                                                                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Icons</i>   | are small pictures that represent programs, documents, data, or the containers (directories) in which those items are kept.                                                                              |
| <i>Windows</i> | are work areas that open up on the Desktop. You look at and work with information in these windows.                                                                                                      |
| <i>Menus</i>   | are lists of tasks you can perform.                                                                                                                                                                      |
| <i>Pointer</i> | shows you where you are on the screen. It changes shape to let you know what you can do there. An hourglass, for example, indicates that you need to wait while the computer performs your instructions. |

## A.0.4 Using the mouse

---

Use the mouse to point to objects on the screen. When you move the mouse, the pointer moves. When the pointer touches an object, you are pointing to it.

Use the buttons on the mouse to tell your computer what you want to do with the object. There are three ways to use the mouse buttons:

**Click** a button by briefly pressing and releasing it

**Double-click** a button by clicking twice in rapid succession

**Drag** (move) an object by pointing to it, then holding down a button while moving the mouse. Releasing the button “drops” the object in the new location.

When you see instructions to click on an object, point to the object, then click the mouse button.

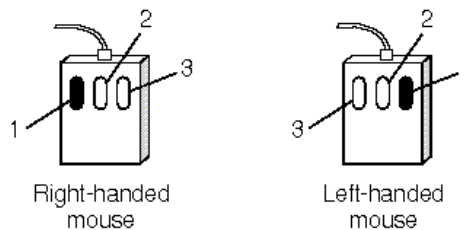


**Figure 1-2 Mouse buttons**

**Always use mouse button 1 unless instructed otherwise.** Mouse button 1 is usually the left button. Left-handed people may prefer that the right button function as button 1 and can change the configuration accordingly. For information on how to do so, see the *Graphical Environment Guide*.

## A.0.5 Pressing onscreen buttons

---

When using the various Desktop programs, you will see a variety of dialog boxes that contain onscreen “buttons.” To press an onscreen button, click on it.

These buttons always initiate the same actions:

|        |                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK     | accepts any changes you made, closes the window, and initiates the appropriate action. In a message window, press OK to indicate you understand the message. |
| Cancel | undoes your changes and closes the window.                                                                                                                   |
| Help   | displays information about the active program.                                                                                                               |

---

## A.0.6 Using windows

---

Windows play an important role in your work on the Desktop. For example, you can have several windows open at the same time, such as one for reading your mail and one for writing contracts. You can then move easily back and forth between these two workspaces, and you can transfer a document or tool from one window (workspace) to another, just as you would on your desk.

Select a window to work in by clicking on it. That window's frame changes color to identify it as the active window. Although you can have many windows open at the same time, you can only enter text, draw, or use controls in one window (the active window) at a time. Programs may be running in other windows, but your computer needs to know to which window it should direct your input.

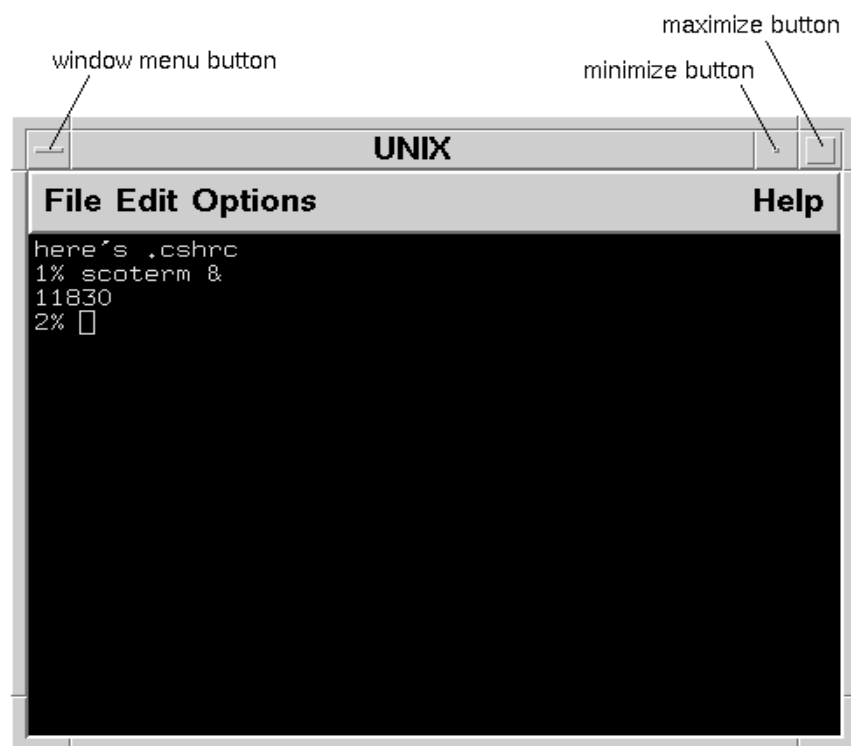


**Figure 1-3 Window Components**

Every window has a Window menu you can use to move, resize, or close the window. Open this menu by clicking on the Window menu button in the upper left corner of the window's frame.

To close a window, select Exit from the *File* menu or double-click on the Window menu button or select Close from the Window menu.

---

## A.0.7 Scrolling

---

When there is more information to display than can fit in a window, use the scroll bars to see more:

- To scroll smoothly through the window's contents, drag the scroll bar slider.
- To move in short jumps toward the top or bottom (or right or left edge) of the window's contents, click on the arrow at either end of the scroll bar.
- To jump by one full window, click on the scroll bar between the slider and one of the arrows.

The position of the slider in the scroll bar indicates how much of the window's contents lies to either side of the portion displayed in the window.

## A.0.8 Using menus

---

Each window has a menu bar that lists the names of the menus available in that window. To open a menu, click on its name. To select an item from the open menu, click on that item. To close the menu without selecting an item, move the pointer off the menu and click (or release) the mouse button.

If the menu item you select requires that you make additional choices, a submenu appears. Use the same methods for selecting from submenus.

## A.0.9 Using icons

---

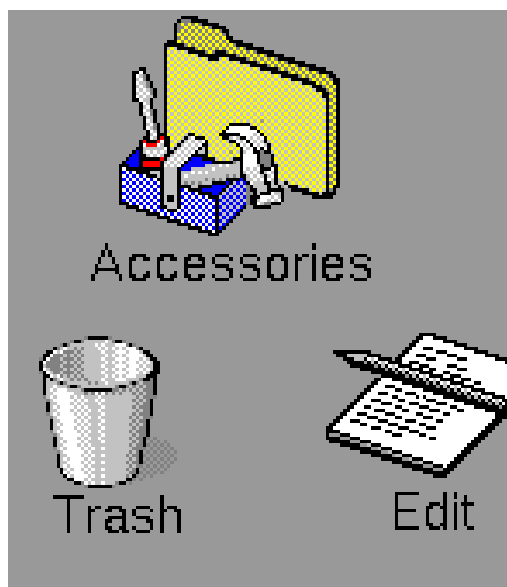


**Figure 1-4** Icon Types

Files and directories on the Desktop are represented as pictures, known as icons. These graphics are designed to give you information about the object that the icon represents. Icons represent unique functions and are illustrated accordingly. The **Trash** icon, for example, represents the *Trash* desktop, which contains your discarded files and directories.



---

To activate an icon, double-click on it. For example, if you double-click on the **Help** icon, you can select from the online help books available in the Documentation Library. For more information on using icons, windows, menus, programs, and other Desktop features, click on *Using the Desktop* in this library.

## **A.0.10 An overview of the SCO Panner window manager**

---

The SCO Panner window manager allows you to use your screen to view different aspects of a much larger workspace than can be displayed at one time. You can organize that workspace to suit your needs. In addition, because you have more space available, your screen becomes less cluttered.

For example, you can control the SCO Panner window manager by using a feature known as the “pan-ner,” which contains a map of your entire workspace, divided by a grid into a number of rectangular regions. These regions serve as work areas. Also provided is a “viewfinder,” which allows you to navigate around the workspace and change your view area.

For more information, see the online help book, *Using SCO Panner*.

