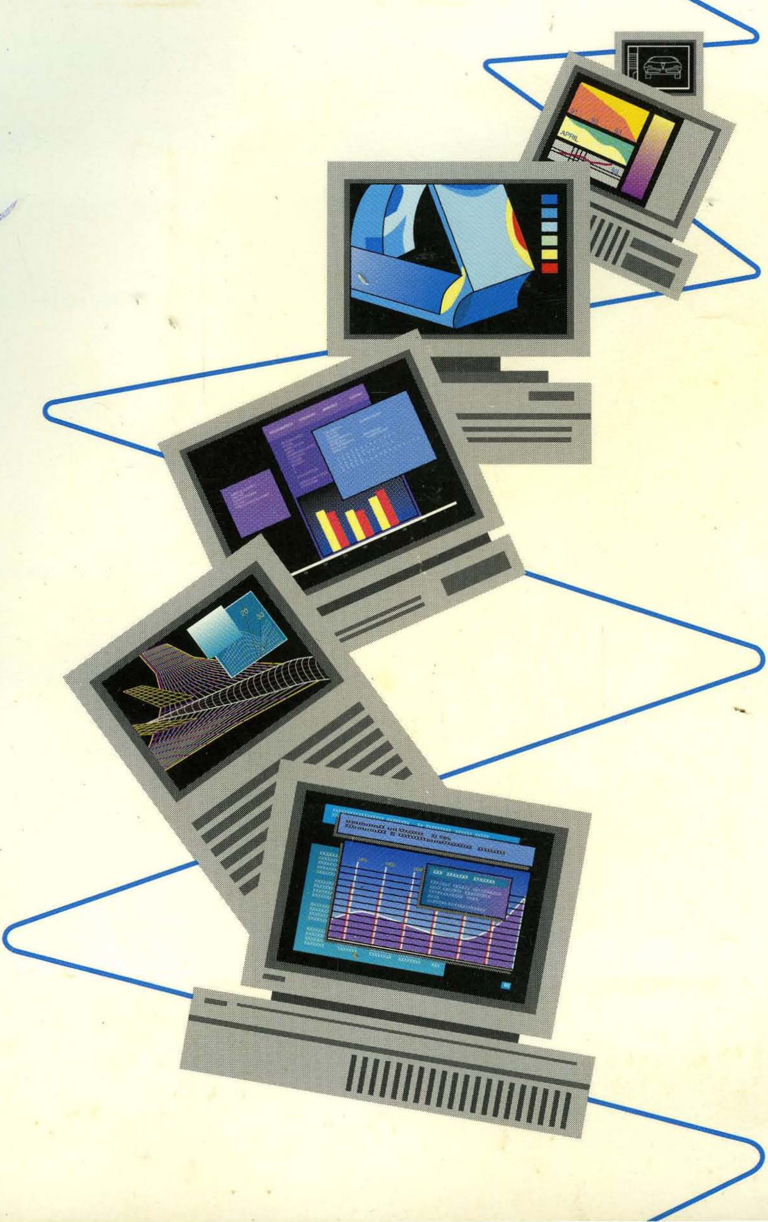
PATHWORKS for VMS

digital

Server Administrator's Guide



PATHWORKS for VMS

Server Administrator's Guide

Order Number: AA–PAGWC–TK

September 1991

Revision/Update Information:	This document supersedes Server Administrator's Guide, Version 4.0, order number AA–PAGWB–TK.
Software Version:	PATHWORKS for VMS Version 4.1

Digital Equipment Corporation
Maynard, Massachusetts

First Published, January 1991
Revised, September 1991

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

The postpaid Reader's Comments forms at the end of this document request your critical evaluation to assist in preparing future documentation.

This document is available on CDROM.

This document was prepared using VAX DOCUMENT, Version 1.2

HOW TO ORDER ADDITIONAL DOCUMENTATION
DIRECT MAIL ORDERS

USA*

Digital Equipment Corporation
P.O. Box CS2008
Nashua, New Hampshire 03061

CANADA

Digital Equipment
of Canada Ltd.
100 Herzberg Road
Kanata, Ontario K2K 2A6
Attn: Direct Order Desk

INTERNATIONAL

Digital Equipment
Corporation
PSG Business
Manager
c/o Digital's local
subsidiary
or approved
distributor

In Continental USA, Alaska, and Hawaii call 800–DIGITAL.

In Canada call 800-267-6215.

*Any order from Puerto Rico must be placed with the local Digital subsidiary (809-754-7575).

Internal orders should be placed through the Software Distribution Center (SDC), Digital Equipment Corporation, Westminster, Massachusetts 01473.

Contents

Preface . . . xiii

1 Introduction to Services

Types of Services . . . 1–2
Service Security . . . 1–3
Disk Service Security . . . 1–3
File Service Security . . . 1–4
How Users Connect to File and Printer Services . . . 1–5
Using the Default Account . . . 1–6
Using VMS Accounts . . . 1–6
How to Choose Services for Applications . . . 1–7
Determining Where to Store Applications . . . 1–7
Setting up Applications with Write Access for Multiple Users . . . 1–8
Using File Services for Applications . . . 1–9
Server Management Tasks . . . 1–9

2 Using the PCSA Manager Menu and Commands

Using the PCSA Manager Utility . . . 2–2
Starting the PCSA Manager Utility . . . 2–2
Exiting the PCSA Manager Utility . . . 2–2
Using the PCSA Manager Menu . . . 2–2
Entering the PCSA Manager Menu . . . 2–3
Exiting the PCSA Manager Menu . . . 2–3
Moving Around the PCSA Manager Menu . . . 2–4
Options Available with PCSA Manager Menu . . . 2–5
Using the PCSA Manager Commands . . . 2–8
Command Syntax . . . 2–8
Entering Commands . . . 2–8
Getting Help . . . 2–9

3 Managing File Services

Understanding How Security Works 3–1
Security in Application File Services 3–2
Security in Common File Services 3–2
Making File Services Available 3–6
Adding a Common File Service with the Menu 3–6
Adding an Application File Service with the Menu 3–8
Adding File Services with the Command Line 3–9
Installing an Application on a Common File Service 3–14
Installing an Application on an Application File Service 3–15
Granting Access to File Services 3–16
Changing File Service Characteristics 3–20
Making File Services Unavailable 3–21
Before Deleting Services 3–21
Deleting a Common or Application File Service 3–22

4 Setting Up Printer Services

Printer Services for Printers Without VMS Queues 4–2
Printers Listed on the Menu 4–2
Printers Not Listed on the Menu 4–7
Printer Services for Printers with VMS Queues 4–13
Printers Not Listed on the Menu 4–13
Printers Listed on the Menu 4–14
Setting Up a Printer Connected to a Terminal Server 4–16
Setting Up a Single Printer 4–16
Setting Up Several Printers 4–19
Preventing Extra Blank Pages 4–20
Editing the Printer Reset Module 4–21
Creating a Printer Reset Module 4–22
Identifying Printer Output for Users 4–24

5 Managing Disk Services

Controlling Security 5–1
Making Disk Service Available Using the Menu 5–2
Adding Application Disk Services 5–3
Installing Applications on a Disk Service 5–4
Making Applications Available to Multiple Clients 5–5
Making Disk Services Available Using the Command Line 5–7
Creating Virtual Disks 5–7
Mounting Virtual Disks 5–10

Modifying Disk Services 5–11
Assigning a Password 5–12
Changing Access 5–12
Limiting Connections to Disk Services 5–12
Defining Whether Users Can Mount Virtual Disks 5–13
Extending Virtual Disk Size 5–13
Assigning Priority to Identically Named Disk Services 5–14
Making Disk Services Unavailable 5–15
Using the Menu 5–15
Using the Command Line 5–16
Accessing Files Within a Virtual Disk from VMS 5–17

6 Managing Users and Groups

Managing Users 6–1
Adding User Accounts 6–2
Modifying the AUTOUSER.BAT File in User Accounts 6–6
Moving User Accounts 6–7
Deleting User Accounts 6–12
Managing Security in User Accounts 6–13
Managing the Default Account 6–15
Managing Groups 6–16
Determining Groups and Their Users 6–16
Creating Groups 6–17
Granting Group and Public Access to Services 6–18
Adding Users to Groups 6–18
Removing Users from Groups 6–19
Deleting Groups 6–19

7 Reconfiguring the Server

Reconfiguring the File Server 7–2
Displaying the Server Configuration 7–2
Changing the Server Configuration 7–3
Changing System Parameters 7–4
Changing the System Page File 7–6
Restarting the File Server 7–6
Reconfiguring the Disk Server 7–7
Reconfiguring the LAST Software 7–9
Changing Timeout on the Disk Server 7–9
Configuring Servers with Group Codes 7–10

8 Improving Server Performance

How Cache Works 8–2
Improving Performance on the File Server 8–2
Collecting Server Data 8–3
Evaluating the Data Collected 8–4
Displaying Cache Parameters 8–6
Adjusting Cache Parameters 8–9
Changing System Parameters 8–10
Changing the System Page File 8–12
Restarting the File Server 8–12
Changing the File Server Priority 8–13
Improving Performance on the Disk Server 8–13
Improving Performance on the Transport Software 8–16

9 Maintaining the Server

Maintaining the File Server 9–1
Monitoring Activity 9–1
Reallocating Resources 9–4
Using the File Server Log File 9–6
Starting and Stopping the File Server 9–10
Managing File Services in a Cluster 9–10
Maintaining the Disk Server 9–11
Monitoring Activity 9–11
Changing Timeout 9–13
Starting and Stopping the Disk Server 9–14
Managing Disk Services in a Cluster 9–14
Backing Up and Restoring Services 9–15
Backing Up Services and User Accounts 9–15
Restoring PCSA and User Accounts 9–18

10 Using the Broadcast Utility

11 Managing Clients

Adding a Node 11–1
Deleting a Node 11–2
Listing Remote Boot Clients 11–3
Deleting a Remote Boot Client 11–3
Restoring a Boot Database 11–4
Listing Client Operating Systems 11–4

12 Managing PATHWORKS Server 3100 Systems

Backing Up and Restoring Data 12–2
Backing Up an Entire Disk 12–2
Restoring Disks 12–4
Shutting Down the Server 12–6
Rebooting the Server 12–7
Listing Nodes 12–8

A Managing VMS and DOS File Differences in File Services

Differences Between VMS and DOS File Structures A–1
Using VMS Files in a DOS Environment A–2
Using VMS Files in File Services A–2
Using Binary Files with Carriage Control Information A–4
Using File Services with Actual and Estimated Length A–4
Correcting Problem Files A–5
Using DOS Files in a VMS Environment A–7

B Setting Up HP LaserJet Printers

C User Profile Form

D Disk Server Startup Parameters

E LAST Startup Parameters

F File Server Startup Parameters

G How Required VMS System Parameters Are Calculated

Prerequisite Information G–1
Parameter Values in the PCFS$STARTUP_PARAMS.DAT File G–2
Memory Required for LANSDRIVER G–2
WSMAX Parameter G–2
SPTREQ Parameter G–3
CHANNELCNT Parameter G–4
System Page File Size G–4
NPAGEDYN Parameter G–5

H Managing VAXmate Clients

Reconfiguring a VAXmate Client H–2
Changing the Ethernet Address H–3
Adding a VAXmate Client for Remote Boot H–5
Creating the Virtual Disk for Remote Boot H–5
Configuring a Client for Remote Boot H–8

Glossary

Index

Examples

2–1 Help for PCSA Manager Commands 2–9
6–1 Connections to File Services 6–9
6–2 Device Names 6–11
6–3 Sample List of Registered Users 6–12
7–1 File Server Configuration 7–3
8–1 Caching Display 8–5
8–2 File Server Parameters 8–6
9–1 Sample Log File 9–7
9–2 Disk Services 9–12
12–1 Sample Listing of Known Nodes 12–9
B–1 Cable Connections B–1

Figures

2–1 PCSA Manager Menu 2–4
2–2 PCSA Manager Menu Options 2–6
4–1 Printer Queue Options 4–3
4–2 PATHWORKS Server 3100 Terminal Line Names 4–4
6–1 User Options Menu 6–2
9–1 Disk Devices for Backup 9–16
12–1 Utility Options Menu for PATHWORKS Server 3100 12–2

Tables

1–1 Access to File and Printer Services 1–7

1–2 Determining Where to Store Applications 1–8

1–3 Server Management Tasks 1–10

4–1 Default Names for Generic Queues, Forms, Subdirectories, and Services 4–6

4–2 Replacements for the Escape Key 4–10

4–3 Device Control Libraries 4–15

4–4 Reset Modules for Printers on the Menu 4–23

5–1 Default Locations for Types of Disk Services 5–8

5–2 Space Allocation for Virtual Disks 5–9

6–1 Disk Quota on a New Disk 6–8

A–1 VMS File Types to Be Used in File Services A–3

A–2 Creating VMS Files Without Carriage Control Information A–6

Preface

Purpose

This manual explains how to set up and manage services for PATHWORKS systems. It also describes how to reconfigure the server and tune for performance.

Audience

This manual is written for system administrators who have have completed the following tasks:

- Connected the network, including all cables, workstations, VAX computers, printers, and other hardware
- Installed the server software
- Installed the client software
- Made an initial connection from the workstation to the server
- Loaded DOS
- Configured clients for local or remote boot using the Netsetup utility

Organization

The following table can help you find information in this manual.

Chapter 1	Provides background on services and introduces you to the management functions for PATHWORKS software.
Chapter 2	Describes the tools to help you manage the server.
Chapter 3	Describes how to set up security and manage file services.
Chapter 4	Describes how to set up printer services.

Chapter 5 Describes how to manage disk services.

Chapter 6 Describes how to set up and manage users and groups.

Chapter 7 Describes how to configure resources on the server.

Chapter 8 Describes how to tune for performance.

Chapter 9 Describes how to manage the file server, disk server and Local Area System Transport (LAST) software.

Chapter 10 Describes how to send Broadcast messages.

Chapter 11 Describes how to list clients, add nodes, and manage remote boot workstations.

Chapter 12 Describes how to maintain a PATHWORKS Server 3100 system.

Appendix A Describes how to manage differences in DOS and VMS files using file services

Appendix B Shows how to set up an HP Laserjet printer.

Appendix C Shows a sample user profile.

Appendix D Shows the default startup parameters for the disk server.

Appendix E Shows the default startup parameters for the LAST software.

Appendix F Shows the default startup parameters for the file server.

Appendix G Shows how the VMS system parameters required for the file and disk servers are calculated.

Appendix H Describes how to manage VAXmate clients on a PATHWORKS server.

Glossary Defines terms used in this manual.

Related Documents

For information on ...	See ...
Configuring clients	*Client Installation and Configuration Guide for the VMS Server*
Client commands	*Client Commands Reference*
Server commands	*Server Administrator's Commands Reference*
VMS system management and security	*VMS System Manager's Manual*

Conventions

This manual uses the following conventions:

Convention	Meaning
Ctrl/*x*	While you hold down the Ctrl key, press another key or a pointing device button.
Ctrl/Alt/Del	While you hold down the Ctrl and Alt keys, press the Del key.
Esc *x*	Press the Esc key, release it, and then press another key or a pointing device button.
Return	Press the key that executes commands or terminates a sequence. This key is labeled Return or Enter, depending on your keyboard.
"enter"	Type all required text, spaces, and punctuation marks; then press Return or Enter, depending on your keyboard.
UPPERCASE	In VMS, DOS, and OS/2 syntax, uppercase letters indicate commands and qualifiers. You can enter commands and qualifiers in any combination of uppercase or lowercase, unless otherwise noted.
lowercase	Lowercase letters in VMS, DOS, and OS/2 syntax indicate parameters. You must substitute a word or value, unless the parameter is optional.
teal blue type	In examples of dialog between you and the system, teal blue type indicates information that you enter. In online (Bookreader) files, this information appears in boldface.
boldface	Boldface type indicates a new term that appears in the glossary. In online (Bookreader) files, boldface indicates information you enter.
kp*n*	Press the specified key on the numeric keypad of your keyboard.

Convention	Meaning
two-line commands	In VMS commands, a hyphen (-) at the end of a command line indicates that the command continues to the next line. If you type the hyphen and press Return, the system displays the _$ prompt at the beginning of the next line. Continue entering the command. If you do not type the hyphen, VMS automatically wraps text to the next line.
/	A forward slash in command descriptions indicates that a command qualifier follows.
NOTE	Notes provide information of special importance.
CAUTION	Cautions provide information to prevent damage to equipment or software.
WARNING	Warnings provide information to prevent personal injury.

Terminology

The terms "personal computer" (PC) and "PC workstation" refer to standalone systems. The term "client" refers to a PC, connected to the network by PATHWORKS software, that can access resources on a server. A server is a system that offers services to clients.

The term "PATHWORKS" refers to PATHWORKS software. PATHWORKS is a trademark of Digital Equipment Corporation.

1

Introduction to Services

With the server management tools, you can make applications, data files, printers, and other resources available as services to clients.

This book explains how to manage services. This task involves:

- Understanding how security works
- Choosing the type of service to use
- Setting up disk, file and printer services
- Making applications available by installing them on services
- Adding users so they can access services on the network
- Specifying access to services
- Changing service characteristics
- Making services unavailable

This book also explains how to manage the server to ensure that it runs smoothly and efficiently. A key function in server management is maintaining a balance between resource use and performance. For example, when you increase the number of clients using the server, performance may decline.

Server management involves:

- Monitoring server operation
- Examining security breaches
- Changing the server configuration
- Improving performance by increasing cache memory
- Monitoring VMS operation to ensure that there are sufficient resources for the server configuration

- Backing up the server
- Managing the server in a cluster environment
- Starting and stopping the server
- Managing the **Local Area System Transport (LAST)**, the communication interface between file and disk services and clients

However, before setting up and managing services, you need to understand the following topics:

- Types of services available
- Service security
- How users connect to file services
- How to choose services for applications
- Server management tasks

This chapter explains these topics.

Types of Services

You can make the following resources available to users:

- Applications

  You can make standard applications available as disk or file services. For example, you can create a disk or file service for LOTUS 1-2-3. After you create the service, install the application and define access to it.

  Creating file services is explained in Chapter 3. Creating disk services is explained in Chapter 5.

  How to choose disk or file services for applications is explained in How to Choose Services for Applications.

- Printers

  A printer service makes a VMS print queue available to clients. VMS print queues are automatically available as printer services. You can create additional printer services for printing files on different forms. **Forms** define the physical layout of the page.

For example, users may need to use both landscape and portrait forms on an Epson printer when they print files from an application, such as Lotus 1-2-3. By creating a printer service for each form (landscape and portrait), users can print directly from the application using either service.

Creating printer services is explained in Chapter 4.

- VMS directories and files

  A file service is a VMS directory. Files stored in a file service are available to both VMS and DOS users. For example, a DOS user can create a text file and a VMS user can run the spell checker on the same file.

  VMS accounts are available to users as file services.

  Because file services are VMS directories, users can access VMS directories using DOS commands.

- DOS files

  Users can store DOS files in either a file or disk service.

  Use file services to store files to be shared between DOS and VMS users.

  You create either common or application file services.

  VMS users access files in a virtual disk by using the PCDISK utility.

Service Security

Security is important to maintain server integrity and control access to files and services. You manage security on disk and file services by controlling users' access to them. The following sections describe how security works for disk and file services.

Disk Service Security

Disk services provide two types of access to users:

- Read and write access to only one user at a time
- Read-only access to multiple users at the same time

You can provide additional security for disk services by:

- Limiting connections to the service
- Defining a service password

For more information about controlling disk service security, see Chapter 5.

File Service Security

Access to file services is determined by:

- The VMS username used in connecting to the service
- Type of service

  File service security is different for common and application services.

In addition, the file server maintains a log file to alert the system manager to security breaches. For more information, see Chapter 9.

Security in Application File Services

How security works in application file services

You define security for application services by:

- Specifying *who* is allowed access to the service
- Choosing the *type* of access: read, read-write, or read-write-create

The type of access applies to the service, its files, and all its subdirectories.

For information on using these commands, see Chapter 3.

Security in Common File Services

How security works in common file services

Security in common file services provides more control than application file services. In common file services, you can control access to individual files as well as to the file service itself. Access to common file services is controlled at two levels, according to the:

- Service
- Individual files within the service

Access to the Service

Service access

You can allow or restrict access to the service using the GRANT or DENY commands. Granting user access allows the user to connect to the service. However, granting access is not always sufficient for a user to access files in the service.

Access to the service applies to the top level, or root directory and all the subdirectories beneath it. Keep in mind that a file service is equivalent to a VMS directory.

Access to Individual Files Within Service

Use RMS protection on files in common services.

You can also control access to individual files within a common file service. Each common file service has a **Record Management Service (RMS)** protection associated with it. The service RMS protection defines the default protection on all files within the service that are created by using the file service.

RMS protection determines whether the user connecting to the service can access the file. A user connects to a file service with a VMS username. Each username has a corresponding **User Identification Code (UIC)**.

A file's RMS protection determines whether a user can access a file and is based on the user's User Identification Code. (The file's owner can change the protection on his files.)

For information on defining the RMS protection, see Chapter 3.

Common file services also have the standard VMS protection, which includes **Access Control Lists (ACLs)**. Users can maintain ACLs on files and directories as they do on other VMS directories.

How Users Connect to File and Printer Services

Users connect to services with the USE command. When connecting to file and printer services, the username in the USE command determines whether the user can access the service.

For example, USER1 connects to a service with the VMS username USER1, as follows:

```
USE LPT2: \\SRVR1\LN03_DPORT%USER1 *
```

The asterisk (*) means that the user is prompted for the password.

Users can connect to file services using:

- Their VMS accounts, with a VMS username and password
- A default account, without a VMS username and password

The account used to connect to a printer service determines how print jobs are identified. See Chapter 4 for more information.

Using the Default Account

The purpose of a default account, if present, is to allow users without a VMS account access to services.

When a user connects to a service using the default account, he does not have to specify a VMS username and password, as follows:

```
USE LPT2: \\SRVR1\LN03_DPORT
```

When users connect using the default account, they can access file services granted to the group PUBLIC. All users are automatically part of the group PUBLIC.

Disable the default account to increase system security.

To increase security on your system, you can disable the default account (see Chapter 6). The name of the default account is PCFS$ACCOUNT unless you change it.

Using VMS Accounts

When you add a user, you create a VMS username and account. For a more secure system, you can require that a user connect to a file service with a username and password.

You create a VMS account by adding a user, which is explained in Chapter 6.

Users must be granted access to a file or printer service before they connect to the service.

When users connect using their own VMS account, they can use file and printer services that are granted access for:

- Individual user
- All groups in which they are members
- Group PUBLIC

Table 1–1 summarizes the access users are allowed depending on the account they used to connect to a file service.

Table 1–1 Access to File and Printer Services

A user connecting with VMS account for...	Can access file services granted to...
An individual user	Individual user
An individual user	All groups in which the user is a member
An individual user	PUBLIC
A default account	PUBLIC

How to Choose Services for Applications

You can install applications on a disk or a file service. This section explains the differences between them.

Disk services are faster than file services. Try to store DOS applications on application disk services whenever possible. Disk services limit read-write access to files to only one user at a time.

Use disk services for applications that do not require simultaneous write access.

Group commonly used applications on one application disk or file service.

The next sections describe:

- Determining where to store applications
- Setting up applications with write access for multiple users
- Using file services for applications

Determining Where to Store Applications

Table 1–2 shows guidelines for determining where to store applications.

Table 1–2 Determining Where to Store Applications

Service Type	For Applications
Disk service	Requiring read-only access
Disk service	Allowing many users to read files simultaneously
Disk service	Requiring read and write access for only one user
File service	With software license agreements requiring the application to be installed on a file server.
Disk service	Designed to be installed on a local hard disk
Disk and file service	Requiring write access to the application service for more than one user simultaneously. (The next section explains how to set up these services.)
File service	Requiring read and write access for more than one user at a time
File service	Requiring files to be accessible to both DOS and VMS users, for example, WPS-PLUS.

Setting up Applications with Write Access for Multiple Users

For applications designed to write back to their application directory, try to use a disk service for the application software and a file service for the data files.

The following guidelines describe how to set up these applications:

- Store these applications on a disk service that can be read by multiple users. (See Chapter 5.)
- Some applications let you redirect their data files to another directory. Use this feature, if possible, to redirect the data files to the user's personal directory.
- If the application does not offer a feature to redirect data files, try using the DOS APPEND command to add a path name for the data files. If the APPEND command lets you use the data files, include the APPEND command in the user's AUTOUSER.BAT file when you add a user. (Adding a user is explained in Chapter 6.)

  When you add a user, set up the user to connect automatically to the application. Then, edit the user's AUTOUSER.BAT file to include the APPEND command.

- If you are unable to set up the application so its data files are stored in a separate directory, store the application in a file service. Change the access for the file service from read-only to read/write. For more information, see Chapter 3.

Using File Services for Applications

If you have chosen to use a file service for your application, you now need to decide whether to use an application or common file service.

When to use application file services

Use application file services to store application programs. You can grant all users read access to the service so that they can run the application.

When to use common file services

Use common file services to store data files that users modify. Common file services allow users to control access to their own files (see Chapter 3).

For example, your department uses Lotus 1-2-3. Some users need to create data files to be shared with other users. In this case, use a common file service for the data files.

In common file services, you can control access to individual files. Set the file protection so that the files' owners can write to them and other users can only read them. For example, you can set up the service so that User1 can modify files he creates, but cannot to modify files that User2 creates.

For more information, see Chapter 3.

Server Management Tasks

Table 1–3 summarizes the server management tasks and the chapter where each is described.

The next chapter describes the tools you can use to perform these tasks.

Table 1–3 Server Management Tasks

For the task...	Read this chapter
Add applications (file service)	Chapter 3
Add applications (disk service)	Chapter 5
Add new user	Chapter 6
Add printer service	Chapter 4
Add printer queue	Chapter 4
Add printer form	Chapter 4
Add user to groups	Chapter 6
Add VMS account	Chapter 6
Back up PATHWORKS Server 3100	Chapter 12
Back up disk services	Chapter 9
Back up file services	Chapter 9
Back up user accounts	Chapter 6
Create groups	Chapter 6
Define automatic connections for users	Chapter 6
Delete applications (file services)	Chapter 3
Delete applications (disk services)	Chapter 5
Delete disk services	Chapter 5
Delete file services	Chapter 3
Delete groups	Chapter 6
Delete printer service	Chapter 4
Delete printer queue	Chapter 4
Exit PCSA Manager Menu	Chapter 2
Exit PCSA Manager utility	Chapter 2
Improve performance	Chapter 8
Increase clients	Chapter 7, Chapter 9
Install applications (on file services)	Chapter 3
Install applications (on disk services)	Chapter 5

(continued on next page)

Table 1–3 (Cont.) Server Management Tasks

For the task...	Read this chapter
List DOS operating systems	Chapter 11
List disk services	Chapter 9
List file services	Chapter 9
List file server log file	Chapter 9
Manage access to file services	Chapter 3
Manage security (file server)	Chapter 9
Manage security (file services)	Chapter 3
Manage security (disk services)	Chapter 5
Manage remote boot clients	Chapter 11
Manage VAXmate clients	Appendix H
Rebooting PATHWORKS Server 3100	Chapter 12
Reconfigure file server	Chapter 9
Reconfigure disk server	Chapter 9
Restore PATHWORKS Server 3100	Chapter 12
Share applications (file services)	Chapter 3
Share applications (disk services)	Chapter 5
Share data files (file services)	Chapter 3
Share data files (disk services)	Chapter 5
Share printers	Chapter 3
Send messages to workstations	Chapter 10
Start file server	Chapter 9
Start Local Area System Transport (LAST)	Chapter 9
Start disk server	Chapter 9
Stop file server	Chapter 9

(continued on next page)

Table 1–3 (Cont.) Server Management Tasks

For the task...	Read this chapter
Stop PATHWORKS Server 3100	Chapter 12
Stop Local Area System Transport (LAST)	Chapter 9
Stop disk server	Chapter 9
Understanding how VMS parameters are used in PATHWORKS for VMS	Appendix G

2 Using the PCSA Manager Menu and Commands

The PCSA Manager utility is provided to help you set up and manage services. The utility offers two interfaces:

- The PCSA Manager Menu

  When to use the PCSA Manager Menu

  The PCSA Manager Menu is easy to use. It prompts you for the information required to complete a task and is especially suited to system administrators who are familiar with DOS but unfamiliar with the VMS operating system.

  Using the menu saves you time and eliminates possible mistakes made by entering long command lines.

  The menu provides some options, such as **Add a Printer Queue**, that are unavailable with the commands.

- The PCSA Manager commands

  You can use the PCSA Manager commands, entered on the command line, for the same tasks you perform with the menu. They also provide advanced functions unavailable with the menu.

  When to use the PCSA Manager commands

  PCSA Manager commands are more suited to system administrators with experience using the VMS operating system.

  An advantage of PCSA Manager commands is that you can include them in VMS batch files. All of the commands are available from the DCL $ prompt.

This chapter describes:

- Using the PCSA Manager Utility
- Using the PCSA Manager Menu
- Using the PCSA Manager commands

Using the PCSA Manager Utility

With the PCSA Manager utility, can run either the PCSA Manager Menu or the PCSA Manager commands.

Starting the PCSA Manager Utility

To start the utility, enter:

```
$ ADMINISTER/PCSA
```

The PCSA Manager Menu prompt is displayed:

```
PCSA_MANAGER>
```

Exiting the PCSA Manager Utility

You can exit the PCSA Manager utility and return to the VMS operating system in two ways. At the PCSA_MANAGER prompt, choose one of the following:

- Press Ctrl/Z
- Enter EXIT

Using the PCSA Manager Menu

This section describes:

- Entering the menu
- Exiting the menu
- Moving around the menu
- Options available with the menu

Entering the PCSA Manager Menu

The method of entering the PCSA Manager Menu depends on whether you have a PATHWORKS Server 3100 system or a PATHWORKS system.

For the PATHWORKS Server 3100 system, the main menu is displayed automatically after you log in to the SYSTEM account.

For the PATHWORKS for VMS system, the VMS operating system prompt ($) is displayed after you log in to the SYSTEM account.

You can enter the PCSA Manager Menu from the PCSA Manager utility or from the VMS operating system prompt.

You can shorten the ADMINISTER/PCSA command to ADMIN/PC.

- To enter the menu from the PCSA Manager utility:

  a. Start the utility. At the VMS prompt, enter:

  ```
  $ ADMINISTER/PCSA
  ```

  b. When the PCSA_MANAGER prompt is displayed, enter:

  ```
  PCSA_MANAGER> MENU
  ```

- Or, you can start the menu in one step from the VMS operating system prompt. Enter:

  ```
  $ ADMIN/PCSA MENU
  ```

Note

You can shorten the ADMIN/PCSA MENU command to PCSA MENU.

Exiting the PCSA Manager Menu

To exit the PCSA Manager Menu, choose one of the following:

- Select the **Exit Menu** option with the arrow keys and then press [Return]
- Press [Ctrl/Z]

If you entered the PCSA Manager Menu in one step, you return directly to the VMS operating system prompt ($).

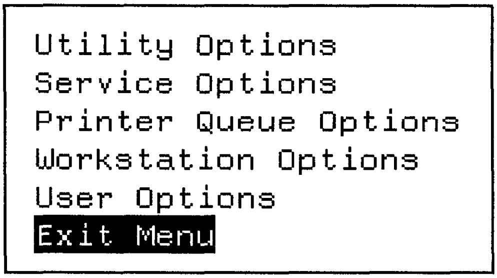
If you entered the PCSA Manager Menu through the utility, you return to the PCSA Manager utility.

Then, exit the utility by pressing [Ctrl/Z] or entering **Exit**.

Moving Around the PCSA Manager Menu

Figure 2–1 shows the top-level selection of the PCSA Manager Menu. Each time you enter the menu, the Exit selection is highlighted.

Figure 2–1 PCSA Manager Menu



To move around the PCSA Manager Menu, follow these guidelines:

- Selecting items

  Use the arrow keys to highlight your selection and then press Return.

  Note

  You can use the Select, Enter or Do keys instead of the Return key.

  After you select a Main Menu item, a submenu is displayed.

  Move to the first menu item by first pressing the Gold/PF1 key and then the up-arrow key.

  Move to the last menu item by first pressing the Gold/PF1 key and then the down-arrow key.

- Scrolling

  To scroll through a selection list that is too large to fit on a single screen, press and release the down arrow key repeatedly.

Caution

Do not hold the down arrow key continuously. Holding the down arrow key continuously to scroll through a large list of selections can stop the PCSA Manager Menu.

- Answering prompts

  Many submenus prompt you to enter information. Each prompt gives guidelines for the response and, in some cases, the prompt also provides default responses. The default responses are displayed in parentheses in the standard VMS format.

  To select the default response, press Return.

- Returning to previous menu

  You have two options:

  - Select Return to Previous Menu, or
  - Press Ctrl/Z

- Canceling an option

  To cancel an option, press Ctrl/Z.

  If you cancel an option in the middle of a task, none of the information you entered prior to canceling is saved.

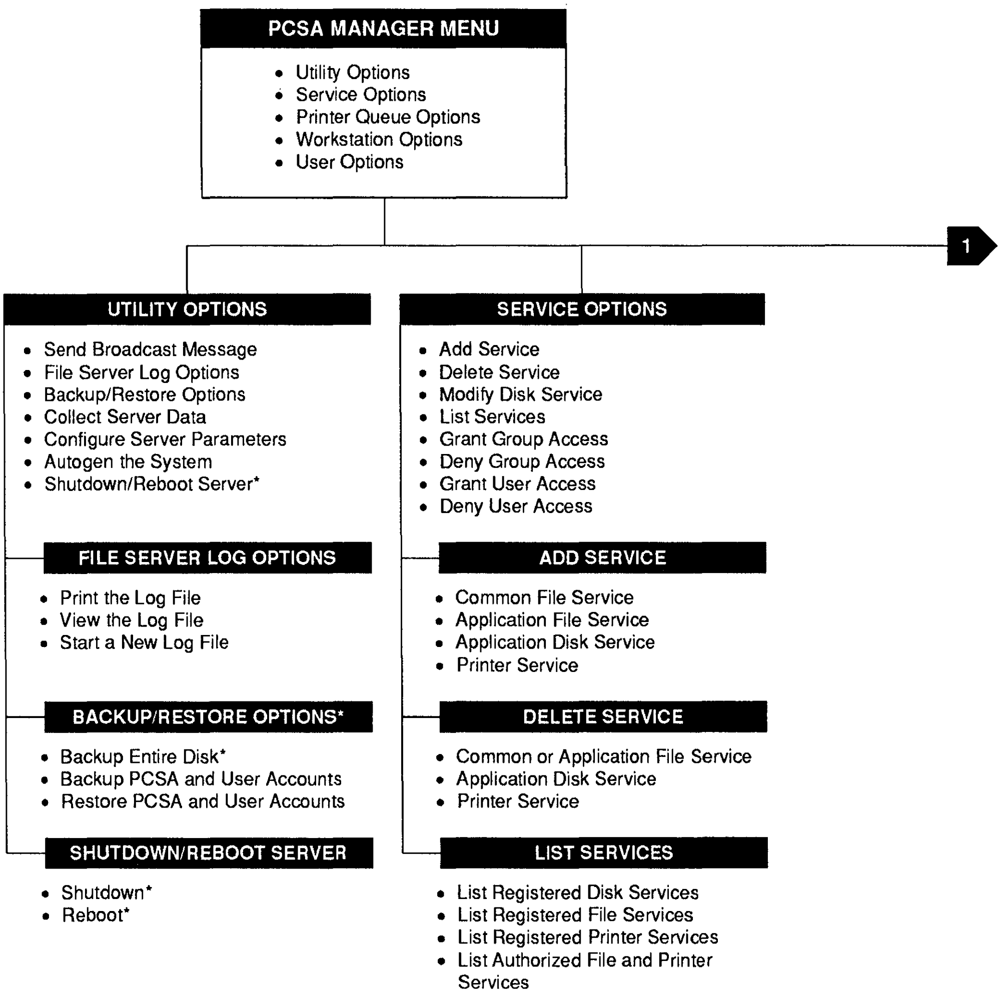
- Completing an option

  Press Ctrl/Z after you answer all of the prompts. The PCSA Manager Menu displays success messages and the work you entered prior to pressing Ctrl/Z is saved. In this case, pressing Ctrl/Z returns you to the previous menu.

Options Available with PCSA Manager Menu

Figure 2–2 is a diagram of each submenu with its options in the PCSA Manager Menu.

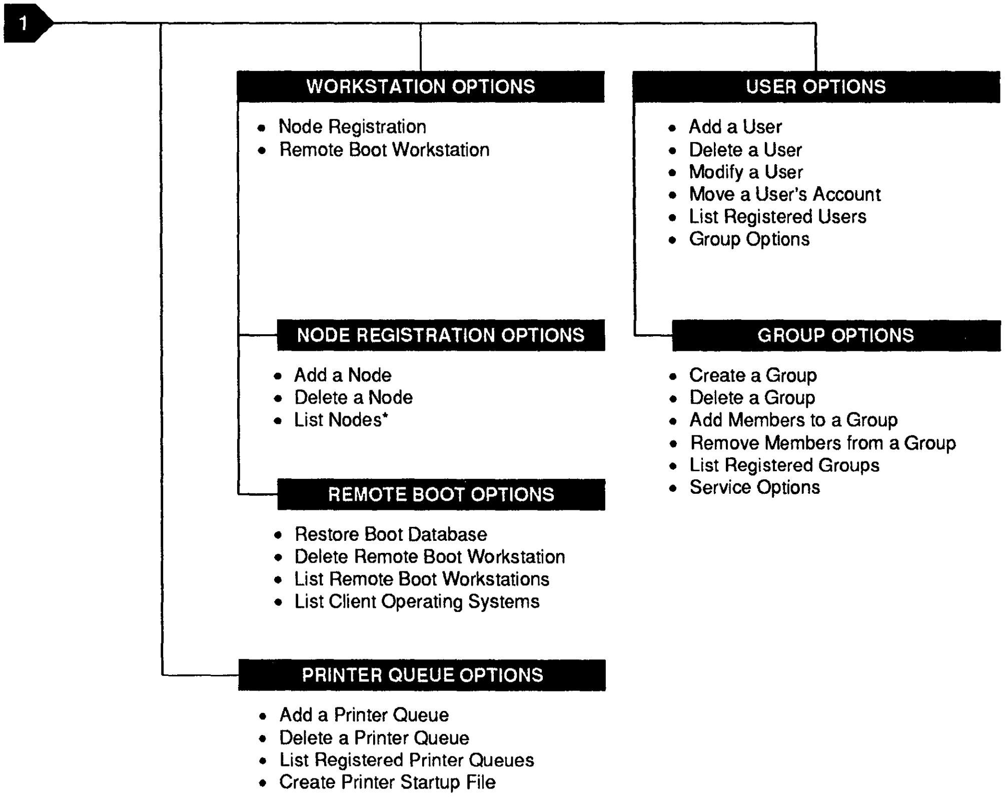
Figure 2–2 PCSA Manager Menu Options



* Option displays only for PATHWORKS Server 3100e systems.

(continued on next page)

Figure 2–2 (Cont.) PCSA Manager Menu Options



TA-0788B-AC

Using the PCSA Manager Commands

This section describes:

- Command syntax
- Entering commands
- Getting help

Command Syntax

The PCSA Manager commands use the VMS command syntax. For example, at the DCL prompt, you enter the command with its qualifiers, if needed.

You do not need to enter values for qualifiers unless you want to change the values.

For example, to limit connections to the file server to 9, enter the following command at the DCL prompt:

```
$  ADMINISTER/PCSA SET FILE_SERVER SERVICE /CONNECTIONS=9
```

Entering Commands

You can run PCSA Manager commands in two ways:

- One method is to first start the PCSA Manager utility and then enter the individual command.

  Using this method, you can run several commands or enter the menu without exiting the utility.

  To run the PCSA Manager commands:

  a. Start the utility by entering:

  ```
  $  ADMINISTER/PCSA
  ```

  Or shorten the ADMINISTER/PCSA command to ADMIN/PC.

  b. At the PCSA_MANAGER prompt, enter the command. For example, to run the SHOW FILE_SERVER SERVICES command, enter:

  ```
  PCSA_MANAGER>  SHOW FILE_SERVER SERVICES
  ```

  After you enter the command, you return to the PCSA_MANAGER prompt, as shown:

  ```
  PCSA_MANAGER>
  ```

  You can then enter other PCSA Manager commands.

    c. When you have finished running the commands, exit the PCSA Manager utility.

- The second method is by entering a PCSA Manager command directly from the VMS prompt. This method is convenient when you want to run only one command.

  For example, to run the SHOW FILE_SERVER SERVICES command, enter:

  ```
  $  ADMIN/PCSA SHOW FILE_SERVER SERVICES
  ```

  When the command is completed, you return to the VMS prompt ($).

Getting Help

Use the online help that is available for all the PCSA Manager commands to find the correct command syntax or determine the general purpose of the command.

To get help, enter:

```
$ ADMINISTER/PCSA HELP
```

Example 2–1 shows the help screen for the commands.

Example 2–1 Help for PCSA Manager Commands

```
HELP

     The HELP command invokes the VAX/VMS help facility to display  help
     about a particular PCSA_MANAGER command.  For more information, see
     the Server Administrator's Commands Reference.


  Additional information available:

  ADD        BROADCAST  CLOSE      CONFIGURE  CREATE     DELETE     DENY
  DISMOUNT   EXIT       GRANT      HELP       MENU       MODIFY     MOUNT
  REMOVE     SET        SHOW       START      STOP       ZERO

Topic?
```

This manual contains many examples of how to use the commands. A complete set of commands, their syntax, and qualifiers are documented in *Server Administrator's Commands Reference.*

3 Managing File Services

File services allow users to share applications, such as database programs, and text and data files.

Managing file services includes:

- Understanding how security works in application and common file services
- Making file services available
- Changing file service characteristics
- Making file services unavailable

Understanding How Security Works

Understanding how security works in file services is important before adding them. Security is different for application and common file services.

In both common and application file services, you control security by specifying *who* can access the service and the *type* of access allowed, that is read-only or read-write-create.

In a common file service, you control access to individual files as well as to the service itself.

In an application file service, you assign access to the service only. Access to individual files within the service is the same as the access to the service.

Security in Application File Services

Note

System file services have the same security as application file services.

The access you assign to application and system file services applies to all files and directories in the service.

How security in application file services works

For example, if User1 has read access to the application file service MYAPP, then User1 can read the directory MYAPP and any files in the directory. Unless you change User1's access to the service MYAPP, User1 cannot write to any files.

You control access to application services with either the Grant option in the menu or the command line (see Granting Access to File Services in this chapter.)

The file server uses identifiers to control access

For application and system file services, **identifiers** control access to *all* directories and files:

- PCFS$READ identifier allows read-only access
- PCFS$UPDATE identifier allows read, write and create access

The identifiers are defined as a VMS Access Control Entry in Access Control Lists (ACLs). An **access control entry** (ACE) defines access to files and directories in the VMS operating system.

The file server adds the identifiers when a user connects to services. Unlike VMS identifiers, the PCSA identifiers are not part of the User Authorization File. Therefore, do not try to use the PCSA identifiers (PCFS$READ and PCFS$UPDATE) as you would VMS identifiers.

Security in Common File Services

You control access to common file services at two levels, by assigning access to the:

How security in common services works

- Service
- Individual files within the service

Assigning Access to Common Services

You assign access to common services by using the GRANT command or menu option, just as application services. Granting access determines who can *connect* to the service.

When you grant read, write or create access to common file services, you control access to the root, or top directory and all its associated subdirectories. For common file services, access to directories is provided by the PCFS$READ and PCFS$UPDATE identifiers.

Assigning Access to Individual Files

How access to files works

A user's access to files in a common service is based on the:

- VMS username used when connecting to the service
- RMS protection on files within the file service
- ACLs placed on files

RMS protection is determined by the VMS username and its associated UIC.

The **Record Management Service** sets protection on files. RMS protection allows access to users based on their **User Identification Codes (UICs)**. A UIC determines which category the user is part of:

- System, a user with VMS system privileges (SYSPRV), or a system UIC
- Owner, the UIC of the user who creates a file
- Group, the user's UIC group code created for each VMS user account
- World, all other VMS users

The UIC consists of a group and user code. When a user connects to a file service, the VMS username in the USE command translates to a UIC.

UICs are created for each user account. Creating user accounts is explained in Chapter 6.

Note

UIC groups are different than the groups you define with the PCSA Manager Menu or command line.

You control access to individual files in a common service by defining RMS protection for the service. The RMS protection for a file service defines the default RMS protection for future files created in the service.

Assigning RMS protection to files in common service

You define the RMS protection for the service when you add it.

Common services added with the menu have a default RMS protection. To define a different protection, use the command line to add a common service.

For information on ACLs, see VMS System Manager's Manual.

In a common file service, you can use ACLs to control access to files in the file service as you do other VMS files. See *VMS System Manager's Manual* for more information.

Example: Access to Files in Common File Service

The following example explains how the VMS username and RMS protection determine a user's access to files in common file services.

1. On SRVR1, you create a common file service, PCCOMMON.

   To allow read and write access on files for the system and owner, set the following RMS protection:

```
PCSA_MANAGER>  ADD SERVICE /DIR /TYPE=COMMON PCCOMMON -
_PCSA_MANAGER> /RMS_PROTECTION=(SYSTEM:RWED,OWNER:RWED,GROUP:,WORLD:)
```

2. Grant the PCCOMMON service read access for all users:

```
PCSA_MANAGER>  GRANT /GROUP PUBLIC /ACCESS=(READ) PCCOMMON
```

   All users can read the PCCOMMON directory once they connect to it.

3. Grant User1 write access to PCCOMMON so User1 can copy a file to PCCOMMON. Enter:

```
PCSA_MANAGER>  GRANT USER1 ACCESS=(R,W,C) PCCOMMON
```

4. User1 connects to PCCOMMON using his VMS username and password:

```
M:\>  USE N: \\SRVR1\PCCOMMON%USER1 *
```

File's owner is defined by the VMS username in the the USE command.

When User1 later creates a file on drive N, User1 is the file's owner.

5. User1 copies the file MYFILE.TXT into PCCOMMON:

   ```
   M:\> COPY MYFILE.TXT N:
   ```

   The file in PCCOMMON has the RMS protection (System:RWED,Owner:RWED,Group:,World:) that you defined for the file service in step 1.

   User1 is the owner of the file, because he used his username to connect to PCCOMMON.

Connecting using the default account

6. User2 connects to PCCOMMON using the default account:

   ```
   M:\> USE N: \\SRVR1\PCCOMMON
   ```

   User2 cannot access User1's file, because he is neither the system nor the owner of the file.

7. However, if instead:

   - Both User1 and User2 connect to PCCOMMON using the default account
   - User1 copies MYFILE.TXT to PCCOMMON

   The default account owns the file MYFILE.TXT.

   User2 can read the file, since both User1 and User2 are seen as owners of the file.

To access files created by default account, connect using the default account.

For access to files created by the default account, users should connect to the common service using the default account, shown in step 6.

Users cannot connect to the default account if you disabled it.

For access to files created by an individual user (instead of the default account), check the file's RMS protection. The RMS protection shows the access allowed all VMS users according to their UIC category.

To access files created by individual user, check the file's RMS protection

For example, if the RMS protection allows the UIC group read-write access, then any file the group creates can be accessed by another UIC group member.

Note

UIC groups are different than the groups you define with the PCSA Manager Menu or command line.

The file's owner can always redefine the RMS protection on an individual file. For example, the owner can allow UIC groups or world access to his file by changing the file's RMS protection.

You define the RMS protection if you use the command line to add a file service.

Making File Services Available

Making applications available as file services involves these steps:

1. Adding file services
2. Installing applications
3. Granting access to services

The menu provides an easy way for you to add common and application file services. The menu grants access to the service when you add it. You can change the access to a service after you add it.

Adding a Common File Service with the Menu

Use a common file service to store popular applications such as spreadsheets or word processors.

By default, common file service created with the menu let all users read and write to the service directories and data files.

The files in the directory have standard RMS protection. You can use RMS protection categories to restrict access to individual files.

Note

The common directory, PCCOMMON, is automatically set up and made available for PATHWORKS Server 3100 systems as a part of the server software installation. You can add additional common directories for users.

To create a common file service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Add Service** from the Service Options menu.
3. Select **Common File Service** from the Add Service menu.
4. Enter a unique 1- to 25-character name when prompted for the name of the common file service.

   ```
   Common file service name (Example: PCCOMMON) :
   ```

The PCSA Manager Menu displays messages while it:

- Creates the directory for the common service
- Adds the service to the file server's service database
- Grants the public group read, write, and create access to the service

For example, after adding the common file service MY_APP, the PCSA Manager Menu displays the following messages:

```
%PCSA-I-DIRCREATED, directory SYS$SYSDEVICE:[MY_APP] created
%PCSA-I-ACLCREATED, ACL created on SYS$SYSDEVICE:[000000]MY_APP.DIR
%PCSA-I-SERADDED, service "MY_APP" added

%PCSA-I-SERGRANTED, service "MY_APP" granted to user/group "PUBLIC"
```

Next, proceed to Installing an Application on a Common File Service in this chapter to install the application.

You can change access to the service with one of the Service Options, described in Granting Access to File Services in this chapter.

Adding an Application File Service with the Menu

Store DOS applications, such as Symphony, in an application file service. In application file services, access allowed to the service and to its files is always the same.

An application file service that you add with the menu allows all users read-only access to the application's files and directories by default.

All files are automatically created with the identifiers PCFS$READ and PCFS$UPDATE.

To add an application file service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Add Service** from the Service Options menu.
3. Select **Application File Service** from the Add Service menu.
4. At the prompt, enter the name of the application file service:

   ```
   Application file service name (Example: MYAPP) :
   ```

   Enter a unique 1- to 25-character name for the application file service.

5. At the prompt, enter the VMS username for the user to whom you are granting read, write, and create access to the application file service.

   ```
   VMS username to be granted RWC access (Default: SYSTEM) :
   ```

   By default, the PCSA Manager Menu grants read, write, and create access to the system administrator's account, SYSTEM.

   The system administrator needs read, read write and create access to install the application.

   Any other user you select should be the system administrator or another individual who has system privileges.

The PCSA Manager Menu then displays messages while it:

- Creates the file service for the application
- Adds the service to the file server's service database
- Grants all users read access to the service

  To change access to the service, refer to Granting Access to File Services in this chapter.

- Grants the specified user read, write, and create access to the service

For example, after adding the application file service TEST_APP, the PCSA Manager Menu displays the following messages:

```
%PCSA-I-DIRCREATED, directory SYS$SYSDEVICE:[PCSA.TEST_APP] created
%PCSA-I-ACLCREATED, ACL created on SYS$SYSDEVICE:[PCSA]TEST_APP.DIR
%PCSA-I-SERADDED, service "TEST_APP" added

%PCSA-I-SERGRANTED, service "TEST_APP" granted to user/group "PUBLIC"

%PCSA-I-SERGRANTED, service "TEST_APP" granted to user/group "SYSTEM"
```

Next, proceed to Installing an Application on an Application File Service to install the application.

You can change access to the service with one of the Service Options, explained in Granting Access to File Services.

Adding File Services with the Command Line

You can also add file services with the command line. Use the command line when you want to:

- Define RMS protection
- Choose a location for file services
- Limit connections to a file service
- Specify fixed-length records instead of stream records
- Specify actual file length instead of estimated file length

These options are not available with the menu.

Defining RMS Protection

RMS protection on common file services sets the default protection on files added to the service.

Using RMS protection on a common service

The default protection allows read, write, execute, and delete access (System:RWED, Owner:RWED, Group:, World:) to the system and owner. You can change the RMS protection, for example, to allow world read access instead.

For files to be truly common, that is to allow all users to read, write, execute, and delete files, set the RMS protection to *World:RWED*.

World read access lets any VMS user read files in the common service, regardless of the account used to connect to the service.

Caution

World read allows *all* VMS users access to the file.

Some applications check security on the server. World read access can cause warning messages in these applications.

Example: Redefining Default RMS Protection for Service

The following example shows how to set world read access to files in the PCCOMMON file service:

Defining RMS protection for common service

1. On SRVR1, create a common file service, PCCOMMON, and set the RMS protection at the same time.

   To allow world read access to files, set the following RMS protection:

```
PCSA_MANAGER>  ADD SERVICE /DIR /TYPE=COMMON PCCOMMON -
_PCSA_MANAGER> /RMS_PROTECTION=(S:RWED,O:RWED,G:,W:R)
```

   All users can read the files in PCCOMMON.

2. For all users to read the directory as well as the files, grant the PCCOMMON service read access as follows:

```
PCSA_MANAGER> GRANT /GROUP PUBLIC /ACCESS=(READ) PCCOMMON
```

The RMS protection defines the default protection for files added to the service. A file's owner can always change an individual's file protection.

Example: Redefining RMS Protection on a File

The following example shows how a file's owner can change the file protection. Suppose you created the PCCOMMON service as explained in the previous example. Then:

1. Grant User1 write access to PCCOMMON:

```
PCSA_MANAGER> GRANT /USER1 /ACCESS=(READ, WRITE, CREATE) PCCOMMON
```

2. User1 connects to PCCOMMON using his VMS account:

```
M:\> USE N: \\SRVR1\PCCOMMON%USER1 *
```

3. User1 copies the file MYFILE.TXT into PCCOMMON:

```
M:\> COPY MYFILE.TXT N:
```

File's owner is User1.

User1 owns the file.

4. The RMS protection of MYFILE.TXT is: (System:RWED, Owner:RWED, Group:, World:R) defined in step 1 of the previous example. At the user's personal computer, User1 can change the RMS protection on MYFILE.TXT with the NET ATTRIB command.

   For example, to change the RMS protection to group read instead of world read, User1 can enter:

```
M:\> NET ATTRIB MYFILE.TXT /PROTECTION=(S:RWED,O:RWED,G:R) MYFILE.TXT
```

   For more information on the NET ATTRIB command, see *Client Commands Reference.*

Choosing a Location for File Services

With the PCSA Manager Menu, you can add file services for applications and common services. For both types of services, the server uses the default location for the services.

If you run out of space in the default locations, you can change the default.

The PCFS$APPLICATION and PCFS$COMMON logicals define the default device and root directory where these services are stored. The PCFS_LOGICALS.COM file defines these logicals.

Changing default locations

You can change the logical definitions by editing the SYS$MANAGER:PCFS_LOGICALS.COM file. However, you should record the original definitions to keep track of the file services you added with the previous logicals.

Changing location of individual services

Rather than change the default location for *all* application or common file services, you can choose a location for individual file services as you add them.

Adding File Services in Specific Locations

To add a file service in a location other than the default, use the ADD SERVICE /DIRECTORY command with the /ROOT qualifier.

Adding a file service in a specific location

Specify:

- A file service name that helps identify the service.
- Root directory, the full VMS directory specification for the file service.
- Service type that identifies whether the service is a common or application file service (default). Before selecting a type, be sure to understand the different security for common and application services.

For example, to add the file service MYSERVICE in the directory DUA0:[MYDIR], enter:

```
PCSA_MANAGER> ADD SERVICE MYSERVICE  /DIR /ROOT =DUA0:[MYDIR]
```

This command adds the application to the file server database. Users cannot access the file service until you grant them access to the service, as described in this chapter.

If you do not use the /ROOT qualifier, the /TYPE qualifier determines the default location for the file service.

Caution

Use the /ROOT qualifier with the root directory [000000] with caution. For example, a file service MYSERVICE stored in a directory [000000] includes the entire disk. If you delete MYSERVICE, you delete the entire disk.

Limiting Connections to File Services

In their license agreements, some applications limit the number of users who can use the application at one time. On an application file service, you can limit the number of possible connections to the service. File services added with the PCSA Manager Menu have unlimited connections.

To create the application file service MYAPP in the default directory and limit the connections to 6, enter:

```
PCSA_MANAGER> ADD SERVICE/DIR MYAPP /TYPE=APPLICATION /CON=6
```

Adding File Services with Fixed-Length Records

A file service creates files in one of the following VMS record formats:

- **Stream**, which means that each record is ended with a carriage return. Stream is the RMS record format STREAM.
- **Sequential**, which means that each record has a fixed length of 512 bytes. Sequential is the RMS record format FIXED.

When you use the PCSA Manager Menu to add a file service, files are created with the RMS record format STREAM. When you use the command line, you select the RMS format (STREAM or FIXED) for all files in the service.

Before choosing a record format for a file service, you need to understand which format is best for your application.

For example, suppose you use the file service WPSPLUS to store reports that users create with WPS-PLUS/DOS. As a system adminstrator, you want to use WPS-PLUS/VMS to combine these files into one report. However, WPS-PLUS/VMS expects files in a format of fixed-length 512-byte records.

To create files in FIXED format, use the /ATTRIBUTES =SEQUENTIAL_ FIXED qualifier.

If you want to use WPS-PLUS/VMS to edit files created in DOS, the files need to be in a fixed-length 512-byte record format. To set up a file service to create files in this format, use the /ATTRIBUTES qualifier to specify SEQUENTIAL_FIXED in the ADD SERVICE/DIR command.

For example, to create an application file service WPS-PLUS for files with fixed length records, enter:

```
PCSA_MANAGER>   ADD SERVICE /DIR WPSPLUS /ATTRIBUTES=SEQUENTIAL_FIXED -
_PCSA_MANAGER>  /TYPE=APPLICATION
```

If you are having trouble in VMS sharing files that have been created by using a file service, read Appendix A, which explains differences between the VMS and DOS formats used in file services.

Adding File Services with Actual Length

By using the PCSA Manager commands, you can select file services of either actual or estimated length:

- In an **actual length** file service, the file server determines the file length in actual bytes.

- In an **estimated length** file service, the file server determines the file length based on the position of the end-of-file pointer.

Some DOS applications require actual length for files. (See the application documentation for more information.)

Using actual file length detracts from server performance.

However, using actual length files detracts from server performance. When a file with actual length is opened, the server must read the entire file into memory to determine the length.

For more information on using actual length and estimated length file services, see Appendix A.

To create a file service MYAPP with actual file length, enter:

```
PCSA_MANAGER> ADD SERVICE /DIR MYAPP /TYPE=APP /FILE_LENGTH=ACTUAL
```

Installing an Application on a Common File Service

After you add the common file service, install an application as follows:

1. Create a backup copy of the application by copying the application diskettes as instructed by the manufacturer.
2. At a personal computer, connect to the common file service. Use the client command USE to connect to the service using the default account:

   ```
   m:\> USE ?: \\server_name\common_service_name
   ```

   server_name is the name of the server where you want to install the application.

   common_service_name is the name of the common file service on the server.

   For example, use the following command to connect the personal computer to the common file service, MY_APP, on the server node SRVR1:

   ```
   USE ?: \\SRVR1\MY_APP
   ```

   The personal computer displays the device, for example, drive K:

   ```
   Device K: connected to \\SRVR1\MY_APP
   ```

3. Install the application from the personal computer. Follow the application's installation instructions.
4. Before running applications, make sure you have set up appropriate printer services on the server.

5. To change access to the service, refer to the section Granting Access to File Services.

Most applications work with a network printer. Some, however, require that you use a local printer for the application to print correctly. Others print only to the logical device, LPT1.

For more information on setting up printer services, see Chapter 4.

Note

Some applications require a program diskette to run. For these applications, each user needs a program diskette in drive A to run the application.

Installing an Application on an Application File Service

After you add the application file service, install the application on the service as follows:

1. Back up the application by copying the application diskettes as instructed by the manufacturer.
2. At a personal computer, connect to the application file service. Use the client command USE:

```
USE ?: \\server_name\application_service_name%user_name password
```

server_name is the name of the server where you want to install the application.

application_service_name is the name of the application file service on the server.

user_name is the VMS name for the user to whom you are granting read, write, and create access to the application file service. For services you added with the menu, the default username is SYSTEM.

password is the password for the VMS account. You can also use an asterisk (*) in place of the password. When you use an asterisk, you are prompted for the password.

For example, the following command attaches your personal computer to the application file service, TEST_APP, on the server named SRVR1:

```
USE ?: \\SRVR1\TEST_APP%SYSTEM *
```

3. Install the application from the personal computer. Follow the application's installation instructions.
4. Before running applications, make sure you have set up appropriate printer services on the server.
5. To change access to the service, refer to the section Granting Access to File Services.

Most applications can work with a network printer. Some, however, require that you use a local printer for the application to print correctly. Others print only to the logical device, LPT1.

For more information on setting up printer services, see Chapter 4.

Note

Some applications require a program diskette to run. In this case, each user needs a program diskette in drive A to run the application.

Granting Access to File Services

After you add file services, you can grant access to them. Access determines whether users can connect to the service. In an application file service, access also determines whether users can access files in the service.

You can grant read, write or create access to file services.

Users with **read** access can read files in the service.

Users with **write** access can write to and modify files in a file service.

Caution

Users with write access can delete files in a file service.

Many PC editors require **create** access for users to edit a file.

You grant or deny access to services for:

- Individual users
- Groups
- Group **PUBLIC**

Public access

Granting access to group **Public** means users can connect to a file service by using the default account.

Default access for application and common file services

Application file services created with the PCSA Manager Menu are automatically granted read-only access for public. Common file services created with the PCSA Manager Menu are automatically granted read, write and create access for public.

To reserve a file service for a specific user, first deny public access and then grant individual user access. (See Denying Group and Public Access that follows.)

You can also deny an individual user access to a file service. Or you can deny public access and then regrant it with different access, such as read-only or read-write.

Before granting a user access to a service, make sure the user has a VMS account. Before granting access to groups, add groups. Adding VMS accounts and groups are described in Chapter 6.

After a user has been granted access to a service, the user must connect to the service using his VMS username.

The following sections describe how to:

- List access granted to file and printer services
- Grant public and group access to file and printer services
- Deny public, group and user access to file and printer services
- Grant user access to file and printer services

Listing Access to File and Printer Services

Listing access to file and printer services

To display all file and printer services to which one or more users have access:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **List Services** option from the Service Options menu.
3. Select **List Authorized File and Printer Services** from the List Services menu.

Granting Public and Group Access

Grant group access to give access to file services to all users in a group or to the group public.

To change the access given to a group, first deny group access and then grant group access. For example, you can change group access from read to read, write and create.

To grant group or public access to a file or printer service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Grant Group Access** from the Service Options menu.
3. Select the file or printer service to which you want to grant access.
4. Select the group to which you want to grant access. To grant public access, select **PUBLIC**.
5. Select the different types of access to the service you can grant:
   - Read
   - Read/Write
   - Read/Write/Create

Messages are displayed as the PCSA Manager Menu grants access to the file service.

Denying Group and Public Access

Changing access from groups or public to individual

To change access from group or group public to individual:

- Deny group or public access
- Grant user access to the service

You can also change the type of access granted by denying access and then regranting the desired access (read, read-write, read-write-create).

To deny group or public access to a file or printer service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Deny Group Access** from the Service Options menu.
3. The PCSA Manager Menu displays a list of existing file and printer services. Select the service to which you want to deny access.

4. The PCSA Manager Menu displays a list of existing groups. Select the group to which you want to deny access. To deny public access, select **PUBLIC**.

A message is displayed as the PCSA Manager Menu denies access to the file service.

Granting User Access

Grant user access to services to restrict access to individual users.

To change access from public to individual:

- Disable public access to a file service by denying public access (see previous section).
- Grant user access to the file service.

To grant an individual user access to a file or printer service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Grant User Access** from the Service Options menu.
3. Select the file or printer service to which you want to grant a user access.
4. Enter the VMS username to whom you are granting access
5. Select the access you want to grant to the user:
   - Read
   - Read/Write
   - Read/Write/Create

   Printer services are always given read, write and create access regardless of the rights you specify.

The PCSA Manager Menu displays messages when it grants the user access to the file or printer services.

Denying User Access

Deny an individual access to file services to restrict the individual from using the service. Deny access only to users for whom you previously granted user access. Do not deny user access to a service that you granted public.

To deny an individual user access to a file or printer service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Deny User Access** from the Service Options menu.

3. Select the file or printer services to which you want to deny access.
4. Select the VMS username for whom you want to deny access.

   Messages are displayed as the user is denied access to the file service.

Changing File Service Characteristics

After you create a file service, you can change the following characteristics:

- Number of connections
- Fixed-length or stream records
- Actual length or estimated length
- Alternate names

Changing the Number of Connections

Limiting connections after the file service is created

If you forget to limit the connections to a service when you create it, you can limit the connections later. Some application licenses require that you limit the number of users.

For example, to limit the connections to 6 on an existing service MYAPP, enter:

```
PCSA_MANAGER>  SET FILE_SERVER SERVICE MYAPP /CONN=6
```

Changing to Fixed Format

Changing to FIXED format

To change a file service from STREAM format to FIXED format, enter:

```
PCSA_MANAGER>  SET FILE_SERVER SERVICE MYAPP /ATTRIBUTES=SEQUENTIAL_FIXED
```

Changing to Actual File Length

Changing to actual file length

To change a file service with estimated length to actual file length, enter:

```
PCSA_MANAGER>  SET FILE_SERVICE SERVICE MYAPP /FILE_LENGTH=ACT
```

Using Alternate Names for File Services

You can use an alternate name, or an **alias** for a file service:

- To use a name other than the one you assigned
- To refer to several services by the same name

For example, an alias can refer to several versions of an application, such as Lotus 1-2-3. Although each version has a different service name, you can assign each version the same alias. Then, you can use the alias in the same command file for different users. An alias is like a logical pointer, because the alias points to different services.

Using the GRANT command to define an alias

Assign the same alias for each different version and associate the alias with each user. For example, to assign the file services LOTUS123V1 and LOTUS123V2 an alias 123 for User1 and User2, enter:

```
PCSA_MANAGER>  GRANT USER1 LOTUS123V1 123
PCSA_MANAGER>  GRANT USER2 LOTUS123V2 123
```

Then, in a command file, use the alias 123.

Note

Grant an alias for either a user or for group PUBLIC. Do not grant an alias for groups other than PUBLIC.

Making File Services Unavailable

A service is made up of a directory and its files. By deleting a file service, you can make a file service unavailable while retaining data files.

For example, a file service can contain ASCII data files with payroll information. Although users no longer need the application, they may still want to access the data files.

The following sections describe the procedure to delete file services.

Before Deleting Services

Before you delete a service you should:

- Send a Broadcast message to all personal computer users to let them know you will be deleting the service. See Chapter 10.
- Make a backup copy of the executable and data files in the service.

For more information on making backups for the PATHWORKS Server 3100 system, see Chapter 12.

For information on backing up file services, see Chapter 9.

After you delete the service, clients cannot access the service from the network.

Deleting a Common or Application File Service

Deleting a service from the menu

To delete either a common or application file service:

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Delete Service** from the Service Options menu.
3. Select **Common or Application File Service** from the Delete Service menu.
4. Select the common or application file service you want to delete.
5. At the prompt, respond whether you want to delete all files for the service.

   When you delete a common or application file service, you remove the network availability of files and directories associated with the service. You can, however, keep the files and directories and access them through the VMS operating system or associate them with a different service.

   The PCSA Manager Menu displays messages while it does the following:

   - Denies access to the service
   - Removes the service from the file server's service database
   - Deletes the directory and files, if you chose to delete them

You can also use the command line to delete the service and its files.

Caution

Use the /ROOT qualifier with the root directory [000000] with caution. For example, a file service MYSERVICE stored in a directory [000000] includes the entire disk. If you delete MYSERVICE, you delete the entire disk.

4

Setting Up Printer Services

The VMS queue with its current form is automatically a printer service.

A VMS queue with its current form is **automatically** available to users as a **printer service**. To make additional forms available on the same printer, you need to create a printer service for each form.

A **form** takes advantage of the special features a printer offers, such as italic printing or printing in different type sizes. Forms specify the:

- Physical page layout, such as paper width or stock, on which a file is printed
- Printing mode, such as landscape, portrait, or letter-quality

For example, a user can print a spreadsheet in landscape mode on a VMS queue LPS$LANDSCAPE that is already set up for landscape printing. Users connect to and then print on the printer service LPS$LANDSCAPE. (For information on printing to a printer service from a client, see *Client Commands Reference*.)

To make additional forms available, add new printer services.

However, you need to create a printer service for each additional form that users require. For example, users may need to use both letter quality and draft forms on an Epson printer when printing files from an application, such as Lotus 1-2-3. After you create a different service for each form (letter quality and draft), users can print directly from the application using either service.

You can make parallel printers connected to a user's personal computer available to other users on the network. For more information, see *Client Installation and Configuration Guide for the VMS Server*.

The procedure you use to set up printer services depends on whether you already have a VMS queue for the printer.

This chapter explains:

- How to set up printer services for the following types of printers:
  - Printers without a VMS queue
  - Printers with a VMS queue
  - Printers connected to a terminal server
- How to prevent extra blank pages on non-PostScript printers
- How to identify printer output

Note

You need OPER and SYSPRV privileges to set up printer services.

Printer Services for Printers Without VMS Queues

This section describes how to set up printer services for printers that do not already have a VMS queue and that are:

- Listed on the menu in the **Add Printer Queue** option
- Not listed on the menu

Printers Listed on the Menu

To make printers on the menu available to network users, add a printer queue by using the PCSA Manager Menu.

When you add a printer queue, the PCSA Manager Menu automatically creates a VMS print queue and a printer service for the standard forms that come with the printers on the menu. For example, landscape and portrait forms are available for LN03 printers; 80-column and 132-column forms are available for LA75 printers. Table 4–1 lists the printer services and forms for printers on the menu.

Note

To create **new** forms for a printer listed on the menu, follow the directions to define forms in the section Printers Not Listed on the Menu later in this chapter.

If you are setting up an HP LaserJet printer, refer to Appendix B for information on connecting the printer to the server.

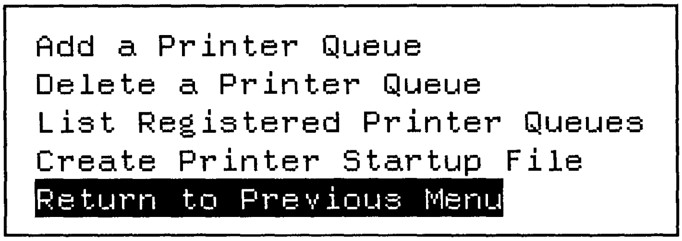
Adding a printer queue

To add a printer queue:

1. Enter the PCSA Manager Menu.
2. Select **Printer Queue Options** from the PCSA Manager Menu.

   Figure 4–1 displays the printer queue options.

Figure 4–1 Printer Queue Options



3. Select **Add a Printer Queue** from the Printer Queue Options menu.

Select printer type.

4. At the prompt for a printer type, select the type of printer to be added.

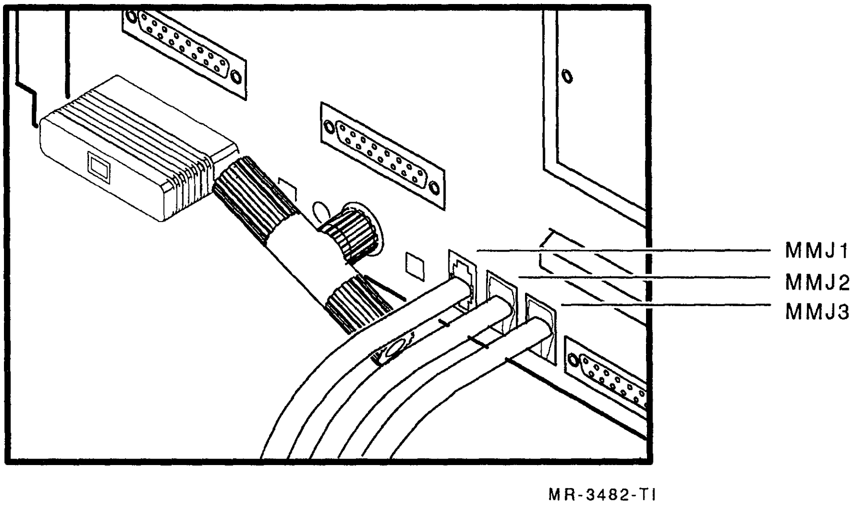
Enter physical line names.

5. At the prompt, respond by entering the physical line name for the printer, for example, TTA2.

   The **physical line** is the terminal line that connects the printer to the server. To add a second printer of the same type, enter the terminal line name for the second printer.

   Valid terminal line names vary depending on your hardware configuration. If you have a PATHWORKS Server 3100 system, the terminal line can be MMJ1, MMJ2, or MMJ3. Figure 4–2 shows the names for the terminal lines for the PATHWORKS Server 3100 system.

Figure 4–2 PATHWORKS Server 3100 Terminal Line Names



The PCSA Manager Menu then:

PCSA Manager Menu defines physical queue,

- Creates the physical and generic queues for the printer

  The **physical queue name** is the server node name followed by $ and the terminal line name. For example, SRVR1$MMJ1 is a valid physical queue name on a server that has the node name SRVR1.

  Defines generic queue,

  The **generic queue name** is PCFS$ followed by the printer type. For example, the generic queue name for an LN03 Plus printer is PCFS$LN03P.

Defines default printer forms,

- Defines the default forms for the printer

  Table 4–1 lists the default forms for each printer type.

- Creates a subdirectory for each printer service in the directory known as PCFS$SPOOL

Defines spool subdirectory,

A **spool subdirectory**, created for each service, stores files before they are printed. Once the file is printed, it is deleted from the subdirectory.

The subdirectory name is the same as the service name and the form. See the third column in Table 4–1 for the subdirectory names for each printer type.

Adds printer service,

- Adds a printer service for each form to the service database

  The service name is the same as the form and the subdirectory name. Table 4–1 lists the default service name for each printer type.

Grants public access to service, and

- Grants all users access to the service

  To change access, see Chapter 3.

- Automatically creates or updates the printer startup file SYS$STARTUP:PCFS_PRINT.COM

Creates printer startup file.

  A **printer startup file** starts the printer queues, defines forms and sets port characteristics for printer services. If you include the printer startup file in the SYSTARTUP_V5.COM file or your site's startup file, it runs automatically when the VMS operating system boots.

Recreating printer startup file

If the startup file becomes corrupted later, you can recreate it using the menu.

To create a printer startup file:

1. Select **Printer Queue Options** from the PCSA Manager Menu.
2. Select **Create Printer Startup File** from the Printer Queue Options menu.

   The PCSA Manager Menu displays messages while it automatically creates a startup file, SYS$STARTUP:PCFS_PRINT.COM.

Table 4–1 Default Names for Generic Queues, Forms, Subdirectories, and Services

Printer	Generic Queue Name	Form, Subdirectory, and Service Names	Output Mode
LN03	PCFS$LN03	LN03_DPORT	Digital Portrait
		LN03_DLAND	Digital Landscape
		LN03_SPORT	Standard Portrait
		LN03_SLAND	Standard Landscape
LN03 Plus	PCFS$LN03P	LN03P_DPORT	Digital Portrait
		LN03P_DLAND	Digital Landscape
		LN03P_SPORT	Standard Portrait
		LN03P_SLAND	Standard Landscape
Epson 850	PCFS$EPSON850	EPSON_FX_850_80	80-column
		EPSON_FX_850_132	132-column
Epson 1050	PCFS$EPSON1050	EPSON_FX_1050_80	80-column
		EPSON_FX_1050_132	132-column
LA50	PCFS$LA50	LA50_D80	Digital 80-column
		LA50_D132	Digital 132-column
LA75 Companion	PCFS$LA75	LA75_D80	Digital 80-column
		LA75_D132	Digital 132-column
		LA75_S80	Standard 80-column
		LA75_S132	Standard 132-column
LJ250	PCFS$LJ250	LJ250_D80	Digital 80-column
		LJ250_D132	Digital 132-column
		LJ250_HP80	Printer Control Language 80-column
		LJ250_HP96	Printer Control Language 96-column
		LJ250_HP144	Printer Control Language 144-column
DEClaser 2100	PCFS$DL2100	DL2100_DPORT	Portrait
		DL2100_DLAND	Landscape

(continued on next page)

Table 4–1 (Cont.) Default Names for Generic Queues, Forms, Subdirectories, and Services

Printer	Generic Queue Name	Form, Subdirectory, and Service Names	Output Mode
DEClaser 2200	PCFS$DL2200_SIMPLEX	DL2200_DPORT_SIMPLEX	Simplex, portrait
		DL2200_DLAND_SIMPLEX	Simplex, landscape
DEClaser 2200	PCFS$DL2200_DUPLEX	DL2200_DPORT_DUPLEX	Duplex, portrait
		DL2200_DLAND_DUPLEX	Duplex, landscape
HP LaserJet	PCFS$HPLASERJET	HP_LASERJET_PORT	Standard Portrait
		HP_LASERJET_LAND	Standard Landscape
IBM ProPrinter	PCFS$PROPRINTER	PROPRINTER_80	Standard 80-column
		PROPRINTER_132	Standard 132-column
NEC Silentwriter	PCFS$SILENTWRITER	SILENTWRITER_ PORT	Portrait
		SILENTWRITER_LAND	Landscape

Printers Not Listed on the Menu

This section describes how to set up printer services for printers that are not listed on the menu.

To make printers that are not listed on the menu available, you need to perform the following tasks:

- Define port characteristics
- Set device characteristics
- Create device control libraries
- Define forms
- Create a generic or physical queue

- Update the VMS startup file
- Add the printer service

This section describes:

- Terms you need to understand before setting up printer services
- An example procedure for setting up a printer service for an Epson printer

Note

Although Epson printers are listed on the menu, use the same procedure for printers not listed on the menu.

Term Definitions

Before you start, you should be familiar with the following terms.

Generic queue

A **generic queue** is a logical device for a physical queue. The generic queue channels a print job to the physical queue. A generic queue can control one or more physical queues.

Separating the physical queue from the generic queue makes it easy to redirect print jobs when a physical device fails. For example, a job you print on the physical queue MMJ1 can be redirected to another physical queue by using a generic queue.

Physical queue

A **physical queue** is the mechanism that controls access to the physical port. You connect a printer to a physical port on the VMS computer.

Device control library

A **device control library** is a VMS text library that contains one or more files, or modules. These modules contain character sequences that instruct the printer to take a particular action. For example, they instruct the printer to print in letter-quality mode or to load a sans serif font.

The character sequences are specific for each type of printer and are described in the programming manual for the printer.

To take advantage of the special features a printer offers, create files, or modules containing the special character sequences for the printer.

Each module is an **entry** in the device control library.

A **form** defines the:

Forms define setup modules,

- Setup modules sent to the printer from the device control library

and page layout.

- Physical layout of the page, such as page width or paper stock, on which a file is printed

A printer service associates a form with a VMS queue.

The printer service associates a specific **form** with a **VMS print queue**.

Example: Setting Up an Epson Printer

This section describes how to set up two printer services:

- For printing in the Roman font in Near Letter Quality mode (NLQ)
- For printing 12-characters-per-inch

The example in this section describes setting up printer services for an Epson FX-850/1050 printer that:

- Communicates at 9600 baud
- Is connected to the TXA1 terminal line on the VMS computer

Set port characteristics

To set up these printer services:

1. Make sure that the VAX port characteristics match the printer's communication characteristics, such as baud rate and parity.

   To find the communication characteristics on the printer, read the printer documentation. You may also need to check the settings on the printer to find the baud rate the printer is set for.

   For example, to set up the print queue PCFS$EPSON for the Epson printer connected to TXA1, enter:

   ```
   $   SET TERM/PERM/WIDTH=80/NOWRAP/PASTRHU/TTSYNCH -
   _$  /SPEED=9600 /DEVICE_TYPE=UNKNOWN /FORM /TAB TXA1
   ```

Set device characteristics.

2. Set the device characteristics for TXA1 to be spooled to an intermediate device.

   The default device is SYS$DISK, the current default disk, although you can specify any existing VMS disk. You must enter a port name, such as TXA1:

   ```
   $  SET DEVICE/SPOOLED TXA1
   ```

Create entries for the device control library.

3. Create control files for the printer. For example, create control files for an Epson printer containing codes for Roman font in Near Letter Quality (NLQ) mode, 12-characters-per-inch, and reset.

   The **reset** mode places the printer in a known state between printer jobs.

   The printer documentation describes the sequence your printer uses for different modes, such as NLQ, 12-characters-per-inch, or reset.

   The following instructions show how to create files for each mode (NLQ-Roman, 12 cpi, and reset) if you can use an Escape character to enter the Escape key:

   ```
   $  CREATE EPSON_NLQ_ROMAN.TXT
   Esck0 Ctrl/Z
   ```

   ```
   $ CREATE EPSON_12CPI.TXT
   EscM Ctrl/Z
   ```

   ```
   $ CREATE EPSON_RESET.TXT
   Esc] VMS;2 Esc\ Esc@ Ctrl/Z
   ```

   However, certain VMS terminal characteristics and terminal types (for example, VT1xx, VT2xx, VT3xx or other series terminal) may prevent you from using the Escape key to enter an Escape character. If this is the case, use any editor to create the device control library modules.

   Table 4–2 displays the EDT and EVE key sequences to use in place of the Escape key.

Table 4–2 Replacements for the Escape Key

If you use this editor:	Replace ESC with this key sequence:
EDT	PF1 2 7 PF1 kp3 The 2 and 7 keys are located on the main keyboard; other keys are located on the keypad. You can use this key sequence in screen mode. To exit the EDT editor, enter Ctrl/Z and then Exit at the Asterisk (*) prompt.
EVE	CTRL/V CTRL/[- Ctrl V and Ctrl [(left bracket)

4. Create a device control library, for example, SYS$LIBRARY:PCFS_EPSON_DEVCTL.TLB, or any name you choose:

```
$  LIBRARY/CREATE/TEXT SYS$LIBRARY:PCFS_EPSON_DEVCTL.TLB
```

5. Insert each control file into the library. Enter:

```
$  LIBRARY/INSERT SYS$LIBRARY:PCFS_EPSON_DEVCTL.TLB EPSON_NLQ_ROMAN.TXT
$  LIBRARY/INSERT SYS$LIBRARY:PCFS_EPSON_DEVCTL.TLB EPSON_12CPI.TXT
$  LIBRARY/INSERT SYS$LIBRARY:PCFS_EPSON_DEVCTL.TLB EPSON_RESET.TXT
```

6. Define a form for the printer using the DEFINE/FORM command.

   First, determine the form numbers already used by entering:

   ```
   $  SHOW QUEUE/FORM
   ```

   Create a form by entering:

```
$   DEFINE/FORM formname number /SETUP=module /NOWRAP /STOCK = stockname -
_$  /WIDTH=n /NOTRUNCATE
```

formname is the 1 to 31 character name you assign a form.

number is an unused form number in the range 1 to 999.

module specifies the module in the device control library that sets up this form.

stockname is the type of paper on which jobs queued with this form are printed. If a queued job requires a stock different than the stock currently being used, the queued job must wait until the requested stock is available.

n specifies the physical width of the paper in terms of columns or character positions. The value for n must be a number between 1 and 65535.

Define separate forms for each module.

Define separate forms for the NLQ-Roman and 12-character-per-inch modes you created in step 1. You do not need to define a form for the reset form.

For example, to define a form number 100 for NLQ-Roman mode and 101 for 12-character-per-inch mode, enter:

```
$   DEFINE/FORM EPSON_NLQ_ROMAN 100 /SETUP=EPSON_NLQ_ROMAN /NOWRAP -
_$  /STOCK=DEFAULT /WIDTH=80 /NOTRUNCATE

$   DEFINE/FORM EPSON_12CPI 101 /SETUP=EPSON_12CPI /NOWRAP -
_$  /STOCK=DEFAULT /WIDTH=132 /NOTRUNCATE
```

The module name you specify with the /SETUP qualifier must match the name of the control file you defined in step 3.

7. Create the queue:

```
$   INITIALIZE/QUEUE/START/LIBRARY=PCFS_EPSON_DEVCTL -
_$  /SEPARATE=(FLAG, RESET=(EPSON_RESET)) /DEFAULT=(NOFEED) TXA1
```

The /START qualifier specifies that the queue should be started when the queue is created.

The /LIBRARY qualifier specifies the device control library.

Create a generic queue.

8. Create a generic queue associated with the queue.

   For example, to create a generic queue PCFS$EPSON associated with TXA1, enter:

   ```
   $  INITIALIZE/QUEUE/START/GENERIC=(TXA1) PCFS$EPSON
   ```

   Generally, you have one generic queue serving many device queues that distributes the load evenly among the different printers.

   You can limit the load to several printers by specifying the printers that the generic queue feeds after the /GENERIC qualifier.

   For example, if you wanted the generic queue PCFS$EPSON to service printers TXA1 and TXA2, enter:

   ```
   $  INITIALIZE/QUEUE/START/GENERIC=(TXA1, TXA2) PCFS$EPSON
   ```

   The generic queue PCFS$EPSON will feed both printers connected to the TXA1 and TXA2 ports. The feed queues TXA1 and TXA2 must have been started with an INITIALIZE /ENABLE_GENERIC command.

   The LPS40 and LN03R printers have different generic queues associated with different default characteristics. Set up more than one generic queue to feed a single physical queue.

Update the VMS startup file.

9. Create a startup file for the printers. For example, create a file PCSA_PRINTER.COM. In the file, include the DEFINE/FORM command you entered in step 6 and the INITIALIZE commands from steps 7 and 8.

   Update the VMS startup file specific to your site.

   The VMS startup file is SYS$STARTUP:SYSTARTUP_V5.COM.

   Edit the SYSTARTUP_V5.COM file to make sure it calls the printer startup file you create.

You insert these commands in the startup file to ensure that the queue is started each time the VAX server boots. The startup file is also a record of the queue in case the queue needs to be rebuilt.

Add a printer service.

10. Add a printer service for each different form. When you add the printer service, keep the following in mind:

    a. Respond to the prompt for the queue by entering the name of the physical or generic queue to which the files are queued. For example, for the Epson printer, enter PCFS$EPSON.

    b. Respond to the form name prompt by entering the form names you specified in the DEFINE/FORM command. For example, enter EPSON_NLQ_ROMAN for NLQ-Roman mode and EPSON_12CPI for 12-cpi mode.

    Follow the directions in the next section to add a printer service.

Printer Services for Printers with VMS Queues

Create printer services for new forms.

If a printer already has a VMS queue, create a separate **printer service** for each **form** to be used with a printer.

This section describes how to set up printer services for printers with VMS print queues and that are:

- Listed on the menu
- Not listed on the menu

Printers Not Listed on the Menu

You can make printers that already have a VMS queue but that are not listed in the menu available as services. For example, add two printer services for an Epson printer to be used for printing both in the NLQ-Roman font and 12-characters-per-inch mode.

Use the menu to add a printer service as follows:

Adding printer services

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Add Service** from the Service Options menu.
3. Select **Printer Service** from the Add Service menu.
4. Enter the name of the printer service you are adding in response to the printer service prompt.

Add a printer service for each form.

Remember to add a separate printer service for each form you use with a printer.

Enter a unique 1- to 25-character name for the printer service. For example, to add a printer service for an EPSON printer, enter EPSON.

5. At the prompt for the queue, enter the name of either the generic or physical queue.

Use either a physical or generic queue name.

   - If you use a generic queue name, enter the name of a generic VMS queue you created. For example, you can use a generic queue name PCFS$EPSON for a generic VMS queue you already created for the Epson printer.
   - The **physical queue name** is the server node name followed by $ and the terminal line name.

     For example, SRVR1$MMJ1 is a valid physical queue name on a server that has the node name SRVR1.

6. At the form prompt, enter a 1- to 31-character form name to use with the service. You can use either the VMS default form or a different form name.
7. An existing VMS queue should already have a VMS startup file defined. If not, define it (see Printers Not Listed on the Menu in Printer Services for Printers Without VMS Queues.)

The PCSA Manager Menu displays messages while it creates the printer service and automatically grants public access to the service.

To change access rights to a service, refer to Chapter 3.

Printers Listed on the Menu

A device control library is provided for each printer listed on the menu. However, these device control libraries, listed in Table 4–3, may not offer all the special features available in another device control library. You can use entries from the supplied device control library with other entries from another device control library.

To use entries from both libraries, extract entries from one library and merge them into the second library.

An **entry** is a module in the device control library.

Table 4–3 Device Control Libraries

Printer	Library Name
LN03	PCFS_LN03_DEVCTL.TLB
LN03 Plus	PCFS_LN03P_DEVCTL.TLB
LA50	PCFS_LA50_DEVCTL.TLB
LA75 Companion	PCFS_LA75_DEVCTL.TLB
LJ250	PCFS_LJ250_DEVCTL.TLB
DEClaser 2100	PCFS_DL2100_DEVCTL.TLB
DEClaser 2200	PCFS_DL2200_SIMPLEX_DEVCTL.TLB
DEClaser 2200	PCFS_DL2200_DUPLEX_DEVCTL.TLB
HP LaserJet	PCFS_HP_LASERJET_DEVCTL.TLB
NEC Silentwriter	PCFS_SILENTWRITER_DEVCTL.TLB
IBM ProPrinter	PCFS_PROPRINTER_DEVCTL.TLB

After merging entries into one device control library, you need to create a printer service for each printer form.

The directions in this section assume that you already have created forms and entries in the device control library for the additional features you want.

For information on creating module entries for a device control library, see Printer Services for Printers Without VMS Queues.

If you do not want to merge entries, create a printer service as explained in Printers Not Listed on the Menu.

Merging entries from different device control libraries

To merge the entries:

1. List your device control library entries for the printer.

   For example, to list the entries in the device control library MY_DEVCTL.TLB, enter:

   ```
   $  LIBRARY/LIST/TEXT SYS$LIBRARY:MY_DEVCTL.TLB
   ```

2. Note the entry names that you want to merge into the file server's device control library.

3. Extract each entry from your device control library.

For example, to extract the entry MY_MODE, enter:

```
$   LIBRARY/EXTRACT=MY_MODE/TEXT/OUTPUT=MY_MODE.TXT MY_DEVCTL.TLB
```

4. Stop the queue before inserting the entry into the device control library.

   If jobs on the queue are printing, enter:

   ```
   $ STOP /QUEUE queuename /NEXT
   ```

   If no jobs on the queue are printing, enter:

   ```
   $ STOP /QUEUE queuename
   ```

5. Insert each entry into the file server's device control library for the printer. The device control library for the LN03 is PCFS_LN03_DEVCTL.TLB.

   For example, to insert the entry MY_MODE into the file server's device control library, PCFS_LN03_DEVCTL.TLB, enter:

```
$ LIBRARY/INSERT/TEXT PCFS_LN03_DEVCTL.TLB MY_MODE.TXT
```

6. Restart the queue by entering:

   ```
   $ START/QUEUE= queuename
   ```

7. Add a printer service for each form, as explained in Printers Not Listed on the Menu.

Setting Up a Printer Connected to a Terminal Server

This section describes how to set up a single printer or printers connected to a terminal server and make them available to network users. A DECserver is an example of a terminal server.

Setting Up a Single Printer

To set up a single printer connected to a terminal server:

1. Connect the printer to a port on the DECserver and connect a terminal to another free port for command input.

   The following example assumes that you connect the printer to port number 8 on the DECserver.

   At the DECserver, enter the following commands to grant you the proper privileges. Note that the default password SYSTEM may have changed:

```
Local> SET PRIV
Password> SYSTEM
```

Enter these commands to check that port number 8 is working correctly. The second command should cause a spiral test pattern to print on the printer you connected to port number 8. The last command stops the test pattern from printing.

```
Local> SHOW PORT 8
Local> TEST PORT 8
Local> LOGOUT PORT 8
```

2. Set the port characteristics permanently.

   One of the port characteristics is the speed of the printer. In this example, the printer speed is 9600.

   ```
   Local> DEF PORT 8 ACCESS REMOTE
   Local> DEF PORT 8 AUTOBAUD DISABLE
   Local> DEF PORT 8 BREAK DISABLE
   Local> DEF PORT 8 INPUT SPEED 9600 OUTPUT SPEED 9600
   Local> DEF PORT 8 DEDICATED NONE PREFERRED NONE
   Local> DEF PORT 8 FORWARD SWITCH NONE
   Local> DEF PORT 8 BACKWARD SWITCH NONE
   ```

3. Associate a name, such as XYZ, with the port:

   ```
   Local> DEF PORT 8 AUTOCONNECT DISABLE NAME XYZ
   Local> LOGOUT PORT 8
   ```

4. Check that you entered the commands in step 2 correctly by entering:

   ```
   Local> SHOW PORT 8
   ```

5. Display the Ethernet address of the DECserver by entering:

   ```
   Local> SHOW SERVER
   ```

   Record the Ethernet address of the DECserver, which you need in the next step.

6. Change the default name of the server to another name, such as MYSERVER, by entering:

   ```
   Local> DEF SERVER NAME MYSERVER
   ```

   This command defines the DECserver name to itself.

7. At the DECserver, enter the INIT command to reset the terminal:

   ```
   Local> INIT
   ```

A screen is displayed on the VAX console or on the DECserver console.

8. Enter the following commands to set up the port for the DECserver:

   ```
   $  SET DEFAULT SYS$SYSTEM
   $  RUN LATCP
   LCP>  SHOW PORT
   ```

9. Note the port numbers that are already defined and enter a new port number. Port numbers must have a prefix of LTA followed by a number that can be as large as 999:

   ```
   LCP>  CREATE PORT LTA991:
   ```

10. Associate the DECserver name, port name, and port number in the SET PORT command:

    ```
    LCP>  SET PORT/NODE=MYSERVER  /PORT= XYZ LTA991
    ```

11. Verify the information by entering:

    ```
    LCP>  SHOW PORT LTA991:
    ```

    Information similar to the following is displayed:

    ```
    Local Port Name = LTA991:
    Specified Remote Nodename = MYSERVER
    Specified Remote Port Name = XYZ
    ```

12. Exit the LATCP program:

    ```
    LCP>  exit
    ```

13. Make sure that the printer on the DECserver can be accessed from the VMS server. You can test this by copying a file from the VAX to the port LT991. To copy the file MYFILE.TXT to port LTA991, enter:

    ```
    $  COPY MYFILE.TXT LTA991:
    ```

14. Check that the terminal is set to LTA991 by entering:

    ```
    $  SHOW TERM LTA991:
    ```

15. Set the terminal characteristics for LTA991 for the width, page size, case, and speed by entering:

    ```
    $  SET TERM LTA991: /PERM /WIDTH=80 /PAGE=66 /NOBROADCAST  -
    _$  /LOWERCASE /SPEED=9600
    ```

16. Set the device characteristics for LTA991 to be spooled to an intermediate device. The default device is SYS$DISK, although you can specify any existing VMS disk. You must enter a queue name, such as MYPRINT, which is the name of the queue you create later:

    ```
    $ SET DEVICE LTA991: /SPOOLED=(MYPRINT,SYS$SYSDEVICE)
    ```

17. Set the protection on the device:

    ```
    $ SET PROTECTION=(S:RWLP,O,G,W)/DEVICE LTA991:
    ```

18. Set up a printer queue using the physical device, such as LTA991. Follow the directions to add a printer service described in Printer Services for Printers Without VMS Queues.

19. Once these commands work properly, include the commands that you entered to the LATCP program in steps 14 and 15 in the startup file, LTLOAD.COM.

Setting Up Several Printers

The procedure to set up several printers with a DECserver is similar to setting up a single printer with a DECserver.

1. Follow steps 1 through 8 in Setting Up a Single Printer for each printer. After you complete these steps, each printer should have a a different port number.

2. Copy a file to each port you created, as described in step 13 in Setting Up a Single Printer .

3. You can set up one service on the DECserver to control several printers. You define the service name, which you can associate with more than one port number.

   For example, to use a printer service PCSASPOOL with ports 1 and 8, enter:

   ```
   Local >  SET SERVICE PCSASPOOL CONNECTIONS -
   ENABLED QUEUE ENABLED PORTS 1,8
   ```

4. Rerun the SET PORT command using the service name for each port. For example, to use the two ports LTA990 and LTA991, enter:

```
$    MCR LATCP
LCP> SET PORT /SERVICE=PCSASPOOL/QUEUED /NODE=MYSERVER /NAME=XYZ LTA990:
LCP> SET PORT /SERVICE=PCSASPOOL/QUEUED /NODE=MYSERVER /NAME=ABC  LTA991:
```

5. Set the terminal characteristics for each port. For example, for port LTA990, enter:

```
$  SET TERM LTA990 /PERM /WIDTH=80 /PAGE=66 /NOBROADCAST  -
_$ /LOWERCASE /SPEED=9600
```

6. Set each device as a spooled device to the disk desired for spooling:

```
$ SET DEVICE LTA990: /SPOOLED=(PCFS$LN03,SYS$SYSDEVICE)
$ SET DEVICE LTA991: /SPOOLED=(PCFS$LN03,SYS$SYSDEVICE)
```

7. Set up a printer queue using the physical device, such as LTA991. Follow the directions to set up a printer queue in Printer Services for Printers Without VMS Queues.

8. To check that the DECserver is set up properly, run two different print commands to:

   a. Print a large number of files to one printer to ensure that the first printer is busy

   b. Print a single file to the same queue to see if the file is sent to the second printer

Preventing Extra Blank Pages

Using printer services to print to non-PostScript printers may cause print jobs to end with an extra blank page. You can prevent the extra blank page from printing by following the directions in this section.

The method you use depends on whether the printer is listed on the PCSA Manager Menu in the **Add a Printer Queue** option.

Preventing Blank Pages for Printers Listed on the Menu

If you are using PATHWORKS for the first time, the software automatically suppresses the extra blank page.

When you add new printer types, blank pages are automatically suppressed.

If you are adding print queues for printer types that have not already been added with the menu, the software automatically suppresses extra blank pages.

However, when you add queues for printer types that are already managed by the menu, you need to edit the reset module.

When you add queues for printer types that are already managed by the menu, you need to change the reset module.

For example, if you have already set up an HP LaserJet printer with a previous version of the menu and you are creating additional queues for HP LaserJet printers, you need to edit the printer reset module. Follow the directions in the next section, Editing the Printer Reset Module.

Preventing Blank Pages for Printers Not Listed on the Menu

To prevent blank pages for printers not listed on the menu, do one of the following:

- For printers with existing VMS queues, edit the printer reset module as described in the next section, Editing the Printer Reset Module.
- For printers without VMS queues, create a reset module. See the section Creating a Printer Reset Module later in this chapter.

Editing the Printer Reset Module

Use the command procedure PCSA$FIX_RESET_MODULES to search for and edit existing reset modules. The procedure adds or removes a control string that suppresses a blank page at the end of the print job. The printer reset module is a module in the printer device control library.

For example, to edit a reset module for an HP LaserJet printer that you already set up with a previous version of the menu:

1. Log in to the SYSTEM account, or make sure that you have SYSPRV and BYPASS privileges.
2. Start the command procedure by entering:
   ```
   $  @SYS$MANAGER:PCSA$FIX_RESET_MODULES
   ```
3. At the prompt, indicate whether you want to add or remove the control string. Select **A** to add the control string that suppresses the blank page.

   You can select help at each prompt by entering ?.
4. The procedure searches the device control libraries for reset modules and displays them. The procedure can change all the reset modules that are displayed, or you can select the modules to be changed.

For example:

```
   Reset module name               Library name
   =========================       =======================
*  RESET                           OUR_DL2100_DEVCTL
*  RESET                           PCFS_HP_LASERJET_DEVCTL
*  RESET                           DAVES_LA50_DEVCTL
*  RESET                           PCFS_LJ250_DEVCTL
*  RESET                           LN03_LIBRARY
```

The modules marked with an asterisk are the ones to be changed.

5. Stop all execution queues for non-PostScript printers using the generic queue names listed in Table 4–1. For example, to stop the execution queue for the HP LaserJet printer, enter:

   ```
   $ STOP /QUEUE /NEXT PCFS$HP_LASERJET
   ```

6. Restart the queues. For example, to start the queue for the HP LaserJet printer, enter:

   ```
   $ START /QUEUE PCFS$HP_LASERJET
   ```

   Stop all the queues before restarting any one of them.

Note

On a system with many printer execution queues, consider rebooting the system instead of stopping and restarting each queue.

Creating a Printer Reset Module

To set up a reset module for a printer without a VMS queue, follow these steps:

1. Follow steps 1 and 2 in Printers Not Listed on the Menu in the section Printer Services for Printers Without VMS Queues.
2. Follow step 3 in the same section to create control files. When you create a reset module:
   a. Include in the reset module the following control string. This string prevents the extra blank page:

```
<ESC>]VMS;2<ESC>\
```

Note

Be sure to enter VMS in uppercase.

b. Include the control strings for your printer shown in Table 4–4.

   (If you do not know the control strings for the reset module, consult the printer documentation.)

Note

Be sure to follow the control sequences exactly, without any extra punctuation or characters.

   For example, the complete control string for the HP LaserJet printer should be:

```
<ESC>]VMS;2<ESC>\<ESC>P<ESC>E<ESC>\
```

Table 4–4 Reset Modules for Printers on the Menu

Device type	Reset control string
LA50	<ESC>[0w<ESC>[0"z<ESC>[0z
LA75	<ESC>[?58l<ESC>[0z<ESC>c
LJ250	<ESC>P<ESC>%@<ESC>[0z<ESC>c<ESC>\
DEClaser 2100	<ESC>P<ESC>[0z<ESC>[!p<ESC>\
DEClaser 2200	<ESC>P<ESC>[0z<ESC>[!p<ESC>\
LN03	<ESC>[!p<ESC>[0z
LN03P	<ESC>[?58l<ESC>[!p<ESC>[0z
HP LaserJet family	<ESC>P<ESC>E<ESC>\
IBM Proprinter	<ESC>@
NEC Silentwriter	<ESC>P<ESC>E<ESC>\

3. Follow the remaining steps in Printers Not Listed on the Menu in the section Printer Services for Printers Without VMS Queues.

Identifying Printer Output for Users

The file server identifies the owner of a print job according to the VMS username used when connecting to the printer service. The job's owner is printed on the banner page, the first page of printer output.

The banner page of the print job is determined in the following way:

- If the user connects to the printer service and specifies a user name and password, then the user name is displayed on the banner page. For example, USER1 connects to SRVR1 by entering:

  ```
  USE LPT2: \\SRVR1\LN03_DPORT%USER1 *
  ```

  Then the banner page displays the owner of the printer job as:

  ```
  SRVR1::USER1
  ```

- If the user connects to the printer service without specifying a user name and password, the file server identifies the owner of the print job as the default account on the server.

  For example, USER1 connects to SRVR1, as follows:

  ```
  USE LPT2: \\SRVR1\LN03_DPORT
  ```

  Then the banner page displays the owner of the job as:

  ```
  SRVR1::PCFS$ACCOUNT
  ```

5 Managing Disk Services

Use disk services to make applications and personal files available to users.

This chapter describes managing disk services, including:

- Controlling security
- Making disk services available using the menu
- Making disk services available using the command line
- Modifying disk services
- Making disk services unavailable
- Accessing files in a disk service from VMS

> **Note**
>
> Refer to the Software Product Description (SPD) to check whether disk services are available for clients with your network configuration.

Controlling Security

You need to understand how to control disk service security before making disk services available. You control security of disk services by:

- Defining a password
- Defining access to the service: read-write or read-only
- Limiting the number of connections

You can control these security features when you mount the disk. **Mounting** a virtual disk makes a disk available to all users or selected users.

You mount virtual disks using either the menu or the command line. With either method, you define security when you mount the disk.

Defining Disk Service Password

Defining a password

Define a password to restrict access to a disk service. Disk services without passwords let all users connect to them.

Defining Access

Controlling access

You also control security of disk services by limiting access to them. You can offer disk services with either of the following types of access:

- Read and write access for only one user
- Read access for a limited number of users

Limiting Connections

Limiting connections

Limit connections to a disk service for applications with licenses for a limited number of users. Disk services with read and write access are automatically limited to one user.

Limit the connections to a service when you mount it.

In a cluster environment, you can limit connections to disk services for only one node in the cluster and not for the entire cluster. For example, in a three-node cluster, a limit of two connections allows six total connections.

Making Disk Service Available Using the Menu

The menu offers an easy way to set up applications on virtual disks and make them available to users.

Applications stored on a virtual disk allow read and write access to only one user at a time. For applications that require read-write access for more than one user, use a file service instead.

To make applications available, follow procedures explained in the next section. Making applications available involves:

- Adding an application disk service
- Installing the application
- Making the application available as a read-only service to multiple clients

Adding Application Disk Services

Adding application services

To add an application disk service:

1. Create a backup copy of the application by copying the application diskettes as instructed by the manufacturer.
2. Select **Service Options** from the PCSA Manager Menu.
3. Select **Add Service** from the Service Options menu.
4. Select **Application Disk Service** from the Add Service menu.
5. At the prompt, enter a unique 1- to 25-character name for the application disk service, such as PC_APP.
6. At the prompt, enter the password for the service.

   Ensure security by using a password.

   Using a password, you restrict access to the application disk service.

   The server stores the password in the database. When users try to access the service, they are prompted for the password.

   The default is no password, which means that everyone can access the application on the disk service.
7. Select the size of an application virtual disk according to the:
   - Number of software applications you install on the disk
   - Size of each application

   Refer to the documentation accompanying the applications to determine the space requirements for the virtual disk you are creating.

The PCSA Manager Menu displays messages while:

- Creating and mounting the application disk service with read and write access
- Adding the service to the disk server's service database

An application disk service is initially mounted with read and write access so you can install the application.

For example, after adding the application disk service PC_APP, the PCSA Manager Menu displays the following messages:

```
%PCSA-I-CREATEDISK, creating SYS$SYSDEVICE:[PCSA.LAD]PC_APP.DSK
%PCSA-I-FORMATDISK, formatting disk, Size = 1.2MB, Allocation = 2400/2400
%PCSA-I-DISKCREATED, SYS$SYSDEVICE:[PCSA.LAD]PC_APP.DSK created

%PCSA-I-DISKMOUNTED, SYS$SYSDEVICE:[PCSA.LAD]PC_APP.DSK;1 mounted
%PCSA-I-MOUNTINFO, service name = PC_APP, server node = SRVR1

%PCSA-I-APPDISKMNTED, application disk service PC_APP mounted R/W
%PCSA-I-APPDISKINST, please install your software, and remount the service
read-only
```

Installing Applications on a Disk Service

After you add the application disk service, install the application by copying the application software to the disk service.

To install the application:

1. Backup the application diskettes by following the directions supplied by the manufacturer.

Connect to the disk service.

2. At a personal computer, connect to the application disk service with the USE command:

   ```
   USE ?: \\server_name\disk_service_name /virtual
   ```

   The **server_name** is the name of the server on which you are installing the application.

   The **disk_service_name** is the name of the disk service you used when you add the service.

   For example, use the following command to connect to the application disk service, PC_APP, on the server SRVR1:

   ```
   USE ?: \\SRVR1\PC_APP /virtual
   ```

   The client displays the drive connected to the service, for example drive I:

   ```
   Device I: connected to \\SRVR1\PC_APP
   ```

3. Install the application from the personal computer. Follow the application's installation instructions.

Set up a printer service.

4. Before running applications, make sure you have set up appropriate printer services on the server.

   Most applications work with a network printer. Some, however, require that you use a local printer for the application to print correctly. Others print only to the logical device, LPT1.

   For more information on setting up printer services, see Chapter 4.

   Note

   If applications require a program diskette to run, each user needs a program diskette in drive A.

Making Applications Available to Multiple Clients

After you install the application on a disk service, you must remount the service read-only to make it available to many users. Disk services that you added with the menu are mounted with read and write access for only one user.

When you remount the service, you can increase security by limiting the number of users who can read the service.

Remount the service to make it available to many users.

To make the application available to many users as a read-only service, follow these steps:

- Dismount the disk service
- Remount the service for read-only access

Dismounting the Disk Service

To dismount a disk service:

Dismounting disk services with the menu

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Modify Disk Service** from the Service Options menu.
3. Select **Dismount Disk** from the Modify Disk Service menu.
4. At the service name prompt, enter the name of the disk service you are dismounting, such as PC_APP.
5. If the server is in a cluster, you are asked if you want to dismount the service from the cluster.

6. At the prompt, respond whether you want to dismount the service permanently.
7. At the prompt, respond if you want to purge the service from the service database.

Dismounting the disk makes it unavailable to clients.

8. At the prompt, confirm to dismount the disk.

   The DISMOUNT DISK command disconnects all clients and closes the disk service.

Remounting for Read-Only Access

To remount the virtual disk with read and write access:

Mounting virtual disk with the menu

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Modify Disk Service** from the Service Options menu.
3. Select **Mount Disk** from the Modify Disk Service menu.
4. At the prompt, enter the disk service's file name, such as PC_APP.
5. The default service name is the file name specified in step 4. To use a service name other than the default, enter the name at the prompt.

Ensure security by using a password.

6. At the prompt, enter the password to assign a password.
7. If the node is part of a cluster, respond if you want to mount the service clusterwide.

Write access limits access to one user.

8. Respond whether you want to mount the service with write access. Write access means only one user can connect to the service at a time.
9. Respond whether you want to mount the service permanently.
10. At the prompt, set the service rating.

    A **rating** is a numerical value that assigns a priority to a disk service. Use a rating to differentiate disk services with the same name. When several services have the same name, the disk service with the highest rating is used.

    The range is 1 to 65535.

    Refer to Assigning Priority to Identically Named Disk Services in this chapter for an explanation on how to use ratings.

Ensure security by limiting connections.

11. You are prompted for the number of connections. This question is asked only if you answered NO to step 8.
12. At the prompt, choose the service type: Application, Boot, System, or User.

    The service type defines the default location for the service. See Table 5–1 for a complete explanation of how to use the defaults.
13. Confirm to mount the disk.

Making Disk Services Available Using the Command Line

Virtual disks, which are stored on the server, provide fast access to DOS files. You make virtual disks available to users by mounting them. A mounted virtual disk is a **disk service**.

You can use the command line instead of the menu to make virtual disks available to users. Use the command line when you want to:

- Create virtual disks for individual users
- Define locations for virtual disks
- Limit space the disk occupies

A **personal disk service** gives users quick access to personal files. A disk service is well suited for personal use because only one user can read from and write to it at the same time.

To make disk services available to users, you need to:

- Create virtual disks
- Mount virtual disks as disk services

Creating Virtual Disks

When you create a virtual disk, you define its location and space allocation.

Defining a Location

Think about the location of virtual disks to help you organize them. You can organize directories for specific uses and store virtual disks in the appropriate directory. Or, you may want to organize virtual disks on different devices to evenly distribute requests for them.

You create a virtual disk in either default or explicit locations.

Using Default Locations

The server provides logicals that define default locations for virtual disks. To create a virtual disk in the default locations, use the /TYPE qualifier in the CREATE command.

Using default location for virtual disk

Table 5–1 shows each service type and the default directory for each type.

Table 5–1 Default Locations for Types of Disk Services

Disk Service Type	Virtual Disk Location
APPLICATION	LAD$APPLICATION_DISKS
BOOT	LAD$BOOT_DISKS
SYSTEM	LAD$SYSTEM_DISKS
USER	current default VMS directory

Default type is USER.

The default service type is USER. For example, to create a virtual disk in your default VMS directory, use the default /TYPE qualifier, as follows:

```
PCSA_MANAGER >  CREATE DISK MYSERVICE
```

Use the /TYPE qualifier to create the disk in the default application directory.

To create an application virtual disk in the default location for application disks, use the /TYPE qualifier as follows:

```
PCSA_MANAGER >  CREATE DISK MYAPP /TYPE=APPLICATION
```

The disk MYAPP.DSK is stored in the LAD$APPLICATION_DISKS directory.

When you mount the disk, use the same /TYPE qualifier that you use in the CREATE command.

Using Explicit Locations

You can also specify a directory in which to create a virtual disk. The directory overrides the value given with the /TYPE qualifier.

Creating a virtual disk in a specific directory

For example, to create a virtual disk MYDISK for User1's personal use in the directory DUA0:[USER1], enter the command:

```
PCSA_MANAGER>   CREATE DISK DUA0:[USER1]MYDISK
```

Make sure you have read and write access to the VMS directory you specify.

Limiting Virtual Disk Space

When you create a virtual disk, you define its size and its initial allocation. The size of the virtual disk is a maximum limit that the disk can ever occupy. The allocation limits the space initially allocated when you create the disk.

When you create a virtual disk, the disk is formatted for the size you specify. By default, the disk allocation equals its full size.

To conserve disk space, reduce the allocation by setting it between the minimum and maximum values shown in Table 5–2. Table 5–2 shows the disk sizes you can use and the allocation allowed for each size.

To use more disk space than you initially allocated, you need to extend the disk size (see Extending Virtual Disk Size).

Table 5–2 Space Allocation for Virtual Disks

Disk Size	Minimum Allocation	Maximum Allocation
360 KB	12	720
720 KB	14	1440
1.2 MB	29	2400
1.44 MB	33	2840
5 MB	66	10240
10 MB	16244	20480
20 MB	16244	40690
32 MB	16244	65535
64 MB	16633	131702
128 MB	32977	262144
256 MB	65665	524288
512 MB	65921	1048576

Note

To access virtual disks larger than 32 MB, users need to use DOS V4.0 or later.

For example, to allocate only 1800 blocks of the 1.44 MB reserved in the following command, enter:

```
PCSA_MANAGER> CREATE DISK DUA0:[USER1]USER1 /SIZE=1.44 /ALLOCATION=1800
```

Mounting Virtual Disks

After you create the virtual disk, make it available by mounting it. Once mounted, the disk is available to users as a **disk service**.

Mount a disk to make it available to clients.

When you mount a virtual disk, you can:

- Define access as read-only or read-write
- Restrict access by assigning a password
- Limit the number of connections to a read-only service
- Make it available temporarily or permanently

Note

To mount a virtual disk, you need write access to the virtual disk or OPER and SYSPRV privileges.

When you mount a virtual disk, its default location is defined by the /TYPE qualifier (see Creating Virtual Disks.)

Defining Access

Default = 30 users

When you mount a virtual disk from the command line, by default, 30 users can read from the disk service but not write to it.

To mount a virtual disk with read and write access for one user, enter:

```
PCSA_MANAGER> MOUNT DISK MYSERVICE /ACCESS=WRITE /TYPE=APPLICATION
```

Assigning a Password

To assign a disk service password, use the MOUNT command.

Use the /PASSWORD qualifier to ensure security.

For example, to mount the virtual disk USER1.DSK with a password NOENTRY, enter the following command:

```
PCSA_MANAGER> MOUNT DISK USER1.DSK /PASSWORD=NOENTRY
```

Limiting Connections to Read-Only Services

To ensure security, limit the connections to read-only services. (Write access is automatically limited to one user.)

Ensure security by limiting connections to a disk service.

For example, to limit the connections to the disk service MYSERVICE to 3, enter:

```
PCSA_MANAGER> MOUNT DISK MYSERVICE /CONNECTIONS=3
```

Making a Disk Available Temporary or Permanently

You mount a disk either temporarily or permanently.

Mount disks temporarily for short-term storage. Temporary disks are mounted as long as the disk server keeps running. Permanent disks are mounted each time the server reboots.

Use the /PERMANENT qualifier for permanent mount.

By default, a virtual disk is mounted temporarily.

For example, to mount the virtual disk USER1.DSK permanently, enter the following command:

```
PCSA_MANAGER> MOUNT DISK USER1.DSK  /PERMANENT
```

Modifying Disk Services

After you mount disk services, you can change them by:

- Assigning a password
- Changing access
- Limiting connections
- Defining whether users can create, mount, and modify virtual disks
- Extending the virtual disk size
- Assigning priority

Assigning a Password

You can assign a password if you:

Assigning a password for a mounted disk service

- Forgot to assign a password when you mounted a disk service
- Want to change the disk service password

You can assign a password to a mounted disk service. For example, to assign the password NOENTRY for the disk service MYSERVICE, enter:

```
PCSA_MANAGER>  SET DISK_SERVER SERVICE MYSERVICE/PASSWORD=NOENTRY
```

To remove a password from the disk service MYSERVICE, enter:

```
PCSA_MANAGER>  SET DISK_SERVER SERVICE MYSERVICE/NOPASSWORD
```

Changing Access

You can change access to a mounted disk service.

By default, applications you added using the menu allow read and write access for one user.

If you use the MOUNT command instead of the menu to make the service available, the default access is read-only for 30 users.

Whether you use the menu or the command line, you can change the default access or redefine the access.

For example, to modify the disk service MYSERVICE for read and write access:

1. Dismount the disk service MYSERVICE by entering:

   ```
   PCSA_MANAGER>  DISMOUNT DISK MYSERVICE
   ```

2. Remount the disk with read and write access. Enter:

   ```
   PCSA_MANAGER>  MOUNT DISK MYSERVICE /ACCESS=WRITE /PERMANENT
   ```

Limiting Connections to Disk Services

You can also limit the connections to a mounted disk service.

To limit the connections to 3 on a mounted service MYSERVICE, enter:

```
PCSA_MANAGER>  SET DISK_SERVER SERVICE MYSERVICE /CONNECTIONS=3 /PERMANENT
```

Defining Whether Users Can Mount Virtual Disks

By default, users can create, mount, modify and delete virtual disks when they have either of the following:

- Access to the VMS directory where they are creating the disk. For example, users can create virtual disks in their own VMS directories.
- VMS OPER and SYSPRV privileges.

You can disallow users to create, mount, modify and delete virtual disks.

By default, users are allowed to create, mount and delete virtual disks.

To find out whether users are allowed to perform these operations on virtual disks, enter:

```
PCSA_MANAGER> SHOW DISK_SERVER CHARACTERISTICS

Disk server characteristics:

Disk server request timeout : 90
All users may perform virtual disk functions.
PCSA_MANAGER>
```

To disallow users to create, mount, modify, and delete virtual disks, enter:

```
PCSA_MANAGER> SET DISK_SERVER CHARACTERISTICS /NOUSER_MOUNT
```

To retain this value each time the disk server starts, insert the SET DISK_SERVER CHARACTERISTICS /NOUSER_MOUNT command in the SYS$STARTUP:LAD_STARTUP.COM file.

Extending Virtual Disk Size

You can extend the size of a virtual disk beyond its initial allocation.

Suppose you create a virtual disk MYDISK with the following command:

```
PCSA_MANAGER> CREATE DISK DUA0:[USER1]MYDISK /SIZE=1.44MB /ALLOCATION=1800
```

Extend the size of the disk so that its total size is between its initial allocation and the maximum allocation shown in Table 5–2.

To extend the virtual disk MYDISK1 by 1000 blocks, enter:

```
PCSA_MANAGER> MODIFY DISK DUA0:[USER1]MYDISK1 /EXTEND=1000
```

The total disk size is 2800 blocks.

Assigning Priority to Identically Named Disk Services

A large network can offer several services of the same name, for example, the service SYMPHONY, containing the software for Lotus Symphony.

A rating assigns a priority to disk services with the same name.

Use a disk service rating to control which service users access among identically named services. A **rating** is a numerical value that assigns a priority to a disk service. With services of the same name, the disk service with the highest rating is used.

Assign a higher rating to service on a server that is more reliable or faster than others in the network.

For example, assign a higher rating to the Symphony service on SRVR1 and a lower rating to the Symphony service on the other servers.

Requests for services with the same name and rating are dynamically distributed in the network.

When identically named services have equal ratings, requests for the services are dynamically distributed. The service most accessible at the time of the request is used.

Assigning Ratings to Disk Services

To change the disk service rating of service Symphony on SRVR1:

Display disk service ratings

1. On the node SRVR1, display the rating for the disk service Symphony by entering:

   ```
   PCSA_MANAGER>  SHOW DISK_SERVER SERVICE/SERVICE=SYMPHONY
   ```

   The server displays:

```
Disk Server Services:

Service name  Type  Server  Limit  Users  Acc  Rating  Status
------------  ----  ------  -----  -----  ---  ------  -------------
SYMPHONY      APPL  SRVR1       1      2  RW        1  MNT  PERM
```

   Before changing the rating, check whether the disk service is mounted, which is indicated by "MNT" in the display.

2. Compare the rating of Symphony on SRVR1 to the rating on other servers, for example SRVR2 and SRVR3.

   To see the rating of the other Symphony services, log in to each server that offers the service. For example, log in to SRVR2 and then enter:

   ```
   PCSA_MANAGER>  SHOW DISK_SERVER SERVICE/SERVICE=SYMPHONY
   ```

The server displays:

```
Disk Server Services:

Service name  Type  Server  Limit  Users  Acc  Rating  Status
------------  ----  ------  -----  -----  ---  ------  -------------
SYMPHONY      APPL  SRV2        1      1  RW        5  MNT  PERM
```

3. On SRVR1, change the rating for Symphony to the highest rating. The highest rating is 65535. The default rating is 1. Enter:

```
PCSA_MANAGER>  SET DISK_SERVER SERVICE SYMPHONY /RATING =65535
```

When users try to connect to Symphony, the request goes to the service with the highest rating, that is the service on SRVR1.

Making Disk Services Unavailable

To make a disk service unavailable and delete its contents, you need to:

- Dismount the disk service
- Delete the virtual disk

This section describes how to make disk service unavailable by:

- Using the menu
- Using the command line

Using the Menu

Using the menu, you can do both tasks in one menu option, as follows:

Note

Before deleting a virtual disk, make a backup copy of the files in the service (see Chapter 9.)

Use the menu to delete the virtual disk.

1. Select **Service Options** from the PCSA Manager Menu.
2. Select **Delete Disk Service** from the Service Options menu.
3. Select **Application Disk Service** from the Delete Disk Service menu.
4. Select the disk service you want to delete.

Using the Command Line

You can also perform each step separately using the command line. For example, you may want to dismount but not delete a disk service before you back it up.

You can also use the command line.

You can use the command line to:

1. Dismount the disk service
2. Delete the virtual disk

Dismounting Disk Services

Dismounting makes the disk service unavailable to clients without deleting the contents of the virtual disk.

For example, to dismount the disk service MYDISK, enter:

```
PCSA_MANAGER> DISMOUNT DISK MYDISK
```

Deleting the Virtual Disk

If the contents of a virtual disk are no longer needed, you can delete the disk to make space available for other uses.

To delete a virtual disk, use the DELETE DISK command.

Before deleting a virtual disk, make a backup copy of the files in the service (see Chapter 9.)

Caution

Specify the directory of the virtual disk. Otherwise, the server tries to delete the virtual disk from your default VMS directory.

For example, to delete User1's personal virtual disk from the directory [USER1] on the device DUA0, enter:

```
$ PCSA_MANAGER> DELETE DISK DUA0:[USER1]MYDISK.DSK
```

Accessing Files Within a Virtual Disk from VMS

From DOS, clients can access files within a virtual disk. From the VMS operating system, you can also access the files within a virtual disk by using the PCDISK utility.

The PCDISK utility provides file management for virtual disks and other devices that are formatted on DOS and accessible from VMS. For example, the PCDISK utility lets you read a DOS diskette from the VMS floppy drive.

This utility is a command-line interface that resembles DOS. With PCDISK, you can perform the following functions:

- Copying files between virtual disks
- Listing files
- Transferring files between virtual disks and VMS

How to run the PCDISK utility

To run the PCDISK utility, enter:

```
$ RUN SYS$SYSTEM:PCDISK
```

After the PCDISK prompt is displayed, you need to connect the virtual disk that contains the files you want to reference. You connect the virtual disk with the USE command. For example, to connect the virtual disk MYDISK.DSK to drive A, enter:

```
$ RUN SYS$SYSTEM:PCDISK
PCDISK> USE A: MYDISK.DSK
A:\>
```

Then, to display the contents of the DOS device A, enter:

```
$ RUN SYS$SYSTEM:PCDISK
PCDISK> USE A: MYDISK.DSK
A:\> DIR
```

For more information on the PCDISK utility, see *Server Administrator's Commands Reference.*

6

Managing Users and Groups

The next step in managing services is to set up users and groups. First, add users to the system and then set up groups. A **group** is a collection of users who share access to file services.

Adding a user creates a:

Adding a user creates an account that users connect to from their PCs.

- User account on the server to which users connect by using the LOGON command at their personal computers
- AUTOUSER.BAT file in the user's account that is run automatically when users connect to their accounts

  When you add a user, you can customize the AUTOUSER.BAT file to include:

  - DOS commands specific for each user
  - Connections to services on the network

Add groups so users can share access to file services.

After users have an account, you can assign them to groups. By using groups, you assign access to all users in a group with only one command.

After you add users and groups, grant them access to services, as discussed in Chapter 3. Granting access is necessary before users can connect to services.

This chapter describes how to manage users and groups.

Managing Users

Managing users involves:

- Adding user accounts
- Modifying the AUTOUSER.BAT file in user accounts
- Moving user accounts
- Deleting user accounts

- Managing security in user accounts
- Managing the default account

Adding User Accounts

When you add a user, a VMS account is automatically created.

Adding a user automatically creates a VMS account, which is an an entry in the User Authorization File (UAF), with the following VMS properties:

- A VMS directory associated with the account
- PCFS$USER identifier used for identification and associated with the account

Note

Users added with the Add User command or menu option are **registered users**.

Appendix C contains a sample User Profile Form that you can use as a guide to collect the necessary information about a user.

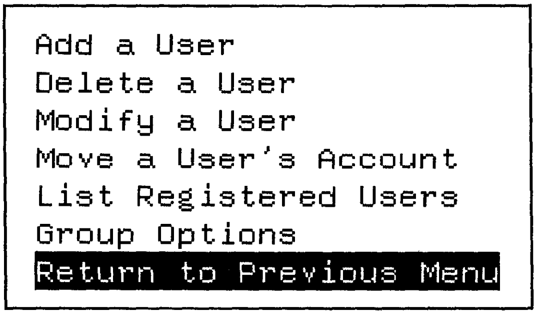
The procedure that follows shows you how to add user accounts.

To add a user:

Adding a user

1. Select **User Options** from the PCSA Manager Menu. Figure 6–1 shows the menu selections.

Figure 6–1 User Options Menu



2. Select **Add a User** from the User Options menu.

Steps 4–7 add users without VMS accounts.

3. At the prompt, enter the VMS username for the user.

   If the user already has a VMS account, skip to step 8.

4. At the password prompt, enter the user's password.

   You can accept the default password, WELCOME, and let individual users set their own passwords.

   The password has no expiration unless you set it. Managing Security in User Accounts in this chapter describes how to set a password expiration date.

5. At the prompt, enter the path for the user's account.

   The path for the account consists of a device name followed by a directory name.

   For example, to specify a path with the device name SRVR1 and the directory name USER1, enter:

   ```
   SRVR1:[USER1]
   ```

6. At the prompt, enter the file version limit for the user's account.

   The **file version limit** is the number of versions of a VMS file that are saved in a user's VMS account. It does not apply to files created in DOS or OS/2.

   A file version limit helps users who access files in their user accounts from VMS. For example, suppose you set User1's file version limit to 100. When User1 edits a file in her VMS account, she can keep up to 100 versions of the file. However, in DOS or OS/2, she can keep only one version of the file.

   The default file version limit is 1. You can accept the default, or you can specify a file version limit from 1 through 32,767.

   If you select a file version limit of 1, you can change it later by using the VMS SET FILE/VERSION_LIMIT command.

   You can also change the version limit for the entire directory by using the VMS SET DIRECTORY command.

7. At the prompt, respond whether you want to allow interactive logins.

   This prompt is not displayed for the PATHWORKS Server 3100 system.

Interactive login allows the user to log in to her account from any terminal or from any personal computer in the network.

8. The following prompts ask you for service names. Select services the user wants to connect to automatically when logging on to the user account from a personal computer.

   The services you select are included in the user's AUTOUSER.BAT file.

   The services you select are included in the user's AUTOUSER.BAT file.

   Note

   Before the user connects to the service, make sure the user is granted access to the service. (For information on granting access, see Chapter 3.)

   At the prompt, select a common directory.

   The list of common file directories displayed includes any common file services you added to the server. If there are no common file services, NONE is displayed.

   Note

   For PATHWORKS Server 3100 systems, the common file service PCCOMMON is automatically added to the server as part of the installation procedure and is included in this list.

   To add a common directory that is offered on a different server on the network, select **-Other Service-**.

   Selecting a common directory on a different server

   If you select -Other Service-, enter the:

   - Node name for the server that offers the common file service you want the user to be able to access.
   - Name of the common file service you want the user to connect automatically.

   Select application file services.

9. At the prompt, select file service application(s) for the user.

   The list of applications displayed includes any application file services you added to the server using the Add Service option, Application File Service.

Selecting applications on a different server

To select an application file service that is offered on a different server on the network, select **-Other Service-**.

If you select -Other Service-, at the prompts, enter the service's node name and file service name, as you did for a common file service.

When you have finished, select **Finished selecting applications**.

Select application disk services.

10. At the prompt, select disk service application(s) for the user.

    The list of applications displayed includes any application disk services you added to the server using the Add Service option, Application Disk Service.

Selecting applications on a different server

To select an application disk service that is offered on a different server on the network, select **-Other Service-**.

If you select -Other Service-, at the prompts, enter the service's node name and file service name, as you did for a common file service.

When you have finished, select **Finished selecting applications**.

Selecting printer services

11. At the prompt, select printer services for LPT1, LPT2, and LPT3. This prompt also is displayed for LPT2 and LPT3.

    The list of printer services displayed includes those you added with the Add Service option, Printer Service.

Selecting printer services on a different server

To add a printer service that is offered on a different server on the network, select -Other Service-.

If you select -Other Service-, enter the service's node name and service name at the prompts.

Make sure the user has the access to the printer service before connecting to the service.

Note

To allow PC users to print screen graphics using the Shift and Prt Sc (Print Screen) keys, you must edit the GRAPHICS command line in the AUTOEXEC.BAT file to include the printer type.

The AUTOEXEC.BAT file is in the root directory of the client boot device.

For information on the GRAPHICS command, see your DOS manual.

Select a language for PCSA applications.

12. At the prompt, select the default language, which specifies the language for PCSA applications. To use a language other than English, select a language here.

13. Respond whether you want to use EDT to edit the AUTOUSER.BAT file. You can edit the AUTOUSER.BAT file to:

Include DOS commands in the AUTOUSER.BAT file.

    - Include DOS commands from a command file on the server node. (Use the include file command that comes with your editor.)
    - Add any DOS commands to be run when a user runs LOGON to connect to the user account from a personal computer. For example, you can add a new directory to the user's path.
    - Include group codes, which are explained in Chapter 7.

    Press Ctrl/Z and enter EXIT to save the edits and return to the **Add a User** menu selection.

    You can use your own EDT initialization file instead of the initialization file supplied. To use your own file, define the logical PCSA$EDITOR_COMMAND to point to your initialization file. Then, add the logical definition to your LOGIN.COM file.

Modifying the AUTOUSER.BAT File in User Accounts

You can edit the user's AUTOUSER.BAT file in the user account to change:

- Connections to services
- Other commands that are run automatically when the user runs the LOGON command to connect to the user account from a personal computer

To modify the AUTOUSER.BAT file:

Changing the AUTOUSER.BAT file

1. Select **Modify a User** from the User Options menu.
2. At the prompt, enter the VMS username of the user whose AUTOUSER.BAT file you want to change.
3. At the prompt, respond whether you want to use EDT to edit the AUTOUSER.BAT file. Enter **Y** to edit the file.
4. When you are finished editing the file, save it and exit the editor.

Moving User Accounts

You may want to change the disk where a user account is stored in the following situations:

- You are adding new disks on the server
- Disk space is low on the disk of the user account

Note

When you move a user account, open files are backed up.

You cannot move an account for a user with an active VMS process.

Before you move a user account, you need to:

- Understand how disk quotas are determined for the disk to which you are moving the account
- Check connections to file services
- Check whether virtual disks in the user account are mounted or dismounted

Understanding How Disk Quotas Are Determined

When you move a user account to a disk with a disk quota, a disk quota for the user is determined. The amount of disk space available to each user is called **DISKQUOTA**.

Table 6–1 shows the resulting DISKQUOTA for a user account on the new disk.

When you successfully move a user account, the previous DISKQUOTA on the user's old disk is deleted.

Table 6–1 Disk Quota on a New Disk

If DISKQUOTA Is Enabled for User		
On Original Disk	**On New Disk**	**Resulting DISKQUOTA for User on the New Disk**
N	Y	The DISKQUOTA record on the new disk preserves the original overdraft and is the larger of: • DISQUOTA for user on the new disk • Size of the user's directory and its subdirectories
Y	N	The DISKQUOTA record from the original disk is carried over to the new disk unchanged.
Y	Y	The DISKQUOTA record on the new disk preserves the original overdraft and is the larger of: • DISKQUOTA for user on the new disk • Size of the user's directory and its subdirectories
N	N	The size of the user's directory and all its subdirectories is computed. That size plus 1000 is the size in blocks of the new DISKQUOTA. Overdraft is 0. [1]

[1] PATHWORKS for VMS can preserve overdraft that already exists for user accounts, but cannot create overdraft for new accounts.

Overdraft is the amount beyond the DISKQUOTA that the user can exceed.

To display or change the current disk quota, use the VMS DISKQUOTA command (see *VMS System Manager's Manual).*

Checking Connections to File Services

Before you move a user account, check whether users are connected to directories or subdirectories associated with the account:

- Connections to *registered* file services in the directory or subdirectories for the user account are stopped automatically.

  For example, if the registered file service PUBLIC points to a directory DUA0:[USER1.PUBLIC], and you are moving User1's account, then users connected to the service PUBLIC are disconnected.

Disconnect clients from unregistered file services in the user account.

- If clients are connected to *unregistered* file services in a directory (or subdirectories) for the user account, you need to disconnect the clients before moving the account:

  1. Determine if any users are connected to the directory of the user account:

     ```
     $ PCSA SHOW FILE_SERVER CONNECTIONS /FULL
     ```

     Example 6–1 shows a sample display of file service connections.

Example 6–1 Connections to File Services

```
File Server connections:

Connect ID  Client  User name     Alias name    Service name  Acc
----------  ------  ------------  ------------  ------------  ---
     65536  MELLO   USER1                        PERSONAL      R
            Root = $1$DUS6:[USER1]
     65537  MELLO   PCFS$ACCOUNT  LN03D2_LJ1$PS
                                                LN03D2_LJ1$PS
```

The text following “Root =” shows the device and directory to which each user has connected. You use the Connect ID to disconnect the service.

2. Broadcast a message telling the users to refrain from connecting to their directory until the Move User operation is complete.
3. If you are moving User1’s account, disconnect User1 from the root directory $1$DUS6:[USER1]. Enter:

   ```
   $ PCSA STOP FILE_SERVER CONNECTION /ID=65536
   ```

Note

Although you have stopped connections, a client who tries to access a disconnected file service is automatically reconnected to that service.

Checking Virtual Disks

After you move a user account, check whether virtual disks in the directory of the user account are mounted or dismounted:

- Mounted virtual disks in the directory for the user account are automatically dismounted. After you move the user account, the virtual disks are remounted and their location updated in the database.

- If you are moving a user account in which virtual disks has been:

  - Mounted permanently

  - Dismounted, with the /NOPERMANENT qualifier

  Then, you need to dismount the disk with the /PERMANENT qualifier.

  For example, if you are moving User1's account, which contains the virtual disk MYDISK.DSK, do the following:

  a. Run the following command:

  ```
  $ ADMIN/PCSA SHOW DISK_SERVER SERVICE
  ```

  Check the information under the Status column to see if MYDISK.DSK has been dismounted temporarily:

```
Disk server services:

Service name  Type  Server           Limit  Users  Acc  Rating  Status
------------  ----  ---------------  -----  -----  ---  ------  -------------
MYDISK        USER  SERVR1  30      1  RO        1  DISMNT PERM
MSWINV21      USER  SERVR1  30      0  RO        1  MNT PERM
```

  For example, DISMNT PERM means that MYDISK has been permanently mounted, but temporarily dismounted.

  b. If MYDISK has been permanently mounted and temporarily dismounted, dismount MYDISK permanently:

  ```
  $ ADMIN/PCSA DISMOUNT DISK MYDISK /PERMANENT
  ```

  c. Remount the virtual disk using the new location for the user account.

  For example, if you are moving User1's account from DUA0 to DUA1, enter:

  ```
  $ ADMIN/PCSA MOUNT MYDISK DUA1:[USER1] /PERMANENT
  ```

Moving a User Account

Now that you have checked connections to file services and virtual disks, you can move a user account.

To move User1's account from the disk DUA0 to DUA1:

1. Display a list of valid devices by entering:

   ```
   $  SHOW DEVICE
   ```

   Example 6–2 shows a sample display of the VMS devices on the server.

Example 6–2 Device Names

```
Device                  Device           Error    Volume         Free  Trans Mnt
 Name                   Status           Count     Label        Blocks Count Cnt
SRVR1$DUA0:              Mounted             0  SRVR1$SYS         23013   163   1
SRVR1$DUA1:              Mounted             0  SRVR1$USER        24162     4   1

Device                  Device           Error    Volume         Free  Trans Mnt
 Name                   Status           Count     Label        Blocks Count Cnt
SRVR1$MUA0:              Online              0
```

2. Select **User Options** from the PCSA Manager Menu.
3. Select **Move a User's Account** from the User Options Menu.

   The current location of the user account is displayed.
4. At the prompt, enter the name of the device where you want the account moved. Enter the device name in the VMS form. You can enter any one of the disks displayed in Example 6–2.

   For example, enter **DUA1:**

   ```
   Enter new device name:  DUA1:
   ```

When the command is successful, informational messages are displayed.

If the command is successful, you receive many messages indicating that the original account is being backed up and then deleted from the original disk.

If the command is unsuccesful, check the device names on the server, as explained in step 1.

If the Move User command ends prematurely

If the Move User command does not complete, for example, because of a system failure or user action, you need to check:

- That the DISUSER flag in the UAF is reset. (The DISUSER flag is normally set during the move user operation.)
- That the Device of the user's login directory is reset
- The old and new directories to determine how much of the directory was successfully copied
- Whether virtual disks in the user account are remounted. If not, you need to remount them.

Deleting User Accounts

By deleting a user account, you remove the user's access to services and to the user's account. Deleting a user removes VMS accounts that you created with the **Add a User** menu option or command in the PCSA Manager utility.

You cannot delete a user who was added with the VMS AUTHORIZE utility instead of the PCSA Manager utility.

To delete a user:

1. Select **User Options** from the PCSA Manager Menu.

Listing users

2. Select **List Registered Users** from the User Options menu.

   The list of registered users includes users added to the server by either the PCSA Manager Menu or PCSA Manager commands.

   Example 6–3 shows a sample list of registered users.

Example 6–3 Sample List of Registered Users

```
Registered users:

User name      UIC          Logins     Directory
-------------  ----------   --------   ---------------
SARRO          [301,323]    Disabled   USER1:[SARRO]
CHUNG          [320,324]    Disabled   USER:[CHUNG]
TEXAN          [330,325]    Disabled   USER1:[TEXAN]

Press RETURN to continue...
```

The following information is displayed for each user:

- User name —the VMS username for the user
- UIC—the VMS user identification code
- Logins—interactive login enabled or disabled for the user's account
- Directory—the location of the user's account (device name:directory name)

3. Select **Delete a User** from the User Options menu.
4. At the username prompt, enter the VMS username of the user you want to delete.

   Enter a registered user.

   If you enter a name that is not registered as a user, the PCSA Manager Menu displays the message, "User not registered".
5. Confirm if you are sure you want to delete the user you entered in response to the previous prompt.
6. At the prompt, respond whether to delete the user's directory and files.

   You can keep a user's files while deleting the user account.

   When you delete a user, you remove the user's entry in the user authorization file (UAF). You can, however, keep the directory and files and access them through the VMS operating system or associate them with a different user.

   Deleting a user removes the user's access to file services.

   When you delete a user, you also remove the user's individual or group access to file services.

Managing Security in User Accounts

After you add users, you need to manage security in their accounts. You manage security in user accounts by:

- Using the VMS security features for user accounts (Refer to *Guide to VMS System Security* for more information.)
- Setting a date for the password in a user's account to expire

Managing passwords involves:

- Setting a date for a user's password to expire
- Informing users, if possible, when their passwords are about to expire
- Changing user passwords

Setting a Password Expiration Date

You need to set a password expiration for user accounts that you created with the PCSA Manager Menu.

To set the password expiration date, use the VMS AUTHORIZE command.

Informing Users of Password Expiration

Clients running the RCV utility are notified before their passwords expire. (For information on configuring clients with the RCV utility, see *Client Installation and Configuration Guide for the VMS Server.*)

For clients running the RCV utility

Unless you change the notification time, a client is notified five days before the password expires and when the password expired.

You may want to change the notification time for users who do not often connect to the server. You can change the notification time by defining a parameter in the PCFS$STARTUP_PARAMS.DAT file.

The parameter defines the amount of notice (in days) the user recives before the password expires. Set the parameter to a value between 0 and 31. A value of 0 means that users are *not* warned before their passwords expire.

For example, to notify users 10 days before password expiration:

1. Edit the PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file. (The PCFS$STARTUP_PARAMS.DAT file is documented in Appendix F.)
2. Insert the following line into the file:

```
PCFS$PWD_EXP_NOTI = 10
```

For clients not running the RCV utility

Clients not running the RCV utility do not receive messages before or when their passwords expire.

It is a good idea for all user passwords to expire on the same date. Set the password expiration by using the AUTHORIZE command.

Changing Users' Passwords

Before their passwords expire, **users** can change their passwords by either:

- Using the NET PASSWORD command at their PCs
- Using the SET PASSWORD command in their VMS accounts

After their passwords expire, **you** need to change the passwords on VMS by either:

- Using the VMS AUTHORIZE command
- Logging in to each user account and then using the SET PASSWORD command

Managing the Default Account

A default account allows **all** users access to file services that are granted public. Any user without a VMS account on the server can connect to these file services. If you store confidential files, such as personnel files, on the server, you may want to limit access to ensure server security.

Ensure security by disabling the default account

You can restrict server access by:

- Disabling the default account.
- Granting limited access, for example, read-only to specific users. See Chapter 3.

To disable the default account, enter:

```
PCSA_MANAGER> SET FILE_SERVER CHARACTERISTICS /NODEFAULT_ACCOUNT
```

Like other VMS accounts, the default account has an entry in the VMS User Authorization File.

Chapter 3 describes access rights given to all users when they use the default account.

If you disable the default account, users need to specify their username and password when connecting to a file service granted PUBLIC.

You can also use the SET FILE_SERVICE CHARACTERISTICS command with the /DEFAULT_ACCOUNT qualifier to change the name of the default account.

Managing Groups

It is easy to give users common access to file services by using groups. You can give all users in a group access at once instead of one at a time.

You can allow certain groups access to some services while restricting other groups. For example, you can give the group LOTUS_READ read access to the file service LOTUS123. You can also give another group LOTUS_WR write access to the same service.

Managing groups includes the following tasks:

- Determining users who need common access rights
- Creating groups
- Granting group and public access to services
- Adding users to groups
- Removing users from groups
- Deleting groups

Determining Groups and Their Users

Determining required groups and members

Create a group for users who need the same type of access to a file service, such as an application service, or data files.

For example, suppose you have the following file services:

- LOTUS123, which contains the Lotus 1-2-3 application
- DATA123, which contains data files to be used with Lotus 1-2-3

Some users may need only read access to the service LOTUS123, which is sufficient to run the application. Other users need write access to the service DATA123.

In this situation, you can create the groups:

- LOTUS_READ, to read from the service LOTUS123
- LOTUS_WR, to write to the service DATA123

Granting groups access to file services

For the LOTUS123 service, assign read access to the group LOTUS_READ. For the DATA123 service, assign write access to LOTUS_WR.

Users can be in multiple groups.

Users can be members of more than one group. For example, a user could be a member of both LOTUS_READ and LOTUS_WR.

Note

Groups are different than the UIC group codes you define with the VMS AUTHORIZE command in the VMS User Authorization File (UAF).

Creating Groups

Use the PCSA Manager Menu to create a group:

You can perform the same tasks from the command line.

1. Choose **User Options** from the PCSA Manager Menu.
2. Select **Group Options** from the User Options menu.
3. Select **List Registered Groups** from the Group Options menu. This option displays the groups already created and their members.

   For example, a sample display might be:

   ```
   Registered groups:

   Group name            User name
   --------------------  ------------
   GROUP1                USER1
   GROUP2                <NO MEMBERS>
   GROUP3                USER5
   GROUP3                USER6

   Total of 3 registered groups
   ```

4. Select **Create a Group** from the Group Options menu to define a new group name. Group names must be ten characters or less.

   After you have defined the group name, follow the instructions to add users to groups.

Granting Group and Public Access to Services

After you create a group, you can grant group access to a file service.

You can grant access to group PUBLIC.

You can also grant the group PUBLIC access to a file service (see Chapter 3). All users are part of a default group named PUBLIC.

Public access to a file service means that users can connect to the service with the default account.

For example, to grant the group LOTUS_READ read access to the LOTUS123 service:

You can perform the same task from the command line.

1. Choose **User Options** from the PCSA Manager Menu.
2. Select **Group Options** from the User Options menu.
3. Select **Service Options** from the Group Options menu.
4. Select **Grant Group Access** from the Group Options menu.
5. At the prompt, select the service **LOTUS123**.
6. At the prompt, select the group **LOTUS_READ**.

For more information on granting groups access to file services, see Chapter 3.

Adding Users to Groups

When you add a user to a group, that user automatically receives the access you grant to the group.

To add users to groups, use the PCSA Manager Menu:

Add users with VMS accounts.

1. Make sure the user you are adding already has a VMS account. You can give the user a VMS account using the:
   - Add User option described in this chapter
   - VMS AUTHORIZE utility
2. Choose **User Options** from the PCSA Manager Menu.
3. Select **Group Options** from the User Options menu.
4. Select **Add Members to a Group** from the Group Options menu. A list of available groups is displayed.
5. Select the group to which you want to add a user.
6. Enter the name of the user you want to add to the group.

Removing Users from Groups

After you grant group access to a file service, an individual user in the group may no longer need it. Then, you can remove the user from a group.

To remove a user from a group:

1. Choose **User Options** from the PCSA Manager Menu.
2. Choose **Group Options** from the User Options menu.
3. Choose **Remove Members from a Group** from the Group Options menu. A list of groups is displayed.
4. Select the group from which you want to remove a user. A list of group members is displayed. To remove a user from all groups, select **All Groups**.
5. Choose the user you want to remove from the group or all groups.

Deleting Groups

After your server has been running for a while, a group may no longer be needed. In this case, you can delete the unnecessary group.

When you delete the group, all users in the group are no longer allowed access to the file service through that group.

To delete a group:

1. Choose **User Options** from the PCSA Manager Menu.
2. Choose **Group Options** from the User Options menu.
3. Choose **Delete a Group** from the Group Options menu. A list of groups is displayed.
4. Select the group you want to delete.

7

Reconfiguring the Server

The server configuration limits the number of:

- Clients that can connect to the server at the same time
- Disk services that can be in use simultaneously

Because users' demands change over time, you may need to adjust the configuration periodically. For example, you may need to add more clients so more users can connect to the server. Because additional clients and disk services use system resources, you do not want to configure the server for more clients or disk services than are actually needed. Therefore, changing the configuration can also mean decreasing the number of clients or disk services.

Changing server configuration can affect VMS resources.

Changing the server configuration and adding layered products affects resources available for the VMS operating system. When you configure the server, the VMS resources are checked and you are prompted to change them, if necessary. If you add layered products, reconfigure the server to ensure that adequate system resources are available.

Changing the server configuration can also affect performance. After you reconfigure the server, you may need to tune for performance, as explained in Chapter 8.

This chapter describes how to reconfigure the:

- File server to change the number of clients

  (Clients are referred to as workstations in the software.)
- Disk server to change the number of disk services
- Local Area System Transport software to change group codes and disk server timeout

Reconfiguring the File Server

Reconfiguring the file server entails:

- Displaying the current configuration
- Changing individual parameters, such as the number of clients
- If necessary, changing system parameters and:
    a. Running the AUTOGEN procedure
    b. Restarting the VMS operating system
- Restarting the file server

Note

Before changing the configuration, make sure that:

- You have CMKRNL, NETMBX, OPER, SYSPRV, TMPMEX, and WORLD privileges
- The MODPARAMS.DAT file, if present, is located in the SYS$SPECIFIC:[SYSEXE] directory

Displaying the Server Configuration

To display the file server configuration:

1. Start the PCSA Manager Menu by entering:

```
$ ADMIN/PCSA MENU
```

2. Select the **Utility Options** menu from the Main menu.

Display the current server configuration.

3. Select the **Configure Server Parameters** option from the Utility Options menu.

   Example 7–1 shows a sample configuration.

Example 7–1 File Server Configuration

```
Number of workstations     [   30]   File extent in blocks       [  256]
Cache size in pages        [ 1024]   Cache buffer size in bytes [ 8192]
Enable open file caching ? [    N]   File close delay in seconds[   15]
```

The parameters, which are displayed on the screen, are defined in the PCFS$STARTUP_PARAMS.DAT file. Appendix F describes each parameter and its function.

For example, the number of clients, which is displayed as Number of workstations, corresponds to the PCFS$NUM_OF_WORKSTATIONS parameter in the data file.

Most parameters, such as cache size, affect performance. See Chapter 8 for a description.

Changing the Server Configuration

To change the file server configuration:

1. Use the cursor keys to move through the fields to the value you want to change:
   - Press Ctrl/H for help on a selected parameter.
   - Press Backspace to delete the character at the cursor position.
   - Press Ctrl/Z to quit without saving.
   - Press Ctrl/E to save the new values.
2. When you save the configuration, informational messages are displayed that describe one of the following situations:
   - Configuration is saved

     If you receive a message indicating that the configuration is saved, you have successfully configured the server. Follow the directions in Restarting the File Server.
   - System parameters are insufficient

     To change system parameters, follow the directions in Changing System Parameters.

- System page file is insufficient

  To change the page file size, follow the directions in Changing the System Page File.

Note

Because changing the configuration affects run-time parameters that are required for the file server, new run-time parameters are computed.

These parameters are stored in the PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file, which is listed in Appendix F.

Changing System Parameters

If you receive the following messages, you need to change system parameters to support the new configuration:

```
              ******************************************
              *    System parameters are insufficient  *
              ******************************************

          System parameters need to be changed to support the
          new configuration.

View the changes needed for the system parameters ? [YES or NO]: (YES)
```

1. You are asked if you want to view the changes to the system parameters.
2. You are asked if you want to change the system parameters.

   If you do not want to change the system parameters, you need to change the configuration until the required system parameters are acceptable. Keep in mind that the required parameters are computed from a snapshot of system resources in use while you complete the menu option.
3. You are asked if you want to edit the system parameter file. If you choose to edit, the system parameter file is displayed with the EDT editor. You do not have to make changes to the file if you do not want to.

   To exit the EDT editor, press Ctrl/Z and enter:

   ```
   *EXIT
   ```

Additional VMS system pages may be needed.

4. When you change the configuration, the VMS system page file is checked. If the following message is displayed (the page file size and log file location may vary), the system does not have enough free pages for the new configuration:

```
To start the file server with the new configuration, you must
     save the new configuration and:

                     > Exit the PCSA Manager menu, and
                     > Run @SYS$UPDATE:SWAPFILES
                     > AUTOGEN the system, and
                     > REBOOT the system

      When you run @SYS$UPDATE:SWAPFILES, change the page file size.
      The current page file size is 13592; the required size is 19306.
      These values are also recorded in DKA700:[PCSA]PCFS$STARTUP_PARAMS.LOG.

   If you do not want to save the new configuration, you should quit now.

      Do you want to save the new configuration ? [YES or NO]: (YES)
```

   Follow the steps displayed on the screen, being sure to exit the PCSA Manager Menu before continuing.

5. If you do not receive an insufficient page file message in step 4, a message is displayed indicating that when you save the configuration, you must also run AUTOGEN and reboot the system.

   You can:

   - Save the configuration
   - Quit without saving the new configuration

6. You are prompted to run AUTOGEN and reboot the system. When you reboot, the system shuts down.

   If you do not want to reboot now, you can run AUTOGEN now and reboot later. However, you must reboot before restarting the file server.

7. If the file server does not start automatically when you reboot the system, you need to start it.

   To determine if the file server is already started:

   a. Start the PCSA Manager utility by entering:

      ```
      $ ADMIN/PCSA
      ```

   b. Enter the SHOW VERSION command:

      ```
      PCSA_MANAGER> SHOW VERSION
      ```

A display similar to the following indicates whether the file server is started:

```
LAD$KERNEL version  : Not available
LADDRIVER  version  : Not available
PCFS_SERVER version : Not available
PCSA_MANAGER version: PCSA_MANAGER V4.1
```

If the display indicates that the PCFS_SERVER version is not available, you need to restart the server. Follow the directions in Restarting the File Server.

Changing the System Page File

When you change the configuration, the VMS system page file is checked. If the following message is displayed, the system does not have enough free pages for the configuration:

```
To start the file server with the new configuration, you must
      save the new configuration and:

                  > Exit the PCSA Manager menu, and
                  > Run @SYS$UPDATE:SWAPFILES
                  > REBOOT the system

      When you run @SYS$UPDATE:SWAPFILES, change the page file size.
      The current page file size is 13592; the required size is 19306.
      These values are also recorded in DKA700:[PCSA]PCFS$STARTUP_PARAMS.LOG.

   If you do not want to save the new configuration, you should quit now.

      Do you want to save the new configuration ? [YES or NO]: (YES)
```

Follow the steps on the screen, being sure to exit the PCSA Manager Menu before continuing.

Restarting the File Server

Restart the file server for the new configuration to take effect:

1. Exit the PCSA Manager Menu, if necessary, to get to the VMS operating system prompt ($).
2. Enter one of the following commands, depending on the transport you use:
   - For DECnet, enter:

     ```
     $ @SYS$STARTUP:PCFS_STARTUP DECNET
     ```

   - For TCP/IP, enter:

     ```
     $ @SYS$STARTUP:PCFS_STARTUP TCP
     ```

- For DECnet and TCP/IP, enter:

  ```
  $ @SYS$STARTUP:PCFS_STARTUP DECNET/TCP
  ```

3. If the file server does not start, read the startup log file PCFS$LOG_FILES:PCFS$STARTUP.LOG. The log file contains error messages that prevent the file server from starting. Enter:

   ```
   $ TYPE PCFS$LOG_FILES:PCFS$STARTUP.LOG
   ```

Reconfiguring the Disk Server

Reconfigure the disk server to change the maximum number of disk services.

The disk server provides 256 disk services by default. Servers with many network key disks may require more than the default number of disk services. A network key disk is a disk service used to boot a user's personal computer and is unique for each client.

Note

Before changing the configuration, make sure that:

- You have CMKRNL, NETMBX, OPER, SYSPRV, TMPMEX, and WORLD privileges
- The MODPARAMS.DAT file, if present, is located in the SYS$SPECIFIC:[SYSEXE] directory

Changing the maximum number of disk services

To change the maximum number of disk services, use the following procedure:

1. Edit the data file SYS$STARTUP:ESS$LAD_STARTUP.DAT, which is used when the disk server starts. The original file is shown in Appendix D.

   To increase the maximum number of disk services, you need to define a value for the MAXIMUM_SERVICES parameter in the data file. For example, to change the maximum services to 500, specify the desired value in the file:

   ```
   MAXIMUM_SERVICES = 500 !maximum disk services
   ```

Restart the disk server

2. For the change to take effect, restart the disk server. Restarting the disk server stops the server first. Enter:

   ```
   $ @SYS$STARTUP:LAD_STARTUP
   ```

Check the NPAGEDYN parameter

   Before the disk server starts, it checks that the VMS system resources are adequate for the new configuration. Changing the maximum disk services may require that you also change the VMS SYSGEN parameter NPAGEDYN.

3. If a message is displayed on the screen indicating that you need to change system parameters, you need to change them before the disk server can start:

   a. Append the PCFS$MODPARAMS.DAT file to the MODPARAMS.DAT file.

      The PCFS$MODPARAMS.DAT file contains the required SYSGEN parameters. The MODPARAMS.DAT file contains any SYSGEN parameters that you previously modified. Both files are stored in the SYS$SPECIFIC:[SYSEXE] directory.

      To append the files, enter:

```
$ APPEND SYS$SPECIFIC:[SYSEXE]PCFS$MODPARAMS.DAT SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT
```

   b. Run AUTOGEN and restart the VMS operating system before the new configuration can take effect:

      1. Start the PCSA Manager menu by entering:

         ```
         $ ADMIN/PCSA MENU
         ```

      2. Select the **Utility Options** menu.

      3. Select the **Autogen the system** option from the Utility Options menu.

      4. Follow the prompts to run AUTOGEN with reboot.

   c. If the disk server does not start automatically when you reboot the system, you need to restart the server now.

      1. Determine if the disk server is already started:

         a. Start the PCSA Manager utility by entering:

            ```
            $ ADMIN/PCSA
            ```

         b. Enter the SHOW VERSION command:

            ```
            PCSA_MANAGER> SHOW VERSION
            ```

A display similar to the following indicates whether the disk server is started:

```
LAD$KERNEL version  : Not available
LADDRIVER  version  : Not available
PCFS_SERVER version : PATHWORKS for VMS
PCSA_MANAGER version: PCSA_MANAGER V4.1
```

2. If the display indicates the LADDRIVER version is not available, you need to start the server:

    a. Exit the PCSA Manager utility.

    b. Start the server by entering:

    ```
    $  @SYS$STARTUP:LAD_STARTUP
    ```

Reconfiguring the LAST Software

You need to reconfigure the Local Area System Transport (LAST) software to:

- Change the disk server timeout

  When the server is heavily loaded by processing many requests for disk services, clients cannot access the disk services they request. Increase the amount of time available to process requests for disk services by increasing the **timeout** value.

- Configure servers with group codes in extended local area networks to restrict access to specific servers

Changing Timeout on the Disk Server

The initial timeout value is 90 seconds. To change the disk server timeout to another value, follow these steps:

1. Edit the ESS$LAST_STARTUP.DAT file.

The initial timeout value is 90 seconds.

2. To increase the timeout to 120 seconds, for example, insert the command in the file:

   ```
   TIMEOUT= 120
   ```

3. Stop the LAST software, as follows:

   a. Start the LASTCP utility by entering:

   ```
   $  MCR ESS$LASTCP
   LASTCP>
   ```

b. Stopping the transport disconnects all users from file or disk services. Before you stop the transport, display the active connections. Enter:

```
LASTCP> SHOW ACTIVE NODES
```

c. If no other users are using LAST, stop LASTCP. Enter:

```
LASTCP> STOP TRANSPORT
```

4. For the new timeout to take effect, start the file server and the disk server. Starting either server automatically starts the transport software.

   - To start the disk server, enter:

     ```
     $ @SYS$STARTUP:LAD_STARTUP
     ```

   - Start the file server as described in Restarting the File Server.

Configuring Servers with Group Codes

In an extended local area network with many services, users may not be able to access all the services offered. You can use group codes to restrict access to selected servers in the extended LAN so users can access the services they need.

Servers and clients must use the same group code to recognize each other.

Group codes are numerical identifiers you assign a server or a logical group of servers, for example, servers in the accounting group.

Clients must use the same group code to recognize a server in that group. For example, clients using the accounting group code recognize only those servers with the accounting group code.

A server can have only one group code, and a client can use only one group code at a time.

Note

Group codes are different from the groups you associate with users, described in Chapter 6.

Clients that remote boot use the group code 0 when they boot. After they remote boot, clients can use other group codes.

This section describes how to use the LAST software to:

- Configure group codes on the server and client
- Use group codes for servers and clients that remote boot

Configuring Group Codes on the Server and Client

To restrict server access to clients in the accounting group, assign the same group code to the server and the client. The following example shows how to assign group code 5 to both the server and client:

Configuring servers for group codes

1. Stop the disk and file server.
   - For the disk server, enter:

     ```
     PCSA_MANAGER>  STOP DISK_SERVER CONNECTIONS
     ```

   - For the file server, enter:

     ```
     PCSA_MANAGER>  STOP FILE_SERVER CONNECTIONS /ALL
     ```

2. Exit the PCSA Manager Menu.
3. Edit the file SYS$STARTUP:ESS$LAST_STARTUP.DAT. Find the line with a "GROUP = " statement and change it to read:

   ```
   GROUP=5
   ```

4. Stop the LAST software, as follows:
   a. Start the LASTCP utility by entering:

      ```
      $  MCR ESS$LASTCP
      LASTCP>
      ```

   b. Display the active connections to the transport, since stopping the transport disconnects all users from file or disk services. Enter:

      ```
      LASTCP>  SHOW ACTIVE NODES
      ```

   c. If no other users are using LAST, stop the transport. Enter:

      ```
      LASTCP>  STOP TRANSPORT
      ```

Restart the LAST software

5. Start the file server and the disk server. Starting either server automatically starts LAST, which enables group codes.

   - To start the disk server, enter:

     ```
     $  @SYS$STARTUP:LAD_STARTUP
     ```

   - Start the file server as described in Restarting the File Server.

Configuring clients for group codes

6. Configure clients to recognize group code 5 by adding a LAST command to each user's AUTOUSER.BAT file:

   a. Start the PCSA Manager Menu.

   b. Select the **User Options** menu.

   c. Select the **Modify a User** option from the User Options menu.

   d. At the prompt, enter the VMS username of the user whose AUTOUSER.BAT file you want to change.

   e. At the prompt, respond whether you want to use the EDT editor to edit the file. Enter **Y**.

   f. Using the EDT editor, insert the following command in the user's AUTOUSER.BAT file:

      ```
      LAST /G:5
      ```

7. Exit the editor, being sure to save the file.

Using Group Codes for Remote Boot Servers and Clients

A server offering remote boot must have a group code 0. To use group codes in a network where clients remote boot, you need one server that offers remote boot (group code 0) and a second server with another group code.

Clients that remote boot also use the group code 0 when they remote boot. After they remote boot, they can use a group code other than 0.

Setting group code at the client

For example, for a client to use group code 5 after remote booting, the user can enter:

```
F:\>  LAST/GROUP:5
```

If the remote boot node goes down, clients must use use group code 0 to reconnect to the network key disk and then reset the group code:

1. Start the client software with a group code 0:

   ```
   F:\>  LAST/GROUP:0
   ```

2. Connect to the network key disk by entering:

   ```
   F:\>  USE ?: 00-11-22-35-34-90
   ```

   Connecting to the network key disk boots the PC over the network.

3. Reset the group code to 5 by entering:

   ```
   F:\>  LAST /GROUP:5
   ```

8

Improving Server Performance

Increase cache to improve performance.

If server response is slow when users access services, you can adjust the server to improve performance. Increasing the cache size can yield a dramatic improvement in performance. **Cache** is physical memory on the VMS computer that is accessed at high speeds. The amount of available cache is limited by physical memory.

Maintaining a tuned server is a continual process, because demands for system resources change over time.

You need to tune the server for performance after you have configured the server. Because the server uses system resources such as memory, adding clients to the server configuration can adversely affect server performance. Conversely, increasing the cache size to its maximum can limit the number of clients in the server configuration.

Increasing cache takes away resources from the VMS operating system.

Adjusting the server to improve performance can also limit resources available to VMS users, such as memory.

Cache is a resource you configure on the file and disk servers. To increase the cache, use the same configuration process described in Chapter 7. When you increase cache, the configuration process ensures that enough resources are allocated to support the new cache configuration. Increasing cache may also require that you reallocate VMS resources, such as memory or CPU time.

If increasing cache no longer improves performance, then you have probably already tuned your server to its maximum efficiency.

This chapter describes improving performance by increasing cache and adjusting VMS system resources, if necessary. The topics discussed are:

- How cache works
- Improving performance on the file server

- Improving performance on the disk server
- Improving performance on the transport software

How Cache Works

Before tuning the server, you need to understand how the server uses cache.

In general, increasing the cache size improves server performance. The server stores files temporarily in cache memory. A file in cache can be accessed quickly, because it does not have to be accessed from the disk.

However, the performance of write operations improves **until** the volume of data written exceeds the write capacity of the current cache size. After the cache capacity is exceeded, the server has to reallocate cache buffers and performance declines.

Because files for applications are stored on the VMS server, there is significant overhead in opening and closing files. To reduce this overhead, you can store open files in cache. Using cache for open files is called **open file caching**. Many personal computer applications open and close files repeatedly in rapid succession. If a file in the open file cache is opened soon after it is closed, the file can be reopened quickly, because the file's data structures have remained in the cache.

Improving Performance on the File Server

To improve performance on the file server, follow these steps:

1. Collect server data, which records statistics of cache use.
2. Evaluate the data collected.
3. Display cache parameters.
4. Adjust cache parameters.
5. Change system parameters, if necessary, and:
   a. Run the AUTOGEN procedure.
   b. Restart the VMS operating system.
6. Restart the file server.
7. Change the file server's VMS priority.

Stream files are cached.

The file server uses cache for stream files only. **Stream files** are files whose records end with a carriage return. DOS files are stream files. VMS files can also be stream files.

Attaining better performance is an iterative process. The first step in improving performance is measuring the resources that the server actually uses. Collecting server data provides statistics on cache use. After you change cache parameters, you need to collect data again to evaluate whether changing the parameters actually improved performance.

When you change the cache parameters in the file server configuration, you need to restart the file server for the change to take effect.

Similarly, when you redefine VMS system parameters, you need to run the VMS program AUTOGEN to reconfigure the VMS operating system.

Collecting Server Data

Using the PCSA Manager Menu, you can collect data on server performance. The results of the collection are stored in a data file, which you use to decide whether to change the file server cache. The next section describes how to evaluate the data file.

Note

The cache counters, which are displayed using the command line, are initialized when you start the collection process.

Use the PCSA Manager Menu to collect server data, as follows:

1. Start the PCSA Manager Menu and select the **Utility** option.
2. Select the **Collect Server Data** option from the Utility menu.
3. When prompted, select the start time, stop time, and interval over which data is collected. The data file shows the effectiveness of the current cache configuration.

Evaluating the Data Collected

The data you collect are stored in an ASCII text file. Read the file to evaluate whether to change the file server cache after the collection period has completed. You defined the period over which data is collected when you collect server data.

To see the data you collected:

1. To display the data file, enter:

   ```
   $ TYPE PCFS$LOG_FILES:PCFS$CACHE_STATISTICS.TXT
   ```

2. The collection log file reports any problems that occur when you collect server data. To display a log of the collection program, enter:

   ```
   $ TYPE PCFS$LOG_FILES:PCFS$COLLECTOR.LOG
   ```

The data file reports the:

- Open file hit rate
- Cache hit rate
- Cache availability
- Average size of read packets requested
- Average size of write packets requested

An explanation of each field follows.

Example 8–1 displays a sample data file.

Open File Hit Rate

Open file caching keeps a file open in cache memory after the file has been closed.

The **open file hit rate** is the percentage of times a requested file is in cache.

To use open file caching, you need to enable it, as explained in Adjusting Cache Parameters.

Open file caching is most effective for applications, such as DOS batch files, that open and close the same file frequently. For these applications, open file caching limits the number of times files need to be opened and closed. Open file caching does not benefit applications that open several unique temporary files.

Example 8–1 Caching Display

```
PCSA PATHWORKS for VMS V4.1 - PCFS Server Statistics

Begin Collection Time :  27-JUN-1990 11:30
End   Collection Time :  27-JUN-1990 12:30
Collection Interval   :  15  mins

-----------------------------------------------------------------------------
|     Time Stamp     |Open File|  Cache   |    Cache     | Average RD | Average WR |
|                    |Hit  Rate|Hit  Rate|Availability|Request Size|Request Size|
-----------------------------------------------------------------------------
|27-JUN-1990 11:30 |       0 %|     62 %|       100 %|       2369 |       1185 |
-----------------------------------------------------------------------------
|27-JUN-1990 11:45 |       0 %|     61 %|       100 %|       2437 |       1198 |
-----------------------------------------------------------------------------
|27-JUN-1990 12:00 |       0 %|     61 %|       100 %|       2437 |       1198 |
-----------------------------------------------------------------------------
|27-JUN-1990 12:15 |       0 %|     61 %|       100 %|       2437 |       1198 |
-----------------------------------------------------------------------------
|27-JUN-1990 12:30 |       0 %|     61 %|       100 %|       2437 |       1198 |
-----------------------------------------------------------------------------
```

Many database applications keep files open in memory for the period of time the application is in use. Open file caching does not benefit these applications.

If the hit rate is under 70%, then open file caching is ineffective and you should disable it.

If the open file hit rate is 0%, check if open file caching is disabled.

Cache Hit Rate

The **cache hit rate** is the percentage of time that the data requested is already in the cache. The cache hit rate reflects read operations only. (Since data to be written is always copied to memory, the cache hit for data writes would always be 100%. Therefore, the cache hit rate does not include data writes.)

If the cache hit rate is under 70%, increasing cache size may improve performance.

Cache Availability

The cache availability shows the percentage of time cache memory is available when requested. For example, when a user opens a file, the file is read into cache buffers. If no cache buffers are available, the file server has to reorganize cache memory to make buffers available. Lack of available cache buffers causes overhead for the file server and detracts from file server performance.

If the cache availability is less than 80%, increase the cache size.

Average RD and WR Request Size

Average RD Request size and average WR request size are the average size of packets requested for read and write. These packets are transferred over the network between the client and the server.

Increasing the cache size may not improve performance for small packet sizes. Packets larger than 1024 bytes are large; packets smaller than 1024 are small.

Displaying Cache Parameters

To display the cache parameters:

1. Make sure that:
   - You have CMKRNL, NETMBX, OPER, SYSPRV, TMPMBX, and WORLD privileges
   - The MODPARAMS.DAT file, if present, is located in the SYS$SPECIFIC:[SYSEXE] directory
2. Start the PCSA Manager Menu by entering:
   ```
   $  ADMIN/PCSA MENU
   ```
3. Select the **Utility Options** from the Main menu.
4. Select the **Configure Server Parameters** option from the Utility Options menu.

   Example 8–2 shows a sample display of the server parameters.

Example 8–2 File Server Parameters

```
Number of workstations     [   30]   File extent in blocks      [  256]

Cache size in pages        [ 1024]   Cache buffer size in bytes [ 8192]

Enable open file caching ? [    N]   File close delay in seconds[   15]
```

A description of each cache parameter follows.

Cache Size in Pages

The cache size is the amount of physical memory, in pages, allocated for data caching. **Data caching** stores all data requested for input and output in the cache. Data caching reduces the overhead of waiting for disk access when the user requests to read or write to a file.

The minimum value is 512. The maximum value you can enter depends on the available physical memory.

Enable Open File Caching

Enable open file caching so that files are stored in the open file cache after they have been closed by the user.

You must specify “Y” or “N”.

File Extent in Blocks

The file extent defines the number of VMS disk blocks (512-bytes) that the file server allocates when it creates or extends a file. By default, files are extended in units of 256 blocks at a time when the file server opens a file.

Since extending a file takes a long time, you want to limit the number of times the file server needs to extend a file. To determine an appropriate value for this parameter, you need to consider:

- Average amount that files grow
- How often files grow

Extending a file uses up DISKQUOTA.

The file extent affects the VMS DISKQUOTA when DISKQUOTA is enabled. The VMS DISKQUOTA limits the amount of disk space available to users.

For example, if the file extent is 512, the server allocates 512 blocks to create a file and the available DISKQUOTA is reduced by 512 blocks. Suppose that only five blocks are needed for the file. When the file is extended, all 512 blocks are reserved for the file regardless of whether they are needed. Extending the file may exceed DISKQUOTA although the five blocks required for the file are available. When the file is closed, only the five blocks needed for the file are used.

The maximum value is 65536.

Cache Buffer Size in Bytes

Cache is divided into buffers. The buffer size determines the amount of data the file server reads or writes to the disk at a time.

Before changing the cache buffer size, make sure that you first evaluate and adjust the other cache parameters to improve performance. Although you do not need to change the buffer size often, you may consider changing it after adjusting the other cache parameters.

Use a small buffer size if users run applications that require less than 512 bytes of data at a time.

Applications that do many random reads benefit from small buffer size, if:

- Time between read requests is long
- One buffer does not satisfy the request for data

File Close Delay in Seconds

The file close delay is the number of seconds the server waits before actually closing a file. It is used with open file caching. When open file caching is enabled, a file remains in cache for the number of seconds specified in the file close delay.

You can change the file close delay only if open file caching is enabled.

A file is locked until the delay time has expired. When open file caching is enabled, a VMS user cannot access a file that is in the open file cache. If a VMS user tries to access a file in the cache, the following message is displayed:

```
file locked by another user, unable to open
```

The minimum value is 1 second; the maximum value is 99999 seconds.

Buffer sizes are 512, 1024, 2048, 3072, 4096, 8192, 16384, 32768, and 66536.

Adjusting Cache Parameters

Changing cache parameters

Now that you have examined the cache display, you may want to change how the file server uses cache. For example, you may want to turn open file caching on, or increase the size of the cache buffers.

To change any cache parameter on the file server:

1. Use the cursor keys to move through the fields to the value you want to change:
   - Press Ctrl/H for help on a selected parameter.
   - Press Backspace to delete the character at the cursor position.
   - Press Ctrl/Z to quit without saving.
   - Press Ctrl/E to save the new values.
2. When you save the configuration, informational messages are displayed that describe one of the following situations:
   - Configuration is saved

     If you receive a message indicating that the configuration is saved, you have successfully configured the server. Follow the directions in Restarting the File Server.
   - System parameters are insufficient

     To change system parameters, follow the directions in Changing System Parameters.
   - System page file is insufficient

     To change the page file size, follow the directions in Changing the System Page File.

Note

Because changing the configuration affects run-time parameters that are required for the file server, new run-time parameters are computed.

These parameters are stored in the PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file, which is listed in Appendix F.

Changing System Parameters

If you receive the following messages, you need to change system parameters to support the new configuration:

```
          ******************************************
          *    System parameters are insufficient  *
          ******************************************

     System parameters need to be changed to support the
     new configuration.

View the changes needed for the system parameters ? [YES or NO]: (YES)
```

1. You are asked if you want to view the changes to the system parameters.
2. You are asked if you want to change the system parameters.

   If you do not want to change the system parameters, you need to change the configuration until the required system parameters are acceptable. Keep in mind that the required parameters are computed from a snapshot of system resources in use while you complete the menu option.
3. You are asked if you want to edit the system parameter file. If you choose to edit, the system parameter file is displayed with the EDT editor. You do not have to make changes to the file if you do not want to.

   To exit the EDT editor, press Ctrl/Z and enter:

   ```
   *EXIT
   ```

Additional VMS system pages may be needed.

4. When you change the configuration, the VMS system page file is checked. If the following message is displayed (the page file size and log file location may vary), the system does not have enough free pages for the new configuration:

```
To start the file server with the new configuration, you must
     save the new configuration and:

                    > Exit the PCSA Manager menu, and
                    > Run @SYS$UPDATE:SWAPFILES
                    > AUTOGEN the system, and
                    > REBOOT the system

      When you run @SYS$UPDATE:SWAPFILES, change the page file size.
      The current page file size is 13592; the required size is 19306.
      These values are also recorded in DKA700:[PCSA]PCFS$STARTUP_PARAMS.LOG.

   If you do not want to save the new configuration, you should quit now.

      Do you want to save the new configuration ? [YES or NO]: (YES)
```

Follow the steps displayed on the screen, being sure to exit the PCSA Manager Menu before continuing.

5. If you do not receive an insufficient page file message in step 4, a message is displayed indicating that when you save the configuration, you must also run AUTOGEN and reboot the system.

   You can:

   - Save the configuration
   - Quit without saving the new configuration

6. You are prompted to run AUTOGEN and reboot the system. When you reboot, the system shuts down.

   If you do not want to reboot now, you can run AUTOGEN now and reboot later. However, you must reboot before restarting the file server.

7. If the file server does not start automatically when you reboot the system, you need to start it.

   To determine if the file server is already started:

   a. Start the PCSA Manager utility by entering:

      ```
      $ ADMIN/PCSA
      ```

   b. Enter the SHOW VERSION command:

      ```
      PCSA_MANAGER> SHOW VERSION
      ```

      A display similar to the following indicates whether the file server is started:

      ```
      LAD$KERNEL version   : Not available
      LADDRIVER  version   : Not available
      PCFS_SERVER version  : Not available
      PCSA_MANAGER version: PCSA_MANAGER V4.1
      ```

      If the display indicates that the PCFS_SERVER version is not available, you need to restart the server. Follow the directions in Restarting the File Server.

Changing the System Page File

When you change the configuration, the VMS system page file is checked. If the following message is displayed, the system does not have enough free pages for the configuration:

```
To start the file server with the new configuration, you must
      save the new configuration and:

                     > Exit the PCSA Manager menu, and
                     > Run @SYS$UPDATE:SWAPFILES
                     > REBOOT the system

      When you run @SYS$UPDATE:SWAPFILES, change the page file size.
      The current page file size is 13592; the required size is 19306.
      These values are also recorded in DKA700:[PCSA]PCFS$STARTUP_PARAMS.LOG.

   If you do not want to save the new configuration, you should quit now.

      Do you want to save the new configuration ? [YES or NO]: (YES)
```

Follow the steps on the screen, being sure to exit the PCSA Manager Menu before continuing.

Restarting the File Server

Restart the file server for the new configuration to take effect:

1. Exit the PCSA Manager Menu, if necessary, to get to the VMS operating system prompt ($).
2. Enter one of the following commands, depending on the transport you use:
   - For DECnet, enter:

     ```
     $  @SYS$STARTUP:PCFS_STARTUP DECNET
     ```

   - For TCP/IP, enter:

     ```
     $  @SYS$STARTUP:PCFS_STARTUP TCP
     ```

   - For DECnet and TCP/IP, enter:

     ```
     $  @SYS$STARTUP:PCFS_STARTUP DECNET/TCP
     ```

3. If the file server does not start, read the startup log file PCFS$LOG_FILES:PCFS$STARTUP.LOG. The log file contains error messages that prevent the file server from starting. Enter:

   ```
   $ TYPE PCFS$LOG_FILES:PCFS$STARTUP.LOG
   ```

Changing the File Server Priority

Now that you have adjusted system resources, you also need to consider processing speed. Effective performance in any system balances I/O operations and processing speed (CPU). Successful file server caching uses more resources for processing than for I/O requests.

The VMS priority defines how frequently the CPU is scheduled for a VMS process. The file server has a default VMS priority of eight. If the VMS server is a dedicated LAN server, you can allocate all your system resources to increase server performance. If, on the other hand, the server is used for other time-sharing applications, you do not want to use all your system resources for the file server.

If users have trouble accessing the VMS system for uses other than the file server, reduce the priority of the file server. However, note that decreasing the priority also degrades file server performance.

Note

Changing the file server priority in a cluster changes the priority of all servers in the cluster.

To lower the file server priority:

1. Edit the SYS$COMMON:[SYS$STARTUP]PCFS_STARTUP.COM file.
2. Find the PCFS$PRIORITY parameter and change the number eight to a lower priority.
3. Start the file server, as described in Restarting the File Server

Improving Performance on the Disk Server

Increase the cache size to improve performance on the disk server. At the same time, you need to ensure that the VMS system parameters can support increased cache.

Increasing the cache size should improve the **cache hit rate**, which is the percentage of time data requested is in the cache.

Note

Before changing the cache parameters, make sure that:

- You have CMKRNL, NETMBX, OPER, SYSPRV, TMPMBX, and WORLD privileges
- The MODPARAMS.DAT file, if present, is located in the SYS$SPECIFIC:[SYSEXE] directory

To increase the cache size:

1. Start the PCSA Manager Menu by entering:

   ```
   $ ADMIN/PCSA
   ```

2. Display the current cache hit rate by entering:

   ```
   $ PCSA_MANAGER> SHOW DISK_SERVER COUNTER/CACHE
   ```

   If the rate is less than 80%, increase the cache.

3. Before changing the cache size, disconnect all users from the disk server by entering:

   ```
   $ PCSA_MANAGER> STOP DISK_SERVER CONNECTIONS
   ```

4. Exit the PCSA Manager Menu.
5. Increase the cache size in 256-page increments. The default cache size is 512 pages.

   To increase the cache size, edit the SYS$STARTUP:ESS$LAD_STARTUP.DAT file and enter a value for the CACHE parameter.

   The original SYS$STARTUP:ESS$LAD_STARTUP.DAT file is shown in Appendix D.

   For example, to change the cache size to 768, specify the desired value in the file as follows:

   ```
   CACHE = 768
   ```

6. For the change to take effect, restart the disk server by entering:

   ```
   $ @SYS$STARTUP:LAD_STARTUP
   ```

The VMS system resources required to support the cache are checked before the server starts. You may need to change a system parameter, such as NPAGEDYN. Because the disk server is a VMS device driver, the disk server cache comes from the system non-dynamic memory. NPAGEDYN defines the amount of non-system dynamic memory.

If a message is displayed on the screen indicating that you need to change system parameters, you must change them before the disk server can start:

a. Append the PCFS$MODPARAMS.DAT file to the MODPARAMS.DAT file.

   The PCFS$MODPARAMS.DAT file contains the required SYSGEN parameters. The MODPARAMS.DAT file contains any SYSGEN parameters that you previously modified. Both files are stored in the SYS$SPECIFIC:[SYSEXE] directory.

   To append the files, enter:

```
$ APPEND SYS$SPECIFIC:[SYSEXE]PCFS$MODPARAMS.DAT SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT
```

b. Run AUTOGEN and restart the VMS operating system:

   1. Start the PCSA Manager Menu by entering:

      ```
      $ ADMIN/PCSA MENU
      ```

   2. Select the **Utility Options** menu.

   3. Select the **Autogen the system** option from the Utility Options menu.

   4. Follow the prompts to run AUTOGEN with reboot.

c. If the disk server does not start automatically when you reboot the system, you need to restart the server now.

   1. Determine whether the disk server is started:

      a. Start the PCSA Manager utility by entering:

         ```
         $ ADMIN/PCSA
         ```

      b. Enter the SHOW VERSION command:

         ```
         PCSA_MANAGER> SHOW VERSION
         ```

    A display similar to the following indicates whether the disk server is started:

    ```
    LAD$KERNEL version  : Not available
    LADDRIVER  version  : Not available
    PCFS_SERVER version : PATHWORKS for VMS
    PCSA_MANAGER version: PCSA_MANAGER V4.1
    ```

 2. If the display indicates that the LADDRIVER version is not available, you need to start the server:

    a. Exit the PCSA Manager utility.

    b. Enter:

       ```
       $  @SYS$STARTUP:LAD_STARTUP
       ```

7. Repeat this process until you find a cache size that yields the highest cache hit rate.

Improving Performance on the Transport Software

Now that you have improved performance on the file and disk servers, you can also improve performance on both servers by managing the Local Area System Transport (LAST) software. The LAST software is the communication transport software that must be installed on both the server and the client.

You improve performance of the LAST software by managing how the VMS operating system allocates memory.

Memory Allocation

The VMS operating system accesses memory most efficiently from **lookaside lists**. The IRP, LRP and SRP lookaside lists are fixed-size packets of memory. These lists are used for networked applications, such as the LAST software.

To be sure that the VMS operating system uses lookaside lists for the LAST transport, you must manage the size of these lists. You can improve performance by monitoring the current size and the maximum size of the lists.

These lists are system parameters and are computed by the AUTOGEN program.

When no IRPs, LRPs or SRPs are available on the lists, the VMS operating system loses performance, because it must allocate resources from general memory.

Managing Lookaside Lists

When the current size equals the maximum size, you should increase the size of the lists.

Managing IRPs, LRPs, SRPs

To change the size of the IRP, LRP and SRP lists, change the IRPCOUNT, LRPCOUNT, and SRPCOUNTs.

To tune the lookaside list, do the following steps weekly:

1. Display the IRPCOUNT, LRPCOUNT, and SRPCOUNT values by entering:

   ```
   $ SHOW MEMORY /POOL /FULL
   ```

2. Define a minimum value for the IRPCOUNT, SRPCOUNT and LRPCOUNTs.

   The AUTOGEN procedure computes a maximum value to be approximately 3 times the minimum value.

   For example, when the current IRPCOUNT equals the maximum, increase the minimum by approximately 30% of the old maximum. Repeat the calculation for SPRCOUNT and LRPCOUNT as well.

   For example, if the current IRPCOUNT equals the maximum count of 300, increase the new minimum by 30% of 300, or 90, as follows:

Old Minimum	Current	Old Maximum	New Minimum	New Maximum
100	300	300	190	570

   The computed maximum will be 570.

3. To change LRPCOUNT, IRPCOUNT and SRPCOUNTs, edit the SYS$SPECIFIC[SYSEXE]:MODPARAMS.DAT file. Add one or more of the following lines when needed:

   ```
   MIN_IRPCOUNT = 200 !modified IRP based on use
   ```

4. Run the AUTOGEN procedure to modify the counts and reboot the system. Enter:

   ```
   $ @SYS$UPDATE:AUTOGEN GETDATA REBOOT NOFEEDBACK
   ```

   For more information on the AUTOGEN procedure, see the *VMS System Manager's Manual.*

9

Maintaining the Server

This chapter describes:

- Maintaining the file server
- Maintaining the disk server
- Backing up and restoring services

Maintaining the File Server

Maintaining the file server includes the following tasks:

- Monitoring activity
- Reallocating resources
- Using the file server log file
- Starting and stopping the server
- Managing the file server in a cluster

Monitoring Activity

Monitor file server operation to see who is using resources and which resources are being used.

Occasionally, users leave files open or their personal computers running even though they are not actually using them. Or, users may be unable to end a specific connection. These situations waste server resources and can prevent other users from accessing the resources they need.

Monitoring the server provides information that helps you conserve server resources. For example, when you monitor the server you can also:

- Disconnect a specific client
- Stop all connections to a service

- Close an open file

The following sections describe monitoring server activity and conserving each resource.

Monitoring Connections

You can display the clients using the file server and which services they are using.

Monitoring connections to file server

For example, to display connections to the file server, enter:

```
PCSA_MANAGER> SHOW FILE_SERVER CONNECTIONS
```

A list of clients connected to the file server is displayed:

```
File Server connections:

Connect ID  Client  User name     Alias name     Service name  Acc
----------  ------  ------------  ------------   ------------  ---
        14  NODE1   CHAN          CHAN           CHAN          RWC
     65536  NODE2   USER2         PCCOMMON       PCCOMMON      RWC
     65537  NODE3   USER3         USER1          USER1         RWC
    131072  BERTHA  USER4         LPS$ASCII      LPS$ASCII     RWC
    131073  BERTHA  USER4         LPS$POSTSCRIPT
                                                 LPS$POSTSCRIPT
```

For example, the display shows that User2 is using the client NODE2. However, you know that User2 is away on vacation and you want to disconnect the client NODE2.

Disconnecting a specific client

To disconnect NODE2, enter:

```
$ ADMIN /PCSA  STOP FILE_SERVER SESSION NODE2
```

Monitoring Connections to a Service

Monitoring active services

To view the services and number of current connections, enter:

```
PCSA_MANAGER> SHOW FILE_SERVER SERVICES /ACTIVE
```

A list of active services and the number of clients connected to them is displayed:

```
File Server active services:

Service name  Service type  Att/Len  Limit  Users
------------  ------------  -------  -----  -----
SYS$PRINT     PRINTER       STR/EST   NONE      1
SYS$LN03      PRINTER       STR/EST   NONE      1
VANL          USER          STR/EST   NONE      1
CHAN          USER          STR/EST   NONE      1
LPS$ASCII     PRINTER       STR/EST   NONE      1
PETERSON      USER          STR/EST   NONE      1
```

The display shows the number of users that will be disconnected if you stop connections to a service.

Stop all connections to a service before you back up a particular service or update software in a service.

Stopping connections to a service

To stop all connections to the service CHAN, enter:

```
$ ADMIN /PCSA  STOP FILE_SERVER CONNECTIONS /SERVICE=CHAN
```

Displaying Open Files

Many applications open files and keep them open in memory while the application is running. You need to determine which files are open before you can close them.

Monitoring open files regularly helps you evaluate the number of files needed for each user. You can use this information to determine a limit on the number of open files. To limit the number of open files allowed for each user or for the entire server, see Reallocating Resources .

To close an open file:

Displaying open files

1. Display the open files. Enter:

   ```
   $ ADMIN/PCSA SHOW FILE_SERVER OPEN_FILES
   ```

   In the display, look at the:

   - File identification (the number used to identify the file)
   - Client using the file
   - File type, which shows whether the file is opened on the server you are using or opened on another node in the cluster

     File type includes:

     - **Local**, a file that is opened and locked on the node where you are running
     - **Remote**, a file that is opened and locked by another node in the cluster
     - **Proxy**, a file that is opened and locked by the node you are running on, and the open request is initiated by another cluster node

2. Note the file identification and client of the open file you want to close.

3. You cannot close a proxy file from the server you are currently using. To close a proxy file, log on to the cluster node that requests the open file and then close the file.

4. Send a message to the user informing the user that the file is open and you are going to close it. Use the Broadcast utility.

Closing open files

5. For example, to close a file with identification 13, enter:

```
$  ADMIN/PCSA CLOSE FILE_SERVER FILE 13
```

Reallocating Resources

Maintaining the server includes adjusting resources so that users can access the services they need. You may need to limit access to services for some users so that other users can access them. Or, you may want to reduce the number of connections for each user to improve overall server performance.

This section describes how to change the limit of:

- Connections allowed to the file server
- Clients that can use the file server at the same time
- Open files

These limits are in effect for the period of time that the file server continues to run without stoping, called the file server session. This section also describes how to change these limits permanently.

Limiting the Number of Connections for Each Session

With the USE command, each user can connect to a number of file services on a server. You can limit the number of file services on your server that each user can connect to.

Unless you set a limit, there is no limit on the number of file services the user can connect to.

For example, to limit each user to five file service connections to the current server, enter:

```
$  ADMIN/PCSA SET FILE_SERVER CHARACTERISTICS /CONN = (SESSION = 5)
```

You can also limit the file services that **all** users can connect to on the server. Unless you change it, there is no limit on the total number of file services users connect to.

For example, to limit the total number of file service connections to 100, enter:

```
$  ADMIN/PCSA SET FILE_SERVER CHARACTERISTICS /CONN = (TOTAL=100)
```

Limiting Clients for Each Session

You can temporarily limit the number of clients in the server database to determine the effect that fewer clients have on server performance. Because each client uses system resources, you may want to decrease the number of clients.

You set a limit for the session by using the PCSA Manager commands. Limiting clients in the current session does **not** require that you reconfigure the server. Because you use only one command to change this limit, you can try different limits easily.

The limit of clients in the current session must be less than or equal the limit in the configuration.

The limit of clients in the current session can be less than or equal to the limit in the file server configuration.

You can also limit the total clients when you configure the file server; however, you cannot exceed that limit unless you reconfigure the server.

For example, to limit the number of clients to five, enter:

```
$  ADMIN/PCSA SET FILE_SERVER CHARACTERISTICS /SESSION_LIMIT =5
```

To limit the number of clients permanently, see Chapter 7.

Limiting Open Files

To allocate resources evenly among users, you can limit the number of files that users can open. You can limit the:

- Total number of files the server can open simultaneously
- Number of files each user can open

To limit the total number of files that the *file server* can open, enter:

```
$  ADMIN/PCSA SET FILE_SERVER CHARACTERISTICS /FILE_LIMIT =(TOTAL=100)
```

To limit the total number of files that each *user* can open, enter:

```
$  ADMIN/PCSA SET FILE_SERVER CHARACTERISTICS /FILE_LIMIT =(SESSION =5)
```

Limiting Resources Permanently

Once you have found resource limits that are effective, you can make them permanent. To set these limits automatically each time the file server starts:

1. Edit the PCFS_STARTUP.COM file, the startup file for the file server.
2. Insert the PCSA Manager command in the startup file. For example, to set the limit on the number of connections to 5 for each user, insert the following command in the file:

   ```
   $ SET FILE_SERVER CHARACTERISTICS /CONN= (SESSION=5)
   ```

Using the File Server Log File

Use the file server log file to maintain server security. The log file monitors connections, file accesses, and illegal file access attempts.

The file server log file helps you maintain server security.

The **log file** is a standard text file that contains messages describing network events on the file server. The file server stores information about its operation in the file server log file.

The log file contains messages indicating possible security breaches, such as:

- Invalid user names
- Number of users who opened and changed a particular file
- Unsuccessful attempts to connect to a file service

After an event occurs, it is logged in the file server log file every 60 seconds.

This section describes how to use the PCSA Manager Menu and commands to:

- View the log file
- Detect security violations
- Print the log file
- Start a new log file
- Choose the events to be recorded in the log file

Viewing the Log File

To list the messages in the log file:

Listing the file server log file

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **File Server Log Options** from the Utility Options menu.
3. Select **View the Log File** from the File Server Log Options menu.

   Example 9–1 shows a sample list of file server events.

Example 9–1 Sample Log File

```
7-Jan-90 23:05:18 (netio) Server started on node WRITER
7-Jan-90 23:05:27 (netio) Unit 163 (WRITER): link aborted
7-Jan-90 23:05:49 (netio) Unit 169 (WRITER): link aborted
7-Jan-90 23:05:56 (netio) Unit 165 (WRITER): link aborted
7-Jan-90 23:09:00 (netio) Unit 171 (WRITER): link aborted

Press RETURN for menu . . .
```

Sometimes a log file contains a number of "link aborted" messages. You do not have to respond to these messages unless users are complaining about losing links to the server.

Using the Command Line to View the Log File

You can also use the command line to display the log file.

Note

Do not use the editor on a log file that is currently open.

Displaying the log file name

To display the name of the current log file, enter:

```
$ ADMIN/PCSA SHOW FILE_SERVER STATUS
```

The log file by default is PCFS$LOG_FILES:PCFS_SERVER.LOG.

Using the log file with commands

To display the messages in the log file, enter:

```
$ TYPE PCFS$LOG_FILES:PCFS_SERVER.LOG
```

For an explanation of the messages in the log file, see *Server Messages*.

Detecting Security Violations

Detecting security violations

The file server log file may contain messages that indicate illegal attempts to break into the server. When you examine the file server log file, you should check for these messages.

To examine the security violations:

1. Look in the file server log file for the message:

```
Message from PCFS_SERVER:Invalid Username/Password from client
```

   This message indicates that a user has entered either an incorrect username or password. This message can occur when a user mistypes the username or password and may be inadvertent.

   Although you do not need to take any further action at this point, make note of the client that caused the message to occur. Repeated messages from the same client require further investigation.

2. Look in the file server log file for the message:

   ```
   Login break in attempt detected on PC file server from
   client node nodename on account account_name
   ```

   This message occurs when a user tries to use the same username repeatedly with incorrect passwords. It indicates that someone has tried to break into an account.

   You should be particularly concerned when the account displayed is "SYSTEM."

   When this message is displayed for a user's account, disable the account with the VMS AUTHORIZE utility.

Printing the Log File

To print the file server log file:

Printing the file server log file from the menu

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **File Server Log Options** from the Utility Options menu.
3. Select **Print the Log File** from the File Server Log Options menu.
4. Select a queue to which to print the log file.
5. Select a form on which to print the log file.

Starting a New Log File

Start a new log file to:

- Save space by closing and purging the previous versions
- Copy the log file to another file

Each time the file server restarts, a new log file is started automatically, and the previous log file closes.

To close the current version of the file server log file and create a new one:

Starting a new log file

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **File Server Log Options** from the Utility Options menu.
3. Select **Start a New Log File** from the File Server Log Options menu.

Purging previous log files

4. When you purge the log file, you can keep a certain number of log files. For example, to purge the file and keep five versions, enter:

   ```
   $ PURGE PCFS$LOG_FILES:*.LOG /KEEP=5
   ```

Choosing Events for the Log File

Using the log file with commands

You can choose events that the file server logs by using the command line.

By default, the file server logs fatal and non-fatal errors, security violations, and operator actions. An example of a security violation is an unauthorized user's attempt to access a file service.

Defining events in the log file

You can control which events the file server logs. For example, to log connections to the file server only, enter:

```
PCSA_MANAGER>  START FILE_SERVER LOGGING /EVENTS=CONNECTIONS
```

You can stop logging certain types of events. For example, to stop logging protocol events, enter:

```
PCSA_MANAGER>  STOP FILE_SERVER LOGGING /EVENTS=PROTOCOL
```

Starting and Stopping the File Server

This section describes how to start and stop the file server.

Starting the File Server

In the event that the file server goes down, you can restart it.

Start the file server by entering one of the following commands, depending on the transport you use:

- For DECnet communication, enter:

  ```
  $ @SYS$STARTUP:PCFS_STARTUP DECNET
  ```

- For TCP/IP, enter:

  ```
  $ @SYS$STARTUP:PCFS_STARTUP TCP
  ```

- For DECnet and TCP/IP, enter:

  ```
  $ @SYS$STARTUP:PCFS_STARTUP DECNET/TCP
  ```

If the file server does not start, read the startup log file, PCFS$LOG_FILES:PCFS$STARTUP.LOG. This file contains messages that occur when the server does not start. Enter:

```
$ TYPE PCFS$LOG_FILES:PCFS$STARTUP.LOG
```

Stopping the File Server

Stop the file server when you perform server maintenance.

To stop the file server, enter:

```
PCSA_MANAGER> STOP FILE_SERVER CONNECTIONS /ALL
```

Managing File Services in a Cluster

You can run the file server in a VAXcluster. To ensure data integrity and reasonable server performance, consider the following:

- In a VAXcluster, the file server supports MS-DOS byte range locking. Although cluster file sharing is permitted, file sharing can detract from server performance.

  When you offer a service on multiple nodes in a VAXcluster and a client opens a file for read or write, the file server puts a private lock on the file. If a second file server in the cluster attempts to access the file, then the second file server routes client requests through a DECnet link to the file server that owns the lock. This file server is responsible for arbitrating access to the file for all clients. Because rerouting requests causes overhead, file server performance decreases.

If users frequently share the same file, they should all connect to the same node in the cluster for the best performance.

- In a VAXcluster, use one service database for all nodes, unless some services are restricted to specific nodes. In this case, use a service database for each node in the VAXcluster.
- When running in a VAXcluster, store the log file in SYS$SPECIFIC, to ensure a unique location for the log file.

To restrict a database to the server on which you are running in the VAXcluster:

1. Edit the SYS$COMMON:[SYS$STARTUP]PCFS_LOGICALS.COM file.
2. Make sure the PCFS$SERVICE_DATABASE logical name points to SYS$SPECIFIC:[PCSA].
3. Move the database to SYS$SPECIFIC:[PCSA].
4. Restart the file server for the new database to take effect. See Starting and Stopping the File Server in this chapter.

Maintaining the Disk Server

Managing the disk server involves:

- Monitoring disk server activity
- Changing timeout
- Starting and stopping the server
- Managing disk services in a cluster

Monitoring Activity

You can monitor activity on the disk server. For example, you can check who is using a disk service and whether that user has left a personal computer or connection unattended.

Determine how many disk services are mounted on the server by listing them. The display lists network key disks as well as other disk services and the access allowed for each service.

The maximum number of disk services is 256. If close to 256 disk services are displayed, you may need to increase the maximum disk services. To increase the maximum, see Chapter 7.

You can also use the ***List Registered Disk Services*** *option from the menu.*

To display the available disk services, the limit of users and the number of active users, enter:

```
$ ADMIN/PCSA SHOW DISK_SERVER SERVICES
```

The list of registered disk services includes services added to the network with the following:

- Add Service option, Application Disk
- PCSA_MANAGER command CREATE DISK and mounted with the PCSA_MANAGER command MOUNT DISK

This command produces a display similar to the one in Example 9–2.

Example 9–2 Disk Services

```
Disk Server Services:

Service name  Type  Server  Limit  Users  Acc  Rating  Status
------------  ----  ------  -----  -----  ---  ------  -------------
00-01-02-03-04-05 (POPOF)
              BOOT  SRVR1      1      0  RW        1  PEND PERM
08-00-2B-03-08-F5 (CATCH)
              BOOT  SRVR1      1      0  RW        1  PEND PERM
08-00-2B-03-18-8B (BIGMAX)
PCSAOS2       USER  SRVR1      1      5  RW        1  PEND PERM
PCX           USER  SRVR1   NONE      0  RO        1  MNT PERM
PYAT-KOSHEK   USER  SRVR1      1      0  RW        1  MNT PERM
STASON        USER  SRVR1      1      0  RW        1  DISMNT PERM
```

On the display, note the limit to the disk service and the number of users. Then, you can check that services are actually in use.

Network key disks are displayed with:

- A name consisting of an Ethernet address, six pairs of hexadecimal numbers separated by dashes
- A Type of BOOT

To show disk service users

As a system manager, you may need to identify who is using resources on the server. Use the SHOW DISK_SERVER CONNECTIONS to display what connections are in use and who is using them.

The SHOW DISK_SERVER CONNECTIONS command displays the following information for the server you are currently using:

Listing clients connected to disk server

- Clients connected to the current disk server
- Disk service that clients are connected to
- Access allowed to the virtual disk
- The VMS file name for the virtual disk

For example, to display the connections to the server where you are running, enter:

```
PCSA_MANAGER> SHOW DISK_SERVER CONNECTIONS
```

The server displays:

```
Disk server connections:

Client  Service name  Acc  Container File
------  ------------  ---  -------------------------------------
USER1   MSWIN3_SDK    RO   $2$DUA26:[EWOK.WIN30]MSWIN3_SDK.DSK;1
USER2   RWSTCP        RW   SERVER:[PCSA.LAD]RWSTCP.DSK;1
USER3   TOOL_BOX      RO   CMSLIB:[DISKS]TOOL_BOX.DSK;1
```

Changing Timeout

In some cases, requests for disk services fail, because the PCSA Manager does not wait long enough to process the requests.

You can correct the failure by increasing the timeout value. The **timeout** value is the number of seconds the PCSA Manager waits for a response from the disk server.

The following steps explain how to avoid disk server timeout:

Monitoring timeout at the server console

1. Check the server console to see if the following message is displayed at the server console indicating timeout:

   ```
   PCSA-E-BADDSRV RECV, Receive from disk server failed.
   ```

Monitoring timeout at the client.

2. If you are at the PC instead, check the PC for the following message indicating timeout:

   ```
   Remote node unavailable.
   ```

3. If timeout messages are displayed on either the server or client, increase the timeout value. For example, to increase the timeout to 120 seconds, use the PCSA Manager commands and enter:

   ```
   PCSA_MANAGER>  SET DISK_SERVER CHARACTERISTICS /TIMEOUT=120
   ```

   This command changes the timeout for the disk server session. To change the timeout permanently, reconfigure the transport software, which is explained in Chapter 7.

Starting and Stopping the Disk Server

This section describes how to start and stop the disk server.

Starting the Disk Server

To start the disk server, enter:

```
$  @SYS$SYSTEM:LAD_STARTUP
```

Stopping the Disk Server

You need to stop the disk server to:

- Back it up
- Reconfigure the server

To stop the disk server:

Stopping the disk server disconnects all users from the disk server.

1. Broadcast a message to all users stating that connections to disk services are going to be temporarily disconnected. Use the BROADCAST command.
2. Enter:

   ```
   PCSA_MANAGER>  STOP DISK_SERVER CONNECTIONS
   ```

Managing Disk Services in a Cluster

When managing disk services in a VAXcluster, consider these points:

- Only one disk server in a VAXcluster can offer a disk for write access at one time. If a second disk server in the VAXcluster subsequently mounts the disk, it is mounted as pending. The second request to mount the disk is not completed until the first disk server dismounts the disk.

- To distribute service connections among the servers, offer a disk with read access on multiple nodes in the VAXcluster.
- The disk server's service database resolves conflicts when a disk is offered on multiple nodes in a VAXcluster. Only one copy of the database file is allowed in a VAXcluster, and it must be stored on a disk that is accessible to all nodes.

  The disk server database file is pointed to by the logical LAD$SERVICE_DATABASE.
- In a cluster, you can limit connections to disk services for only one node in the cluster and not for the entire cluster. For example, in a three-node cluster, a limit of two connections allows a total of six connections cluster-wide.

Backing Up and Restoring Services

As part of server maintainance, you need to make routine backups of stored data. A **backup** is a copy of the contents of a service, a directory, or a file.

You make the copy on a tape. Then, if the original is accidentally deleted, you can **restore**, or copy back, the files to the server.

You can back up:

- An application directory or subdirectory
- A user account (directory) or subdirectory
- A selection of files
- A single file

The following sections describe:

- Backing up services and user accounts
- Restoring services and user accounts

Backing Up Services and User Accounts

PCSA services contain DOS and OS/2 files. Since DOS and OS/2 files have only one version, you need to back them up frequently.

You can back up PCSA services and user accounts by:

- Using the PCSA Manager Menu

- Using the VMS BACKUP command to select the files to back up by date and to make incremental backups. These features are unavailable with the menu.

Either way, you can back up only eight levels of subdirectories from the root.

The following sections describe both options.

Backing Up Using the Menu

Using the PCSA Manager Menu, you can back up files by name or directory.

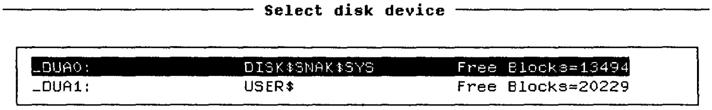
Backing up services stops the disk server and disconnects all clients from disk services.

To back up PCSA services or user accounts on the server disk:

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **Backup/Restore Options** from the Utility Options menu.
3. Select **Backup PCSA and User Accounts** from the Backup/Restore Options menu.

   PCSA disk and file services are referred to as "PCSA."
4. Select the disk from which to back up the PCSA and user accounts. Figure 9–1 shows a sample display of disks.

Figure 9–1 Disk Devices for Backup



```
------------------------- Select disk device -------------------------

 _DUA0:                  DISK$SNAK$SYS            Free Blocks=13494
 _DUA1:                  USER$                    Free Blocks=20229
```

5. Select the tape on which to save the backup files by using the arrow keys and pressing Return.
6. The PCSA Manager Menu highlights all the files on the selected disk and asks if you want to modify the list. If you want to select all user accounts, file services, and disk services, press Return and go to step 9.

   If you want to select particular user accounts, file services or disk services, enter **YES**.

7. Follow the prompts to select the directory to back up.

   The directory you select is displayed and is followed by VMS wildcard characters (*.*;*) representing all subdirectories and files in the directory.

8. Select the files within the directory to be backed up.

9. The PCSA Manager Menu prompts you to insert a blank tape in the tape drive and place the drive on line.

   PATHWORKS Server 3100 Users

   Place a blank TK50 tape cartridge in the TK50 tape drive. Place the tape drive on line by pushing the load/unload button on the TK50 tape drive to the in (load) position.

   The file services, disk services and user accounts are copied to tape. The names of the files being copied are displayed.

   The backup log file is named according to the form:

   ```
   SYS$COMMON:[PCSA]devicename_dd-mmm-yyyy_SELECTIVE.LIS
   ```

   devicename is the device name for the server disk. For example, the device name might be DUA0 or DKA300.

   dd is the day of the backup.

   mmm is the month of the backup.

   yyyy is the year of the backup.

10. Respond to the prompt asking if you want to print the backup log file.

    If you choose not to print the log file, it is saved in the SYS$COMMON:[PCSA] directory.

    If you choose to print the log file:

    a. Respond if you want to delete the log after printing.

    b. Select a print queue and form to be used for printing.

11. Remove the tape from the tape drive and label it. For example:

    ```
    MYSERVER Disk backup: User files, 15-SEP-1991
    ```

Using VMS BACKUP

Use the VMS BACKUP command to:

- Back up specific files by date
- Make **incremental** backup; that is, backups of only those files that have changed since the previous backup

To specify the date of files to be backed up, run the VMS BACKUP command with both the /SINCE and /MODIFIED qualifiers.

Since DOS and or OS/2 files have only one date, the file server identifies the date as the **modified** date instead of the create date.

For example, to back up files created after the first of June in the device and directory DUA0:[MYDIR]:

1. Broadcast a message to all users stating that connections to disk services are going to be temporarily disconnected. Use the BROADCAST command.

Stopping the disk server disconnects all users from the disk server.

2. Stop the disk server. Enter:

   ```
   PCSA_MANAGER> STOP DISK_SERVER CONNECTIONS
   ```

   This command dismounts virtual disks.

3. Use the VMS BACKUP command to perform either incremental or image backups. Enter:

   ```
   $ BACKUP DUA0:[MYDIR] /SINCE=1-JUN /MODIFIED=1-JUN
   ```

4. Restart the disk server. Enter:

   ```
   $ @SYS$SYSTEM:LAD_STARTUP
   ```

Restoring PCSA and User Accounts

If you accidentally delete a file, you can restore it using the Restore PCSA and User Accounts option. Use this option to recreate a file or files on the disk as they were when you performed the backup.

Restoring Services and User Accounts

To restore PCSA disk services, file services and user accounts on the server disk:

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **Backup/Restore Options** from the Utility Options menu.

3. Select **Restore PCSA and User Accounts** from the Backup/Restore Options menu.
4. Select a disk device from the PCSA Manager Menu screen.
5. Select the tape from which you will restore the file.
6. Follow the PCSA Manager Menu prompts to insert a backup save set in the tape drive and place the drive on line.

   PATHWORKS Server 3100 Users

   Place the TK50 tape cartridge that contains the files you want to restore in the TK50 tape drive. Place the tape drive on line by pushing the load/unload button on the TK50 tape drive to the in (load) position. For more information on loading a tape cartridge, see *Installation and Configuration Guide*.

   To continue restoring PCSA and user files, press Return. The PCSA Manager Menu retrieves information about the save set from the backup tape. A **save set** is a collection of files that has been backed up.
7. The PCSA Manager Menu identifies the name of the save set on the backup tape you inserted in the tape drive. Verify that it is correct.

   The name of the save set file is in the following form:

   ```
   devicename_dd-mmm-yy
   ```

   devicename is the device name for the server disk. For example, the device name might be DUA0 or DKA300.

   dd is the day of the backup.

   mmm is the month of the backup.

   yy is the year of the backup.
8. The PCSA Manager Menu selects all files in the save set and asks if you want to modify the list. Modify the list, for example, to restore a particular file not displayed. Follow the prompts to select the directory and files to back up.

   The directory you select is displayed and is followed by VMS wildcard characters (*.*;*) representing all subdirectories and files in the directory.

9. Follow the prompts to verify the selections.

   The screen displays a “Restore Complete” message when the operation is finished.

10. Remove the tape cartridge from the tape drive.

10

Using the Broadcast Utility

Use the Broadcast utility to send messages from the server to clients. You can, for example, let users know about important server information, such as available new services or offline maintenance times.

The PCSA Manager Menu provides an easy way to send messages from the server to one or all clients.

> **Note**
>
> The Broadcast utility is not supported over the TCP/IP network.

This chapter describes how to use Broadcast to send messages to clients.

You can send as many messages as you need from the server. However, clients can only store a maximum of ten messages at a time.

When you make a change to services available to clients, you can send a Broadcast message explaining the change. For example, if you plan to perform a backup, send a Broadcast message telling users that they should disconnect from the services.

To send a Broadcast message:

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **Send Broadcast Message** from the Utility Options menu.
3. At the prompt, enter the name of the node where you want to send a message.

To send a Broadcast message to a particular client, enter the DECnet node name of the client, then press Return. The prompt is repeated so you can send the message to multiple clients. When you have named all the nodes to which you want to send a Broadcast message, press Return.

To send a Broadcast message to all clients on the network, enter *.

4. Enter the Broadcast message you want to send. The message you send using the PCSA Manager Menu can be up to 80 characters long.

Note

Clients can only store up to 10 messages at a time. After 10 messages, Broadcast deletes the oldest message and stores the new one. Therefore, try to limit the number of messages you send until you are confident that users have had enough time to read their messages.

You can modify the STARTNET.BAT file to change the default Broadcast settings, such as the colors in which the messages are displayed. Refer to *Client Commands Reference* for a list of these settings.

11

Managing Clients

After you have configured clients with the Netsetup utility, you can maintain them on the server. The maintenance tasks include:

- Adding and deleting nodes
- Listing remote boot clients
- Deleting remote boot clients
- Restoring the boot database
- Listing DOS operating systems

Note

Clients are referred to as workstations in the software.

Adding a Node

Adding a node defines a DECnet node name and address in the DECnet database on the server.

Use this option only for clients that use the DECnet communication protocol.

To add another client to the DECnet node database on your server:

Use for DECnet clients only.

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Node Registration Options** from the Workstation Options menu.
3. Select **Add a Node** from the Node Registration Options menu.
4. At the prompt, enter the unique 1- to 6-character node name for the node you are adding.

5. At the prompt, enter the DECnet address of the node to be added.

The PCSA Manager Menu displays messages while it adds the node name and address you entered to the DECnet database.

Deleting a Node

When a client no longer needs access to the network, you can delete the node from the DECnet database. Deleting a node saves space in the DECnet database.

This option is available for clients using the DECnet communication protocol.

To delete a client from the DECnet node database, follow these steps:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Node Registration Options** from the Workstation Options Menu.
3. Select **Delete a Node** from the Node Registrations Options menu.
4. When you are prompted for the name or address of the node to be deleted, enter either the 1- to 6-character DECnet node name or the node address of the node you want to delete.

   If you enter a valid node name, the PCSA Manager Menu uses the node name to search the DECnet database and displays a success message with the node address.

   If you enter the node address, the PCSA Manager Menu uses the node address to search the database and displays a success message with the node name.

   If you enter an invalid node name or address, such as a node name longer than 6 characters, the PCSA Manager Menu displays a message and redisplays the prompt. Reenter a valid node name or node address.

The PCSA Manager Menu displays messages while it removes the node from the DECnet node database.

Listing Remote Boot Clients

One of the advantages of remote boot is that clients using remote boot can be centrally maintained on one server node.

Note

Refer to the Software Product Description to check if remote boot is available with your client configuration.

To list the clients registered for remote boot:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Remote Boot Workstation Options** from the Workstation Options menu.
3. Select **List Remote Boot Workstations** from the Remote Boot Workstation Options menu.

Deleting a Remote Boot Client

Delete a remote boot client to remove the client from the network.

To reconfigure a remote boot client for local boot, use the Netsetup utility instead.

To delete a remote boot client:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Remote Boot Workstation Options** from the Workstation Options menu.
3. Select **Delete Remote Boot Workstation** from the Remote Boot Workstation Options menu.
4. At the prompt, enter the 1- to 6-character node name for the client you want to delete.
5. At the prompt, verify if you are sure you want to delete the client.

   Deleting a remote boot client deletes the network key disk the client uses to boot.

The PCSA Manager Menu displays messages while deleting the client profile.

Modifying network key disks

Using the command line, you can change network key disks created with the Netsetup utility, including the:

- Hardware address for the Ethernet controller on the workstation
- Type of Ethernet controller

To change the hardware Ethernet address or the type of Ethernet controller, use the MODIFY WORKSTATION command. (For information, see *Server Administrator's Commands Reference*.)

Restoring a Boot Database

The DECnet database file contains the appropriate NCP commands needed to boot remote clients. If this file is destroyed, you need to recreate it.

To restore a DECnet database file:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Remote Boot Workstation Options** from the Workstation Options menu.
3. Select **Restore Boot Database** from the Remote Boot Workstation Options menu.
4. At the prompt, enter the type of Ethernet controller for the server.
5. At the prompt, respond whether you want to run the command file now. The command file recreates the DECnet database file.

   If you want to run the command file at another time, enter **N**. Later, to run the command file, enter the following at the VMS prompt:

   ```
   $  @SYS$MANAGER:PCSA$REMOTE_BOOT.COM
   ```

Listing Client Operating Systems

Client operating systems, such as DOS operating systems, are available on the network as system services. To keep track of the different client operating systems, list them. They can be either file services or disk services.

To list the client operating systems:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Remote Boot Workstation Options** from the Workstation Options menu.
3. Select **List Client Operating Systems** from the Remote Boot Workstation Options menu.

   The PCSA Manager Menu displays a list of each DOS operating system installed on the server.

12

Managing PATHWORKS Server 3100 Systems

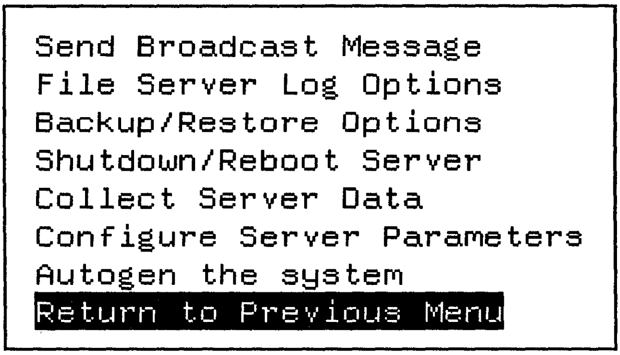
This chapter describes the tasks you need to do to maintain a PATHWORKS Server 3100 system, including:

- Backing up an entire disk
- Restoring disks
- Shutting down the server
- Rebooting the server
- Listing nodes

These options are available only on PATHWORKS Server 3100 systems.

You can perform most of these tasks using options in the Utility Options menu. Figure 12–1 shows the menu choices.

Figure 12–1 Utility Options Menu for PATHWORKS Server 3100



Backing Up and Restoring Data

As part of maintaining the PATHWORKS Server 3100 system, you need to make routine backups of stored data.

The following sections describe:

- Backing up an entire disk
- Restoring disks

A **backup** is a copy of the contents of an entire server disk, a directory, or a file. You make the copy on a tape. Then, if necessary, you can **restore**, or copy back, the files to the server in case the original is accidentally corrupted or destroyed.

Backing Up an Entire Disk

To guard against possible data loss, back up the server system disk at least once every month or when you make a change to the system.

When you back up a server system disk, you save copies of all files that are on the server, including volatile data, such as application and user files, and more stable system data, such as system software.

Backing up an entire system disk disconnects all clients from the server. Users cannot connect to the server until the backup procedure is completed.

In the event of a system failure, you can restore your system using the backup media for your PATHWORKS Server 3100 system. For instructions on restoring the disk, see Restoring the Server Disk in this chapter.

To back up the system disk

To back up an entire disk:

1. Send a Broadcast message to all users notifying them that the server will be unavailable. (See Chapter 10.)
2. Select **Utility Options** from the PCSA Manager Menu.
3. Select **Backup/Restore Options** from the Utility Options menu.
4. Select **Backup Entire Disk** from the Backup/Restore Options menu.
5. Select the device to be backed up.
6. The PCSA Manager Menu asks for confirmation to disconnect all clients.

   Place a blank TK50 tape cartridge in the TK50 tape drive. Place the tape drive on-line by pushing the load/unload button on the TK50 tape drive to the in (load) position. For more information on loading a tape cartridge, see *Installation and Configuration Guide.*

   The program copies any VMS system files, user accounts, file services, and disk services that exist on that disk, to the TK50 tape and displays the names of the files being copied.
7. The PCSA Manager Menu identifies the name of the backup log file.

   The backup log file is named in the form:

   ```
   SYS$COMMON:[PCSA]devicename_dd-mmm-yyyy_IMAGE.LIS
   ```

   devicename is the device name for the server disk. For example, the device name might be DUA0 or DKA1.

   dd is the day of the backup.

   mmm is the month of the backup.

   yyyy is the year of the backup.

8. At the prompt, respond if you want to print the backup log file.

   If you choose not to print the backup log file, it is stored in the SYS$COMMON:[PCSA] directory.

   If you choose to print the backup log file, the PCSA Manager Menu:

   a. Asks if you want to delete the log after printing

   b. Prompts you to select a printer queue to which to print the backup log file

   c. Prompts you to select a form on which to print the backup log file

9. Remove the TK50 tape cartridge from the TK50 tape drive and label it. For example:

```
PCLAN_SYS Disk backup, Save set 10-SEP-1989
```

Restoring Disks

This section describes the procedures for restoring:

- An entire server system disk
- Other disks

Restore the contents of a server system disk using VMS Standalone Backup.

When you restore an entire server system disk, you must shut down the system.

Shut down the server.

To shut down the system, refer to Shutting Down the Server. The shutdown procedure automatically sends a messages to all users notifying them that the system will be unavailable.

Allow 1-2 hours to restore a server disk.

Allow one to two hours to restore an entire server disk.

Restoring a System Disk

To restore an entire server system disk:

1. After shutting down the system, stop the server by pressing the Halt button on the rear of the system unit.

2. Place the TK50 tape cartridge that contains the PATHWORKS Server 3100 kit, which was shipped with your system, in the TK50 tape drive.

Place the drive on-line by pushing the load/unload button on the TK50 tape drive to the in (load) position. For more information on loading a tape cartridge, see *Installation and Configuration Guide*.

3. At the console terminal, load the backup function from the PATHWORKS Server 3100 1/2 tape into memory.

   Get the tape device name.

   Display the name of the tape device by running the following command:

   ```
   >>> SHOW DEV MK
   ```

   Use the name of the tape device in the following command. For example, if the tape device name is **MKB500**, enter:

   ```
   >>> B MKB500:
   ```

4. Enter the date.

   When the prompt ($) appears, place the TK50 tape that contains the files you want to restore in the TK50 tape drive. Place the drive on-line by pushing load/unload button on the TK50 tape drive to the in (load) position.

5. Copy the save set from the TK50 tape to your server disk by entering:

   ```
   $ BACKUP/IMAGE/LOG Tape_device_name: Disk_device_name:
   ```

   Tape_device name is the name you used in step 4, usually MKB500: for a PATHWORKS Server 3100 system.

   Disk_device name is the device name for the server disk you are restoring.

6. When the backup is complete, the following message is displayed:

   ```
   If you do not want to perform another standalone
   BACKUP operation, use the console to halt system.

   If you do want to perform another standalone BACKUP
   operation, ensure the standalone application volume
   is on-line and ready. Enter "YES" to continue:
   ```

   a. Remove the TK50 tape cartridge from the tape drive.

   b. Stop the server by pressing the Halt button on the rear of the system unit.

c. At the console prompt, enter:

```
>>> B
```

This command starts the VMS operating system.

Restoring Other Disks

To restore other disks:

Restoring other disks

1. Dismount the disk that has to be restored and then remount it by entering:

```
$ DISMOUNT disk_name
$ MOUNT/for disk_name
```

2. Place the TK50 tape that contains the files to be restored into the TK50 drive and enter:

```
$ MOUNT/for tape_device
```

3. Enter the backup command:

```
$ BACKUP/IMAGE/LOG tape_device: disk_device
```

When the backup is complete, the dollar sign prompt returns.

4. Dismount the tape device.

```
$ DISMOUNT tape_device
```

5. Use the PCSA Manager Menu to reboot the system. See Rebooting the Server.

Shutting Down the Server

You need to shut down the system during emergency weather situations or when you want to perform housekeeping functions. These include:

- Preventive maintenance
- Changing system parameters
- Stopping batch and output queues
- Dismounting volumes

The Shutdown selection ensures an orderly shutdown because it automatically sends a broadcast message to users, stops batch and device queues, disconnects all services, and stops user processes. It allows you to define a specific time period before the shutdown actually begins and then shuts down the server for the specified time period.

Press the halt button on the back of your server and boot the server.

To shut down the server for the PATHWORKS Server 3100 system:

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **Shutdown/Reboot Server** from the Utility Options menu.
3. Select **Shutdown** from the Shutdown/Reboot Server menu.
4. The PCSA Manager Menu asks you how many minutes you want to wait before starting the system shutdown.

Default wait time is 5 minutes.

   - If you want to wait five minutes before beginning to shut down the system, press Return to accept the default.
   - To specify a different length of time to wait before beginning to shut down the system, enter the number of minutes.

     The system displays messages advising you that all clients have been notified, that the server is shutting down, and that users should log off.

Caution

While it is possible to cancel the Shutdown option by pressing Ctrl/C, you should not do so. If you press Ctrl/C after the shutdown procedure has begun, you can leave the server in an indeterminate state.

Rebooting the Server

When you change VMS system parameters, you need to reboot the system to bring the new parameters into effect. Use the Reboot option from the Shutdown/Reboot Server menu to shut down the server and then automatically reboot it.

The Reboot option automatically sends a Broadcast message to all users advising them of the system shutdown.

When you select Reboot, the PCSA Manager Menu disconnects all services, shuts down the VMS system, and then automatically reboots the server.

To shut down and automatically reboot the server:

1. Select **Utility Options** from the PCSA Manager Menu.
2. Select **Shutdown/Reboot Server** from the Utility Options menu.
3. Select **Reboot** from the Shutdown/Reboot menu.
4. The PCSA Manager Menu asks you how many minutes you want to wait before starting the system shutdown.

Default wait time is 5 minutes.

   - If you want to wait five minutes before beginning to shut down the system, press Return to accept the default.
   - If you want to specify a different length of time to wait before beginning to shut down the system, enter the number of minutes.

   The system displays messages advising you that all clients have been notified, that the server is shutting down, and that users should log off.

Caution

While it is possible to cancel the Reboot option by pressing Ctrl/C, you should not do so. If you press Ctrl/C after the shutdown procedure has begun, you can leave the server in an indeterminate state.

Listing Nodes

You can list nodes defined in the DECnet database, which contains a list of DECnet node names and addresses for:

- Clients, if the server recognizes only registered nodes
- Clients that remote boot
- Other nodes, such as other servers

This option lists only those clients that use the DECnet communication protocol.

Clients are referred to as "workstations" in the software.

To list clients and other nodes:

1. Select **Workstation Options** from the PCSA Manager Menu.
2. Select **Node Registration Options** from the Workstation Options menu.
3. Select **List Nodes** from the Node Registration Options menu.

See Example 12–1 for an example of the List Nodes display.

Example 12–1 Sample Listing of Known Nodes

```
Known Node Permanent Summary as of 1-MAY-1989 08:09:10

Executor node = 4.15 (MILTON)

State                  = on

Remote node =  3.33 (BRONTE)
No information available

Remote node =  4.33 (WOOLFE)
No information available

Remote node =  5.33 (AUSTEN)
No information available
```

The list of nodes includes the DECnet node address for the executor node, which is the server from which you issue the command. The node name for the executor node is displayed in parentheses. Listed below the executor node is the node address and node name (in parentheses) for each remote node listed in the DECnet database for the server.

Note

Once you select the List Nodes option, you cannot stop or cancel the display.

A

Managing VMS and DOS File Differences in File Services

As a system administrator, you probably share files with DOS and VMS users. In most cases, you can easily share the same file with DOS and VMS users by using a file service.

Because DOS and VMS have different file structures, files do not look the same in both environments. Therefore, certain types of files may cause problems when shared by DOS and VMS users in a file service.

This appendix explains:

- Differences in VMS and DOS file structures
- Using VMS files in a DOS environment
- Using DOS files in a VMS environment

Differences Between VMS and DOS File Structures

VMS file structure

VMS uses the Record Management System (RMS) to manage files. RMS sees a file as a sequence of records. When you read or write a file on VMS, RMS reads or writes a record in the file.

How VMS handles carriage control information

VMS stores information about a file's organization, such as length, in the file itself. In some cases, RMS does not store carriage control information in the file. When reading a VMS file, RMS knows how to interpret carriage control information to break records into lines of text.

For more information on VMS file organization, see *Guide to VMS File Applications.*

DOS file structure

DOS sees a file as a sequence of bytes. When you read or write a DOS file, DOS reads or writes a certain number of bytes at a certain byte offset.

How DOS handles carriage control information

DOS does not have a mechanism like RMS to interpret carriage control information; instead individual applications interpret lines of text. In DOS, a file contains only data entered by the user and *not* information about the file.

Using VMS Files in a DOS Environment

Clients may have trouble using certain types of VMS files (for example, binary files) in a file service.

The following sections describe:

- Using VMS files in file services without problems
- Using binary files with carriage control information
- Using file services with actual and estimated length
- Correcting problem files

Using VMS Files in File Services

This section describes VMS file types that do not cause problems when clients use them in a file service. If you create files in the types described in this section, clients can write to and modify them using file service.

Create files of the type described in this section if they are to be used in a file service.

To determine if a VMS file is one of the types that do not cause problems:

1. Enter the ANALYZE/RMS command:

   ```
   $ ANALYZE/RMS myfile.txt
   ```

   Characteristics similar to the following are displayed:

   ```
   RMS FILE ATTRIBUTES

           File Organization: sequential
           Record Format: variable
           Record Attributes:   carriage-return
           Maximum Record Size: 255
           Longest Record: 101
           Blocks Allocated: 3, Default Extend Size: 0
           End-of-File VBN: 2, Offset: %X'0140'
           File Monitoring: disabled
           Global Buffer Count: 0
   ```

2. Note the File Organization, Record Format and Record Attributes. To create VMS files that clients can share easily in a file service, use the formats listed in the Table A–1. Files in these formats do not require RMS.

Table A–1 VMS File Types to Be Used in File Services

File Organization	Record Format	Record Size	Record Attributes
Sequential	STREAM		
	STREAM_LF		
	STREAM_CR		
	UNDEFINED		
Sequential	FIXED	Even	None
		Multiple of 512	NO BLOCK_SPAN
		Power of 2	NO BLOCK_SPAN

RMS is used for files not in the formats in Table A–1. To keep track of record organization, RMS uses extra space in these files by:

- Storing the record length at the beginning of each record in a 2-byte field
- Adding a null byte at the end of the record for odd-length records
- Adding extra space at the end of the disk block for non-spanned records so they do not span block boundaries
- Storing information on file organization for relative and indexed files

For more information on RMS overhead, see *Guide to VMS File Applications*.

Using Binary Files with Carriage Control Information

A DOS client may have trouble using binary files created in VMS in a file service. Problems can occur with binary files with the following record attributes:

- Carriage-return
- PRINT
- FORTRAN

The VMS ANALYZE/RMS command displays the Record Attributes field for VMS file (see Using VMS Files in File Services).

The most common types of binary files, also known as image files, are executable files (.EXE) and spreadsheet files (.SLK and .WIK).

Many binary files have a fixed-length format and record attribute of carriage-return, because this is the VMS default attribute.

When a VMS binary file is read from DOS, the carriage-return and line feed characters may cause an error.

This problem does not occur with VMS text files, which do not actually store the carriage-return character. The file server appends each record with a carriage-return and line feed so that text files look the same to a DOS and VMS user.

For more information on carriage control, see *VMS File Definition Language Facility*.

Using File Services with Actual and Estimated Length

You can create file services with either estimated or actual file length:

- With **estimated length**, the file server determines the file length from the position of the end-of-file pointer.
- With **actual length**, the file server determines the file length by reading the entire file.

You need to know the VMS format of individual files to be used in the service before choosing an actual or estimated length service.

Using File Services with Actual Length

You can use a file service with actual length without a problem if the service contains files:

- With fixed record format and:
  - With record attribute of carriage-return
  - Without carriage control information
- Of the type listed in Table A–1

Using file services with actual length detracts from server performance.

For files of other types, using an actual length service detracts from server performance when the server reads the entire file to determine the file length. The server determines the file length when it opens a file for the first time and when the file changes subsequently. For example, file length is required when the user runs a DOS directory. The server then stores the file length in an application ACE.

Using File Services with Estimated Length

Clients may have trouble using file services with estimated length, because the file length estimate is inaccurate:

Using file services with estimated length may give inaccurate length estimates.

- For files with carriage control information, such as a FORTRAN or PRINT files, the length estimate may be *lower* than the actual file length.

  When the length estimate is low, DOS sees these files as shorter than they actually are and stops reading them before the end of file.
- For files that have extra space for RMS, the length estimate is *higher* than the actual file length.

Correcting Problem Files

To avoid problems with binary files and actual length services, use VMS files that are one of the file types listed in Table A–1.

You can either *create* or *convert* VMS files to be one of the types listed in the table by:

- Using the VMS CONVERT utility

  (See *VMS Convert and Convert/Reclaim Utility Manual* for more information.)

- Using the EXCHANGE/NETWORK utility

  (See *VMS Version 5.2 New Features Manual* for more information.)

- Using a programming language to create VMS files without carriage control attributes. Table A–2 shows the instructions you can use in several programming languages to suppress carriage control attributes. For example, you can use a FORTRAN program to create a binary file without carriage-return characters.

Table A–2 Creating VMS Files Without Carriage Control Information

Language	Instruction
ADA	FORM => "RECORD; CARRIAGE_CONTROL NONE;"
BASIC	RECORDTYPE NONE
C	Not necessary. The default format (STREAM_LF) works for binary files.
FORTRAN	CARRIAGECONTROL = 'NONE'
PASCAL	CARRIAGE_CONTROL := NONE
PL/I	ENVIRONMENT(CARRIAGE_RETURN_FORMAT(0))

For COBOL files, you need to change the OPEN OUTPUT <filename>. to:

```
CALL "FDL$CREATE" USING BY DESCRIPTOR "<file.fdl>"
OPEN EXTEND <filename>
```

The <file.fdl> must include the following statements:

```
FILE
 NAME <filename>
 DEFAULT_NAME < optional defaults....>
 ORGANIZATION SEQUENTIAL
RECORD
 FORMAT <FIXED|VARIABLE>
 SIZE <number> ! use  a size of the base record type
                         ! if using FIXED format
 CARRIAGE_CONTROL NONE
```

Using DOS Files in a VMS Environment

If you write VMS applications to read DOS files created in a file service, you need to understand how these files are stored so your applications can read them. For example, suppose a DOS client creates a spreadsheet in a file service using LOTUS 1-2-3. To write a VMS application that uses the spreadsheet, you need to know the file format the spreadsheet is stored in.

File services create files in these VMS formats:

- STREAM
- FIXED with 512-byte records

You specify STREAM or FIXED format for each service you create.

Use STREAM format for text files.

The default format is STREAM, which causes no problems for *text* files created using a file service. You can use these text files easily in VMS.

Use FIXED format for binary files.

However, many DOS files are *not* text files. DOS binary files do not contain the carriage control and line-feed sequences that RMS expects to find in files with record format STREAM. Reading these files in VMS may cause problems. You need to create a file service with FIXED format to use these files in VMS. For example, WPS-PLUS/VMS expects files in a format of fixed-length 512-byte records.

Create a file service with fixed-length records.

To read DOS binary files in VMS, create a file service with FIXED format by using the /ATTRIBUTES=SEQUENTIAL_ FIXED qualifier in the ADD SERVICE/DIRECTORY command. (See Chapter 3.)

Some PC applications write files that include an end-of-file pointer (EOF). These files present no problems when used in VMS.

Files without an EOF in Fixed-Length File Services

However, files without EOF in a fixed-length service may be problematic in VMS. RMS inserts 0s as necessary to complete a 512-byte record in the last record of the file. If you write a VMS application to read the file, make sure that the extra 0s are not considered user data.

B

Setting Up HP LaserJet Printers

This appendix describes how to connect an HP LaserJet printer to the server.

1. Connect the hardware.

   Connect the LaserJet to the VAX server using the Serial Interface. The cable should be a null modem cable (pins 2 and 3 cross over) with a female DB25 connector at the VAX end and a male DB25 connector at the printer end.

   Example B–1 shows how the cables should cross.

Example B–1 Cable Connections

```
                 PIN      PIN
                 ---      ---

      GROUND      1 ------- 1   GROUND

      TRANSMIT    2 --\ /-- 2   Transmit
                       X
      RECEIVE     3 --/ \-- 3   RECEIVE

  SIGNAL GROUND   7 ------- 7   SIGNAL GROUND
```

2. Configure the LaserJet for proper operation when connected to the VAX server.

   a. Using the printer ON-LINE button, place the printer offline (light above the ON-LINE button is off).

   b. Using the printer MENU button, set the following items (use "+" and "-" buttons to cycle through available settings and use the 'ENTER' button to select a setting):

      COPIES=01
      MANUAL FEED=OFF
      FONT Source=I

FONT NUMBER=00
FORM=060 LINES

c. Hold the MENU button down for 5 to 10 seconds until it changes from “00 READY” to “SYM SET=...”.

   Set the following items (use the "+" and "-" buttons to cycle through available settings and use the ENTER button to select a setting):

   SYM SET=ROMAN-8
   AUTO CONT=OFF
   I/O=SERIAL
   BAUD RATE=4800
   ROBUST XON=ON
   DTR POLARITY=HI

d. Place the printer online using the ON-LINE button.

C

User Profile Form

User's name:

User's password (Default: WELCOME):

Path for user's account:

File version limit (Default: 1):

Allow interactive login? [Y N]

Common directory:

File service application(s):

Disk service application(s):

Printer services for LPT1:

Printer services for LPT2:

Printer services for LPT3:

D

Disk Server Startup Parameters

This appendix contains parameters used when the disk server starts. The parameters are stored in the ESS$LAD_STARTUP.DAT file.

```
!++
! This file will be used to set LADCP qualifiers.
! Entries are
!
! CACHE - Count of disk blocks to cache
! MAXIMUM_SERVICES - Maximum count of services to be mounted
! WRITE_LIMIT - Server wide Count of asynchronous writes
!--

   CACHE = 512  ! Default setting
```

E

LAST Startup Parameters

This appendix contains the parameters used when the LAST software starts. The parameters are stored in the ESS$LAST_STARTUP.DAT file. Changing the values is explained in Chapter 9.

```
!++
! This file will be used to set the appropriate LASTCP qualifiers. The
! following LASTCP qualifiers: ALL_CONTROLLERS, CHECKSUM, TRANSMIT_QUOTA,
! or SLOW_MODE can be set by using the following statement format:
! LASTCP qualifier = 1 to enable   e.g. SLOW_MODE = 1 enables  SLOW_MODE
! LASTCP qualifier = 0 to disable  e.g. SLOW_MODE = 0 disables SLOW_MODE
! The remaining LASTCP qualifiers will require the appropriate value
! settings.
! DEVICE          = (list-of-devices)
! TIMEOUT    = n    minimum interval in seconds
! CIRCUIT_MAXIMUM = n    maximum number of nodes
! GROUP           = n    Group number
! NODE_NAME       = name   Node name
! CONTROLLERS     = ([{controller letter,}...]) Controller list
! TRANSMIT_QUOTA  = n    Number of transmit buffers
!--
ALL_CONTROLLERS = ON
```

F

File Server Startup Parameters

This appendix lists the PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file. It contains:

- Parameters used to configure the file server
- Parameters used to improve file server performance

Some of these parameters are discussed in Chapter 7 and Chapter 8.

PCFS$ADDITIONAL_CHANNELS

This parameter adds a value to the SYSGEN parameter CHANNELCNT for disks that are not mounted when you configure the server.

Do not edit this parameter.

PCFS$AST_LIMIT

This parameter is calculated when you configure the server. It specifies the maximum number of asynchronous system traps that the file server can have outstanding at any one time.

The maximum value is 32767.

It is used to define the AST_LIMIT qualifier used in the VMS RUN command.

PCFS$BUFFER_LIMIT

This parameter is calculated when you configure the server. It specifies the amount of memory in bytes that the file server can use for input output operations.

It is used to define the BUFFER_LIMIT qualifier used in the VMS RUN command.

PCFS$BUFFER_SIZE

The file server cache is divided into buffers, which are measured in bytes. The buffer size determines the amount of data the file server reads or writes to the disk at a time.

Buffer sizes are 512, 1024, 2048, 3072, 4096, 8192, 16384, 32768, and 66536.

PCFS$CACHE_OPEN_FILES

This parameter determines whether files are stored in the open file cache after they have been closed by the user. When open file caching is enabled, a file remains in cache for a period of time specified by by the parameter PCFS$CLOSE_DELAY after it has been closed by an application.

Open file caching is effective for applications that frequently open and close the same files, for example, DOS batch files.

You must specify "Y" or "N".

PCFS$CACHE_SIZE

The cache size is the amount of physical memory, in pages (512 bytes), allocated for data caching. **Data caching** stores all data requested for input and output in the cache. Data caching reduces the overhead of waiting for disk access when the user requests to read or write to a file.

The minimum value is 512. The maximum value depends on the available physical memory, the number of workstations, and the number of open files per workstation.

PCFS$CLOSE_DELAY

This parameter specifies the number of seconds the server waits before closing a file. It is used with open file caching. When open file caching is enabled, a file remains in cache for the number of seconds specified in the close delay. This parameter is not used when open file caching is disabled.

The minimum value is 1 second; the maximum value is 99999 seconds.

PCFS$CLUSTER_ROUTING

This parameter is set when you configure the server:

- To "T"(true) when the node on which you configure the server is a cluster member.
- To "F" when the node on which you configure is not a cluster member

You cannot set this parameter by using the menu or by editing the data file.

PCFS$ENQUEUE_LIMIT

This parameter is calculated when you configure the server. It specifies the maximum number of VMS locks that the file server can have outstanding at any one time.

The maximum value is 32767.

It is used to define the ENQUEUE_LIMIT qualifier used in the VMS RUN command.

PCFS$EXTEND_BLOCKS

This parameter defines the number of VMS disk blocks (512-bytes) that the file server allocates when it creates or extends a file. By default, files are extended in units of 256 blocks at a time when the file server opens a file.

Since extending a file takes a long time, you do not want to extend a file often.

Before changing this parameter, you need to understand how it affects the VMS DISKQUOTA. The file extent affects the VMS DISKQUOTA when DISKQUOTA is enabled. The VMS DISKQUOTA limits the amount of disk space available to users.

For example, if the file extent is 512, the server allocates 512 blocks to create a file and the available DISKQUOTA is reduced by 512 blocks. Suppose that only five blocks are needed for the file. When the file is extended, all 512 blocks are reserved for the file regardless of whether they are needed. Extending the file may exceed DISKQUOTA although the five blocks required for the file are available. When the file is closed, only the five blocks needed for the file are used.

The maximum value is 65536.

PCFS$EXTENT

This parameter is computed when you configure the server. It specifies the maximum size to which the file server can increase its physical memory.

It is used to define the EXTENT qualifier used in the VMS RUN command.

PCFS$FILE_LIMIT

This parameter is calculated when you configure the server. It specifies the maximum number of files that can be opened by the file server at any one time.

The maximum value is 32767.

It is used to define the FILE_LIMIT qualifier used in the VMS RUN command.

PCFS$IO_BUFFERED

This parameter is calculated when you configure the server. It specifies the amount of system buffered input output operations that the file server can have outstanding at any one time.

The maximum value is 32767.

It is used to define the IO_BUFFERED qualifier used in the VMS RUN command.

PCFS$IO_DIRECT

This parameter is calculated when you configure the server. It specifies the amount of direct input output operations that the file server can have outstanding at any one time.

The maximum value is 32767.

It is used to define the IO_DIRECT qualifier used in the VMS RUN command.

PCFS$LOG_DELAY

This parameter specifies the interval in seconds after which the file server writes messages to the log file. The default log file is PCFS_SERVER.LOG and its location is determined by the logical PCFS$LOG_FILES.

The minimum value is 1 second; the maximum value is 300 seconds.

PCFS$LOCK_WAIT

Locks are used to coordinate access to files. When some applications request a lock, the server puts a lock on the requested portion of the file, so that other users cannot access the same portion.

The lock wait is the delay the server waits before responding to failed requests for locked data. Many applications request data in rapid succession. If the request fails, these applications automatically repeat the request. For each repeated request, the file server waits to send responses to the client until the lock wait time has expired.

The PCFS$LOCK_WAIT parameter reduces traffic on the server by delaying the response to the client. It also improves server performance by processing fewer client requests.

If data is unlocked during the the lock wait time, the file server returns a success message on the lock request.

The minimum value is 1; the maximum value is 3000 milliseconds.

PCFS$MAXIMUM_WORKING_SET

This parameter is calculated when you configure the server. This parameter specifies the maximum size of the working set that the file server requires to support the number of workstations and the file server cache size.

It is related to the VMS SYSGEN parameter WSMAX and the MAXIMUM_WORKING_SET qualifier used in the RUN command.

PCFS$NUM_OF_WORKSTATIONS

This parameter specifies the number of workstations allowed to connect to the file server at the same time. Configuring the server allocates the VMS resources required to support the number of workstations specified.

The minimum value is 1 for this parameter.

The maximum depends on the cache size, the available memory, and the number of open files for each workstation.

PCFS$OPEN_FILES_PER_WKST

It represents the average number of open files for each workstation. Although it does not limit the number of files each user can open, it limits the total number of files the server can open for **all** users.

This parameter affects the the PCFS$NUM_OF_WORKSTATIONS and PCFS$CACHE_SIZE parameters.

This parameter affects the SYSGEN parameter CHANNELCNT.

The minimum value is 1 and the maximum value is 40.

PCFS$PAGE_FILE

This parameter is calculated when you configure the server. It specifies the number of free pages in the system page file the file server requires to support the number of workstations and the cache in the server configuration. It is used to define the PAGE_FILE qualifier used in the VMS RUN command.

PCFS$PERCENT_AVAIL_MEM

This parameter is used to calculate the maximum physical memory that can be used in maximizing file server resource calculations. This is a percentage value.

For example, if the node has 16384 pages (8Mb) and VMS occupies 3499 pages, then the maximum memory that will be used in calculations is as follows:

- Maximum physical memory available 16384 - 3499 = 12885
- The server configuration uses:

  12885 x PCFS$PERCENT_AVAIL_MEM)/100

  For example, if PCFS$PERCENT_AVAIL_MEM = 80, the server configuration uses (12885 x 80)/100 = 10308 pages

If the maximum memory is greater than 80 percent of the physical memory, then there is a possibility of POOL EXPANSION FAILURE due to an increase in SYSGEN WSMAX parameter value during the AUTOGEN process.

PCFS$QUEUE_LIMIT

This parameter is calculated when you configure the server. It specifies the maximum number of VMS timer queue entries that the file server can have outstanding.

The maximum value is 32767.

It is used to define the QUEUE_LIMIT qualifier used in the VMS RUN command.

PCFS$SPTREQ

This parameter is calculated when you configure the server. The file server maps some of its structures into VMS system space and therefore requires system pages. This parameter specifies the *contiguous* system page table entries required by the file server.

It is related to the VMS SYSGEN parameter SPTREQ.

G

How Required VMS System Parameters Are Calculated

The file and disk server use VMS system resources. The specific resources and the amount used depend on the server configuration (see Chapter 7 and Chapter 8) and are automatically computed by the configuration procedure. You do not need to calculate the required resources yourself. But, to understand how PATHWORKS for VMS server uses VMS system resources, this appendix explains the formulas used for the following VMS system resources:

- WSMAX
- SPTREQ
- CHANNELCNT
- System page file size
- NPAGEDYN

When you complete the server configuration, the files are stored as follows:

- Computed system parameters are stored in the PCFS$MODPARAMS.DAT file.
- New PCFS$MODPARAMS.DAT file is appended to the MODPARAMS.DAT file.

Prerequisite Information

If you want to do the calculations yourself, you need to know the:

- Parameter values from the PCFS$STARTUP_PARAMS.DAT file
- Memory required for LANSDRIVER

Parameter Values in the PCFS$STARTUP_PARAMS.DAT File

You need values for the following parameters in the PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file:

- PCFS$CACHE_SIZE
- PCFS$NUM_OF_WORKSTATIONS
- PCFS$OPEN_FILES_PER_WKST
- PCFS$ADDITIONAL_CHANNELS

In the formulas that follow, substitute the value for each parameter in the PCFS$STARTUP_PARAMS.DAT file. For example, if the PCFS$STARTUP_PARAMS.DAT file contains the line:

```
PCFS$NUM_OF_WORKSTATIONS = 100
```

Then, you would substitute 100 for PCFS$NUM_OF_WORKSTATIONS in the formulas.

Memory Required for LANSDRIVER

Some calculations require that you know the memory requirements for LANSDRIVER, which is the driver for file services using the LAST transport. The amount of memory for LANSDRIVER depends on whether your system is part of a cluster:

- For non-clustered systems:

```
memory required = ( ( (PCFS$NUM_OF_WORKSTATIONS + 10) * 10630) + 25488 ) / 512
```

- For clustered systems:

```
memory required = ( ( ( PCFS$NUM_OF_WORKSTATIONS + 10 ) * 19024 ) + 25488 ) / 512
```

WSMAX Parameter

The WSMAX parameter is the sum of:

- The memory required for LANSESS
- The additional amount of memory, in pages, required by the file server for each workstation that connects to the server:

  ```
  (PCFS$NUM_OF_WORKSTATIONS + 10 ) * 20
  ```

- 1024, the size of the file server process

- PCFS$CACHE_SIZE

SPTREQ Parameter

To calculate the SPTREQ parameter, first find the number of free SPTs, as follows:

1. Log in to the system account or a privileged account to run the System Dump Analyzer (SDA).
2. Enter the following to start the SDA:

   ```
   $  ANALYZE/SYSTEM
   ```

3. Enter the following at the SDA prompt:

   ```
    SDA>  EXAMINE @LDR$GL_SPTBASE+168
   ```

   Number of free SPTs

   This command displays information similar to the following:

   ```
   80D53968:  00000B5E   "^..."
   ```

   In the above example the number of free SPTs is 00000B5E.

4. Convert the number of free SPTs to decimal form. For example:

   ```
    SDA>  EVAL B5E
   ```

   The system displays information similar to the following:

   ```
   Hex = 00000B5E   Decimal = 2910         BUG$_INVCTERMMSG+0028E
   ```

   In this example, the number of free SPTs is 2910.

   Number of mapped SPTs

5. To obtain the number of SPTs mapped by the file server, translate the PCFS$MAPPED_SPT logical:

   ```
   $  SHOW LOGICAL PCFS$MAPPED_SPT
   ```

   The system displays information similar to the following:

   ```
   "PCFS$MAPPED_SPT" = "1487" (LNM$SYSTEM_TABLE)
   ```

6. Compute the SPTREQ parameter as follows:

   - If the file server is not running:

```
SPTREQ = PCFS$CACHE_SIZE + memory for LANSESS - free SPTs (from step 4)
```

   - If the file server is running:

```
SPTREQ = PCFS$CACHE_SIZE + memory for LANSESS  - PCFS$MAPPED_SPTS - free SPTs
```

CHANNELCNT Parameter

To compute the CHANNELCNT parameter:

Number of mounted disks

1. Find the number of mounted disks by entering:

   ```
   $ SHOW DEV D/MOUNTED
   ```

2. Compute the number of channels for the cluster:

   Number of channels for the cluster

   - If the node is not in a cluster, substitute 0 for the channels for the cluster.
   - If the node is in a cluster:
     a. Find the number of nodes in the cluster by entering:

        ```
        $ WRITE SYS$OUTPUT "" F$GETSYI("CLUSTER_NODES")'"
        ```

     b. Substitute the number of nodes (step a) in the equation:

```
channels for cluster = ( 2 * number of nodes in cluster ) - 1
```

3. Compute the CHANNELCNT parameter using the following equation:

```
CHANNELCNT =   21 + Channels for cluster (step 2b) + PCFS$ADDITIONAL_CHANNELS +
               Mounted disks (step 1) + PCFS$NUM_OF_WORKSTATIONS * (PCFS$OPEN_FILES + 1)
```

System Page File Size

To compute the required page file size:

Page file size in use

1. Determine the system page file in use:

   ```
   $ SHOW MEM/FILE
   ```

   Information similar to the following is displayed:

```
              System Memory Resources on 12-AUG-1991 16:41:10.05

Paging File Usage (pages):                          Free  Reservable      Total
  DISK$SERVR1SYS:[SYS0.SYSEXE]SWAPFILE.SYS          3000        3000       3000
                                                    1592        1592       1592
  DISK$SERVR1SYS:[SYS0.SYSEXE]PAGEFILE.SYS         25185     -185488      50800
                                                   26126     -217151      58992
```

2. Determine the maximum of:
   - PCFS$NUM_OF_WORKSTATIONS * 40
   - 4000

3. Determine the page file size required:

   a. For a standalone system, use the following formula:

   ```
   pagefile size required = WSMAX + maximum  (from step 2)
   ```

   b. On a cluster, use the following formula:

```
pagefile size required = WSMAX +  maximum (from step 1) + (100*PCFS$NUM_OF_WORKSTATIONS)
```

NPAGEDYN Parameter

To determine the NPAGEDYN value for the server:

Nonpaged dynamic memory in use

1. Determine the amount of memory currently in use:

   ```
   $  SHOW MEM/POOL
   ```

   This command displays information similar to the following:

```
System Memory Resources on 14-JAN-1991 12:53:13.45

Fixed-Size Pool Areas (packets):   Total        Free      In Use        Size
 Small Packet (SRP) List            612         213        399           96
 I/O Request Packet (IRP) List      390         229        161          176
 Large Packet (LRP) List             42          19         23         1648

Dynamic Memory Usage (bytes):       Total       Free      In Use     Largest
 Nonpaged Dynamic Memory           822272     106064     716208       40272
 Paged Dynamic Memory              290816      95744     195072       91856
```

2. Check the display for the value specified in the In Use column for Nonpaged Dynamic Memory.

3. Note the values for the SYSGEN parameters:

   - NPAGEVIR
   - NPAGEDYN

Find the number of disk services.

4. Find the number of disk services by entering:

   ```
   $ ADMIN/PCSA SHOW DISK_SERVER SERVICES
   ```

   Multiply the number of disk services by 800.

5. The following calculations determine the value for NPAGEDYN.

Memory available

   The memory available is equal to:

   ```
   NPAGEVIR - Nonpaged Dynamic Memory In Use (step 2)
   ```

   The memory required for PATHWORKS for VMS is 40000 bytes.

```
memory  needed = 40000 + disk services * 800
```

Memory needed

```
n = memory  available - memory needed
```

6. If n is greater than or equal to 0, NPAGEDYN is not changed. If n is less than 0, NPAGEDYN is adjusted as follows:

```
MIN_NPAGEDYN = NPAGEDYN - ( n / 3)  + 256
```

H

Managing VAXmate Clients

When you upgrade your server, VAXmate clients can continue to connect to the server. The server must have the Version 2.2 client software on a system virtual disk called PCSA$DOS_SYSTEM_V22. The VAXmate clients connect to and use the software on PCSA$DOS_SYSTEM_V22. Any clients running Version 2.2 client software continue to work as always.

Managing VAXmate clients on a Version 4.0 server involves some steps that differ from the management of Version 4.0 clients on the Version 4.0 server. Managing Version 2.2 clients can involve:

- Changing the client configuration to change the services the client uses, as needed
- Changing the Ethernet address if you install new Ethernet controllers
- Adding new VAXmate clients to the Version 4.0 server

To reconfigure or add a client that boots locally (from the hard disk or diskette) run the Netsetup utility. However, to reconfigure or add a client that remote boots, you need to use the PCSA Manager commands and the Netsetup utility.

The Version 2.2 *Configuring Clients at the Workstation* manual provides information on running the Netsetup utility to configure clients for local boot. This chapter discusses managing VAXmate clients that boot from a Version 4.0 server.

Specifically, the chapter explains:

- How to reconfigure a VAXmate client
- How to change the Ethernet address in a VAXmate client profile

- How to configure a new VAXmate client running DECnet/PCSA client Version 2.2 software for remote boot from a PCSA Version 4.0 server
- The PCSA Manager ADD WORKSTATION command syntax

Reconfiguring a VAXmate Client

To change the types of services a client can connect to, reconfigure the client profile using the Netsetup utility. When reconfiguring a Version 2.2 client that boots from a Version 4.0 server, you must run the Version 2.2 Netsetup utility, which is on the Version 2.2 system disk, PCSA$DOS_SYSTEM_V22. To reconfigure a Version 2.2 client, follow these steps at the client:

1. With the USE command, connect to the Version 2.2 system disk.

   If you are using Version 4.0 client to reconfigure a Version 2.2 client, you must disconnect from the current system service and reconnect, using the same drive letter, to the Version 2.2 system disk. For example:

   ```
   C:\>  USE J: /D
   C:\>  C:\DECNET\USE J: \\LETTER\PCSA$DOS_SYSTEM_V22 /V
   ```

   The commands in the preceding example:

   - Disconnect the client from the current system service
   - Connect the client to the Version 2.2 system virtual disk, using the DECnet subdirectory on drive C.

2. With the USE command, connect to the client remote boot service, which is identified by the client Ethernet address. The **remote boot service** is virtual disk on which you are storing the client profile. For example:

   ```
   C:\>  USE G: \\LETTER\02-00-2B-01-22-78
   ```

   This command connects to the client remote boot service on the server LETTER.

3. Change directories to the DECnet subdirectory on the Version 2.2 system virtual disk. For example:

   ```
   C:\> J:
   J:\> CD DECNET
   J:\DECNET>
   ```

4. Run the Netsetup utility and make the changes to the client profile. When you have checked the new client profile and are ready to modify the key disk, the Netsetup utility prompts you for the destination drive.
5. Enter the drive letter for the client remote boot service. In the example, the drive letter for the client remote boot service is G.

   The Netsetup utility writes the boot media to the virtual disk, reconfiguring the remote boot disk for the client.
6. Exit from the Netsetup utility.
7. Reboot the client to test the configuration. If the client does not connect to and boot from the server, reconfigure the client. If necessary, use the diagnostic diskettes to check the network connection between the client and the server.
8. Reboot the client for the new configuration to take effect.

Changing the Ethernet Address

If you change the Ethernet controller installed on a VAXmate client, update the client profile to include the new Ethernet address. From the server, enter the PCSA Manager MODIFY WORKSTATION command to change the Ethernet address.

Note

The MODIFY WORKSTATION command requires OPER, SYSPRV and BYPASS privileges.

The MODIFY WORKSTATION command has the following format.

Format

```
MODIFY WORKSTATION   nodename
                    /DEVICE=VAX-ethernet-adapter
                    /ADAPTER=(TYPE=PC-Ethernet-adapter,
                    ADDRESS=hardware-address)
                    /CLIENT_VERSION=pcsa-version
                    /COMMENT=string
```

Parameters

nodename

The network node name is 1 to 6 alphanumeric characters, with at least one alphabetic character.

Qualifiers

/DEVICE=VAX-Ethernet-adapter

An optional qualifier that specifies the Ethernet adapter on the server. If you do not include this qualifier, PCSA Manager determines the type of adapter installed on the server.

/ADAPTER=(TYPE=PC-Ethernet-adapter, ADDRESS=hardware-address)

Specify the Ethernet adapter installed in the client and the hardware address for the adapter.

For the adapter, specify one of the following:

- DEPCA
- LANCE
- 3C501
- 3C503
- 3C523
- NI5010

/CLIENT_VERSION=pcsa-version

Use this qualifier to specify the client software version. For Version 2.2, use 22.

/COMMENT=string

Use this qualifier to include a comment that describes the client. The comment can be up to 17 characters. The comment is displayed when you use the SHOW WORKSTATIONS command.

Example

```
PCSA_MANAGER> MODIFY WORKSTATION  WOOLFE -
_PCSA_MANAGER>  /ADAPTER=(TYPE=DEPCA,ADDRESS=02-60-8C-02-22-78) -
_PCSA_MANAGER>  /CLIENT_VERSION=22 /COMMENT=VXSYS33
```

This example changes the Ethernet address of the client WOOLFE, which has a newly installed DEPCA Ethernet adapter.

Adding a VAXmate Client for Remote Boot

You can configure a VAXmate client for remote boot on a Version 4.0 server. Before you configure the client for remote boot, you need the following information:

- The DECnet node name for the client
- The DECnet node address for the client
- The Ethernet hardware address for the client
- The type of Ethernet controller installed on the client
- The type of DOS the client uses and how that DOS is identified on the server
- How much space to set aside for the boot disk

To configure a newly installed client, follow these steps:

1. Create the virtual disk for the client remote boot service with the ADD WORKSTATION command
2. Configure the client with the Netsetup utility

This section explains how to complete each step.

Creating the Virtual Disk for Remote Boot

To create the virtual disk for the boot media, use the PCSA Manager ADD WORKSTATION command. The ADD WORKSTATION command requires OPER, SYSPRV, and BYPASS privileges, and has the following format.

Format

```
ADD WORKSTATION  nodename node-address comment
                 /DEVICE=VAX-ethernet-adapter
                 /ADAPTER=(TYPE=PC-Ethernet-adapter,
                 ADDRESS=hardware-address)
                 /DOS=installed-dos-name
                 /CLIENT_VERSION=pcsa-version
                 /SIZE=boot-disk-size
```

Parameters

nodename

The 1- to 6-character DECnet node name registered for the client.

node-address

The node address for the client is made up of the area number (from 1 to 63) and local number (from 0 to 1023) in the format xx.xxxx.

comment" "

Use this parameter to include a comment that describes the client. Enclose the comment in quotation marks. The comment can be up to 17 characters long. The comment is displayed when you use the SHOW WORKSTATIONS command.

Qualifiers

/DEVICE=VAX-Ethernet-adapter

An optional qualifier that specifies the Ethernet on the server. If you do not include this qualifier, PCSA Manager determines the type of adapter installed on the server. The Ethernet controller on a VMS server is used to service MOP requests for the client. Use this qualifier only if the server does not recognize the Ethernet controller.

/ADAPTER=(TYPE=PC-Ethernet-adapter, ADDRESS=hardware-address)

Specify the Ethernet adapter installed in the client and the hardware address for the adapter.

For the adapter, specify one of the following:

- DEPCA
- LANCE
- 3C501
- 3C503
- 3C523
- NI5010

/DOS=installed-dos-name

The name you gave DOS when you copied it to the server using the DOSLOAD utility. This qualifier identifies the type and version of DOS that you want the client to use.

/CLIENT_VERSION=pcsa-version

Use this qualifier to specify the client software version. For Version 2.2, specify 22.

/SIZE=boot-disk-size

This qualifier sets the size of the virtual disk you are creating. Specify a size that equals the size of diskette drive A on the client. Specify one of the following:

- 360 Kbytes
- 720 Kbytes
- 1.2 Mbytes
- 1.44 Mbytes

The default size of the virtual disk is 360 Kbytes.

Example

```
PCSA_MANAGER>  ADD WORKSTATION BRONTE 8.765 -
_PCSA_MANAGER> "COMPAQ_CQV33_1.22MB"  -
_PCSA_MANAGER> /ADAPTER=(TYPE=LANCE, ADDRESS=02-60-8C-01-22-78) -
_PCSA_MANAGER> /DOS=VXSYSV33/CLIENT_VERSION=22 /SIZE=1.2MB
```

The command in this example sets aside a 1.2 Mbyte virtual disk to be used by the following type of client:

- A COMPAQ
- DECnet node name: BRONTE
- DECnet node address: 8.765
- Ethernet address: 02-60-8C-01-22-78
- An installed DEPCA Ethernet controller
- Running VAXMATE DOS Version 3.3
- Running DECnet/PCSA Client Version 2.2 software from the server

Configuring a Client for Remote Boot

After you create the virtual disk, you can configure the client with the Version 2.2 Netsetup utility. The Netsetup utility writes the profile to the virtual disk you created. The virtual disk becomes the network key disk for the client.

To configure the client, follow these steps:

1. At the client, connect to the Version 2.2 system disk with the USE command.

   If you are using Version 4.0 client to reconfigure a VAXmate client, you must disconnect from the current system service and reconnect, using the same drive letter, to the Version 2.2 system disk. For example:

   ```
   C:\>  USE J: /D
   C:\>  C:\DECNET\USE J: \\LETTER\PCSA$DOS_SYSTEM_V22 /V
   ```

   The commands in the example:

   a. Disconnect the client from the current system service

   b. Connects the client to the Version 2.2 system virtual disk, using the DECnet subdirectory on drive C.

2. Connect to the virtual disk you created for the client boot device. For example:

   ```
   C:\>  USE G: \\LETTER\2-60-8C-01-22-78/V
   ```

   The USE command in the example connects the client to the virtual disk set aside for the remote boot service and assigns the drive letter G to the disk.

3. Change directories to the DECnet subdirectory on the Version 2.2 system virtual disk. For example:

   ```
   C:\> J:
   J:\> CD DECNET
   J:\DECNET>
   ```

4. Run the Netsetup utility from the server. The Version 2.2 Netsetup utility is stored on the system virtual disk, PCSA$DOS_SYSTEM_V22. For example, enter:

   ```
   J:\DECNET>  NETSETUP
   ```

5. Answer the prompts displayed by the Netsetup utility. For information, see *Configuring Clients at the Workstation*, which is part of the Version 2.2 documentation set.

When you have checked the client profile and are ready to write the key disk, the Netsetup utility prompts you for the destination drive.

6. Enter the drive letter for the virtual disk you created with ADD WORKSTATION command. In the example, the drive letter for the client boot device is G.

   The Netsetup utility writes the boot media to the virtual disk, creating the network key disk for the client.

7. Exit the Netsetup utility.

8. Reboot the client to test the configuration. If the client does not connect to and boot from the server, reconfigure the client. If necessary, use the diagnostic diskettes to check the network connection between the client and the server.

Glossary

The terms that appeared in the text of this book in **boldface** are explained in this glossary. Additional computer-related terms are also explained here.

access (v.)

To use a resource, such as a printer, directory, or disk drive.

access control (n.)

The mechanism for validating the right to use a resource or service, such as a connection, logon, or file access, stored on or connected to a server. A user name and password combination is the most common means of access control.

access control entry (ACE) (n.)

In a VMS access control list (ACL), one identifier and its associated access rights to a service or resource. See also *access control list.*

access control list (ACL) (n.)

In the VMS environment, a list that defines users' rights to use a resource, file, or service.

account (n.)

A set of information on a computer system that allows users access to a multiuser or networked computer. It includes the user's name, often a password, other identifiers, a list of services and privileges the user is allowed, and files belonging to the user.

ACE (n.)

See *access control entry.*

ACL (n.)

See *access control list.*

actual length (n.)

The length of a VMS file in bytes as determined by the file server. See also *estimated length.*

adapter name (n.)

A unique name given to an application. Adapter names are used by NETBIOS applications communicating over the network. See also *remote adapter name.*

alias (n.)

An alternate name for a resource, such as a service, used to refer to several identical resources by the same name. It is also used to refer to the same service by alternate names.

API (n.)

See *application programming interface.*

append path (n.)

A search path that is used to tell DOS where to search for executable files in the directory structure. See also *path name* and *search path.*

application (n.)

A program used for a particular kind of work, such as word processing or database management.

application disk service (n.)

A virtual disk that contains application software. See also *disk service.*

application file service (n.)

A file service that contains application software.

application package (n.)

A set of software application programs that can be used individually or can be shared.

application programming interface (API) (n.)

A standard or proprietary software interface with a network or operating system. Examples of APIs are NETBIOS and Basic LAN Manager.

area (n.)

In networking, a group of interrelated nodes.

ASCII (n.)

American Standard Code for Information Interchange. A set of 8-bit, binary numbers representing the alphabet, punctuation, numerals, and other symbols used to represent text.

Also, a file that is in binary format. See also *binary.*

asynchronous communication (n.)

The method of transmitting data one character at a time over a serial interface. Asynchronous communication can work locally or through a modem. Timing between bits is constant; timing between characters is variable. (Also called start-stop transmission.)

back up (v.)

To copy the contents of an entire disk, directory, or file.

backup (n.)

A copy of the contents of an entire disk, directory, or file.

binary (adj.)

Pertaining to a numbering system that uses a base of 2; it uses only two digits, 1 and 0.

Also, a file type that is in binary format. See also *ASCII.*

boot (v.)

Short for bootstrap. To run or initiate a program that loads the operating system into memory and starts or restarts the computer.

boot image (n.)

The minimum set of instructions needed to start and run a computer, including device drivers, directory structures, and memory management; also, the file containing these instructions.

boot media (n.)

The diskette, hard disk, or virtual disk that contains the startup files. See also *key diskette* and *network key disk.*

broadcast message (n.)

A message sent to personal computer users on the network. Users cannot respond to this message.

Broadcast utility (n.)

A program that enables one-way communication to personal computer users on the network.

burst page (n.)

On a line printer, a page that identifies an individual print job. In continuous-form printing, a burst page is usually printed between individual print jobs. See also *flag page* and *trailer page.*

button (n.)

An on-screen control that users can click on to choose an action or option or to set a state.

cache (n.)

See *cache memory.*

cache hit rate (n.)

The percentage of time the requested data is already in cache memory. See also *cache memory.*

cache memory (n.)

High-speed memory that contains copies of data recently used by the processor. Cache memory fetches several bytes of data from main memory (which is slower) in anticipation that the processor will require the next series of bytes in the sequence.

In networking, cache memory avoids frequent disk input/output over the network, providing faster operation. This use of cache memory stores data in main memory.

client (n.)

A personal computer or workstation, connected to the network with PATHWORKS, that can access resources on a server. A client can have DOS, OS/2, or Macintosh software.

Also, hardware or software that receives resources from a server. See also *server*.

close (v.)

In printing, to send an application's print request to the printer assigned to the application.

command (n.)

An instruction issued to a computer operating system or application.

command line (n.)

That area of the screen in which commands are entered and displayed.

common file service (n.)

A file service used to store files that many users can share and update. An example of a common file service is PCCOMMON.

configuration (n.)

The set of hardware, hardware options, and software on a computer or network.

configure (v.)

To select, install, and customize hardware and software for a computer or network.

CPU (n.)

Central processing unit. The main unit of a computer that contains the circuits controlling interpretation and execution of instructions. The CPU includes the main storage, arithmetic unit, and special registers.

current directory (n.)

The directory in which you are currently working. Sometimes called the default directory.

DCL (n.)

Digital Command Language. The standard command interface to Digital's major operating systems, such as VMS.

DECconnect (n.)

A structured cabling system that provides lines for data transmission on Ethernet networks.

DECnet (n.)

Digital networking software that runs on server and client nodes in both local area and wide area networks. With DECnet, different types of computers that have different operating systems can be connected, and users can access information and services on a remote computer.

DECnet is a networking protocol and transport. See also *TCP/IP.*

DECnet node database (n.)

The file that contains information about the network nodes with which a computer communicates.

default (n.)

The value assumed by a program if a value is not supplied by the user.

device (n.)

A hardware component that performs a specific function. A keyboard is an input device; a printer is an output device; a terminal is an input/output device. See also *logical device.*

device control library (n.)

A VMS text library that contains two or more files. For example, one file sets a printer to the default mode; the other file establishes an alternate mode for the the printer (for example, portrait, landscape, or enhanced mode).

device driver (n.)

See *driver.*

directory (n.)

A list of a set of files stored on a storage device such as a file service or disk.

disk server (n.)

A network program that allocates space on a VMS disk where DOS users can store, create, and maintain DOS files. This space is called a virtual disk. Disk services are available only on VMS servers accessed with the DECnet transport. See also *disk service* and *virtual disk.*

disk service (n.)

A service located on a VMS server that looks like a VMS file on a server, and lets users access it as if it were a local DOS disk drive. The service may contain more than one DOS file. A disk service gives multiple users fast access to read-only files, and gives one user fast access to read-write files. See also *disk server.*

driver (n.)

A background software program typically dedicated to the control of a device or resource on a personal computer. For example, a mouse requires a mouse driver.

enhanced (adj.)

Pertaining to a printing specification for a form or mode. See also *landscape* and *portrait.*

environment variable (n.)

In DOS, a name or a number you define with the DOS SET command.

In a startup batch file, such as STARTNET.BAT, some environmental variables are set every time you boot. For example, the following USE command sets the environment variable DRV (drive) to the value returned by the command. It connects the DOS_SYSTEM service to the returned drive when you start the computer:

```
USE ?: DOS_SYSTEM/VIRTUAL/ENVIRON=DRV
```

estimated length (n.)

In VMS, the file length based on the position of the end-of-file pointer. See also *actual length.*

Ethernet address (n.)

An alphanumeric string, six bytes in length, that identifies a node on the Ethernet. The string is six pairs of hexadecimal digits, separated by hyphens (for example, AA–00–04–00–91–27).

Ethernet controller (n.)

A network controller for the transmission and reception of data between a workstation or server and the Ethernet network. For example, a DEPCA is an Ethernet controller for a personal computer that is connected to the network. See also *network controller.*

file server (n.)

A network program that lets a client connect to available file and printer services.

file service (n.)

Directories, subdirectories, and files on a file server. Users can use network commands from a client to access a file service and then store and retrieve data. A file service provides read/write access to applications and services for many users simultaneously. See also *shared directory.*

flag page (n.)

A cover sheet produced at the start of a printed file. The flag page identifies the file, usually stating the name of the file, the account printing the file, and the job number. See also *burst page* and *trailer page.*

form (n.)

In printing, a characteristic that specifies the physical layout of the page. Types of forms are landscape, portrait, and enhanced.

format (v.)

In the context of disks, to divide a disk into tracks and sectors, label those tracks and sectors for future reference, and create a directory structure in order to make the disk ready to accept new data and programs. The type of formatting done depends upon which operating system will use the disk. Formatting a disk destroys any data previously stored on the disk.

generic queue (n.)

A logical name for a physical queue. See also *physical queue.*

group (n.)

In system administration, a collection of users who have the same access to file services. Once users have accounts, they can be assigned to a group. With one command, the system administrator can assign and modify access for all users in the group.

group code (n.)

A number or set of numbers used by the LAT or LAST protocol to identify network resources and to control access to those resources. Group codes can be used to assign resources to a specific set of users and to balance the load between computers offering identical services. (Also called group code number.)

key diskette (n.)

A diskette that is used to start up the personal computer or workstation and make network connections. The key diskette stores files with configuration information, optional user-specific information, and some DOS utilities. The key diskette is a type of boot media. See also *boot media* and *initial workstation diskette.*

LAD (n.)

Local area disk. Digital's virtual disk software on a local area network. LAD provides high-performance disk services to DOS and OS/2 clients connecting to a VMS server. See also *virtual disk.*

LAN (n.)

Local area network. A self-contained network that offers a high-speed, reliable communication channel. LANs span a limited distance, such as a building or cluster of buildings, but can be connected to WANs with bridge devices.

landscape (adj.)

In printing, pertaining to a VMS form in which the text or image is parallel to the long side of the paper. See also *enhanced* and *portrait.*

LAST (n.)

Local Area System Transport. The network protocol used by the virtual disk server to send and receive data between computers. LAST provides LAN services to LAD drives.

LAT (n.)

Local Area Transport. A character-oriented transport protocol that operates on a LAN to permit communication between nodes and other devices such as terminals, printers, and modems. See also *LAN* and *SETHOST.*

LATCP (n.)

LAT Control Program. A utility that allows the management of LAT services from the client.

load (v.)

To bring software into memory. See also *downline load.*

load file (n.)

A file with information about the Ethernet controller that is installed in a specific client. The load file is used for remote boot.

local (adj.)

Stored on or connected to a client computer, such as a file or a printer. Local is the opposite of being available over a network. See also *remote.*

local area disk (n.)

See *LAD.*

Local Area Transport (n.)

See *LAT.*

local boot (n.)

A process in which a client operating system is loaded and started locally from either the hard disk or a key diskette. See also *remote boot.*

local printer (n.)

A printer that is connected directly to a client. See also *remote printer.*

log file (n.)

A text file that contains messages describing events that occur during operation. Log files are updated frequently during operation and are useful for tracing system operation and errors. Log files are created by file servers, X servers, and many applications and utilities.

logical (adj.)

Nonphysical. For example, logical can refer to a name in the software that represents a hardware device. (Also called logical name.) See also *logical device.*

logical device (n.)

A software name that identifies a hardware device for use by an application or program.

log on (v.)

To enter a user name and a password that identify the user and start the session. (Also called log in.)

LPT1, LPT2, LPT3 (n.)

The default logical device names for local parallel printers. LPT1 is the default logical identification for the client local printer port.

module (n.)

In a device control library, the portion of the library that defines a form or mode for a particular device.

mount (v.)

To make a virtual disk available as a disk service to users on a network.

network (n.)

A group of servers, clients, and devices that are connected to each other by communications lines to share information and resources.

network adapter (n.)

See *network controller.*

network controller (n.)

A combination of hardware, firmware, and software that controls the transmission and reception of data between a workstation or server and the network. For example, a DEPCA is an Ethernet network controller that connects a personal computer to the network. (Also called network adapter.)

Network Control Program (NCP) (n.)

A DECnet utility used to monitor, manage, and configure network nodes.

network key disk (n.)

A virtual disk that enables a client to boot over the network by loading the operating system and network startup information to the client. A network key disk is a type of boot media. See also *boot media* and *remote boot.*

node (n.)

An individual computer, such as a server or client, that can communicate with other computers in a network.

node address (n.)

A unique numerical identification of a node in a network. A node address includes the area and node number.

node name (n.)

A name uniquely identifying a node within a network. The node name must be alphanumeric and contain at least one alphabetic character.

In DECnet, a valid node name is one to six characters in length. An example of a DECnet node name is SERVR7.

In TCP/IP, a valid node name is one to sixteen characters in length, separated from its domain specification by a period. An example of a valid TCP/IP node name (including a domain specification) is alberteinstein.princeton.edu.

node number (n.)

A number uniquely identifying a specific node in the area.

open file caching (n.)

Storage of a file header in cache memory after the file is closed. See also *cache.*

open file hit rate (n.)

The percentage of time the requested file is already in cache memory. See also *cache hit rate.*

packet (n.)

A group of bits, including data and control elements, that are switched and transmitted together.

parallel (adj.)

In data transmissions, pertaining to a method of information transfer in which all bits in a character are transmitted simultaneously, rather than sequentially, on different lines or channels. See also *serial.*

parallel port (n.)

The hardware component used to connect a client to a device that uses parallel data transmission, such as a parallel printer.

parallel printer (n.)

A printer that has a parallel data communications interface. See also *parallel port.*

parameter (n.)

One or more variables that are passed to a program or command before execution. A parameter can be a file specification, option, or device name.

In the following example, filename.txt and LPT1: are parameters of the NET PRINT command:

```
NET PRINT filename.txt LPT1:
```

See also *qualifier.*

password (n.)

A string of characters that uniquely confirms the identity of a user to the system. See also *user name.*

path name (n.)

A default, predefined sequence of directories to be searched when a program or utility looks for a file. Directory names in the path are separated by semicolons. See also *search path.*

personal computer (n.)

See *client.*

personal file service (n.)

A file service that contains a user's DOS data and text files as well as server files. A personal file service is protected from other users by a user name and a password.

physical queue (n.)

A name that corresponds to the physical terminal line for a printer port. See also *generic queue.*

portrait (adj.)

In printing, pertaining to a VMS form in which the text or image is parallel to the short side of the paper. A standard business letter is in portrait mode. See also *enhanced* and *landscape.*

printer service (n.)

The availability of a printer that is connected to a server. From the client, users run network commands to access a printer service and print files. A file server makes a printer service available to clients. See also *shared printer.*

printer startup file (n.)

A file that runs automatically when the operating system starts all the printers defined in the file.

print queue (n.)

A list to which files are added to be printed on a specific printer.

print symbiont (n.)

A program that controls the flow of data to the printer.

privileges (n.)

The level of access to the system or service that a user is allowed; also, a characteristic assigned to a user or program that determines what operations the user or program can perform.

profile (n.)

A set of information about a client or a user. The profile provides information the server may require to recognize the client or the user.

prompt (n.)

A request to the user from the software for information or an input signal.

protection code (n.)

In the VMS operating system, a means of specifying who has rights to a particular file and the type of rights (for example, read or write).

protocol (n.)

A set of rules that governs the format and timing of messages sent and received over a communication link. For example, DECnet and TCP/IP are network protocols.

public file services (n.)

File services to which users connect using the default account without specifying a user name and password. Users connecting in this way are automatically allowed access to public services.

qualifier (n.)

A portion of a command that modifies the action by setting or selecting one of several options. For example, in the following command, /COPIES is a qualifier with a value of 3.

```
NET PRINT filename.txt LPT1: /COPIES=3
```

See also *parameter.*

rating (n.)

In system administration, a numerical value that assigns a priority to a LAT disk service. Ratings differentiate disk and terminal services that have the same name. When several services have the same name, the disk service with the highest rating is used.

read-write access (n.)

The privilege to copy (read) or save to (write) a file, application, or disk area.

redirect (v.)

To assign a logical device name, which is a local representation of a physical device on the network.

remote (adj.)

Stored on or connected to a server or other computer and available to a client over the network only. Remote is the opposite of local. See also *local.*

remote boot (n.)

A process in which a client's operating system is loaded and started remotely from a network key disk. See also *local boot* and *network key disk.*

remote boot database (n.)

A set of information containing a list of clients that can be started by a network key disk.

remote boot diskette (n.)

A diskette containing the minimum necessary software to connect a personal computer to a server. Once the two are connected, the server can start the personal computer with complete network startup software. A remote boot diskette is required to remote boot any personal computer that does not have a DEPCA Ethernet controller. See also *network key disk.*

remote printer (n.)

A printer connected to a server on the network. See also *local printer.*

resource (n.)

A service that is available to the client; also, a source of information or an available means to complete a task. Examples of network resources are applications, file services, disk services, and printers. Resources can be either local or remote.

save set (n.)

In VMS, a collection of files that have been grouped and saved by a backup utility.

sequential fixed (adj.)

Pertaining to a type of file in which each record has a fixed length of 512 bytes.

server (n.)

A computer running PATHWORKS software that offers file, printer, or disk services to clients. See also *client*.

service (n.)

The availability of files, devices, or disks that let clients access resources on the network or on a server. A service enables a client to use resources on a printer, on the network, or on a server. See also *disk service, file service, print service, shared resource*, and *virtual disk service.*

service name (n.)

A label (name) the user or system administrator gives to a file, printer, or disk service to make any one of these services available to other users. For example, PCCOMMON is the service name of the common file service.

session (n.)

The logical link between a client or terminal and a server.

spool subdirectory (n.)

An area in which each printer service stores files while they wait to be printed.

stream (adj.)

Pertaining to a type of VMS file in which each record ends with a carriage return and line feed.

string (n.)

In a command line, an entry that contains more than one number or word and is enclosed in parentheses or quotation marks. Often, the words in a string are joined with underscores. In the following example, a string follows the equals sign:

```
NET PRINT/NOTE=(Final_draft_of_fiscal_report)
```

submenu (n.)

A menu that is subordinate to the main menu. A submenu is associated with a pull-down or pop-up menu and is displayed in response to dragging the pointer over the submenu icon.

system file service (n.)

A file service offering system software, including PATHWORKS for DOS and PATHWORKS network software, DECwindows Motif software and applications, and the DOS operating system and utilities.

system service (n.)

See *system file service.*

task image (n.)

An executable file loaded into computer memory, especially during a remote boot operation.

TCP/IP (n.)

Transmission Control Protocol/Internet Protocol. A set of protocols that governs the transport of information between computers and networks of dissimilar types. The Internet is a group of networks that includes regional networks and local networks at universities and commercial institutions. TCP/IP is an alternative to the DECnet network transport. See also *DECnet.*

terminal server (n.)

A dedicated communications system on the LAN that provides logical connections between its serial ports and service nodes, using the LAT protocol. A terminal server can access services and, in some cases, offer services. DECservers 100, 200, 300, and 500 are terminal servers. See also *service node.*

Transmission Control Protocol/Internet Protocol (n.)

See *TCP/IP.*

transport (n.)

Network software that routes user data to its destination and controls the flow of data.

UAF (n.)

See *user authorization file.*

UIC (n.)

See *user identification code.*

user authorization file (UAF) (n.)

A VMS file that contains information specifying each user's access rights. See also *access control list* and *user identification code.*

user identification code (UIC) (n.)

A number that determines the type of access (read, write, execute, or delete) for files, mail, and common system commands a user is or is not permitted. See also *access control list* and *user authorization file.*

user name (n.)

The name a user types when logging in to the system. The combination of the user name and password uniquely identifies a user account to the system. See also *password.*

user profile (n.)

Information provided to the server that may be required to recognize the user.

utility (n.)

A general-purpose program included in a system to perform common tasks.

virtual (adj.)

Having the attributes, but not the actual form, of something. For example, a virtual disk is space on a VMS disk that functions as if it were a DOS disk.

virtual disk (n.)

Space the disk server program sets aside on a VMS disk. The virtual disk, actually a VMS container file, functions like a DOS-formatted disk. Users can connect to the virtual disk through a DOS drive and can store, create, and maintain DOS files. See also *LAD*.

VMS server (n.)

A VAX or MicroVAX computer running PATHWORKS for VMS, the VMS operating system, and PATHWORKS server software offering clients network resources such as files, routers, remote printing, and applications.

volatile database (n.)

A file containing information that is not retained when the client or server is rebooted.

volume name (n.)

In VMS, a mass storage medium, such as a disk pack or magnetic tape; also, the largest logical unit of file structure for the contents of the media.

WAN (n.)

Wide area network. Two or more standard or extended LANs that are joined by DECnet routers, gateways, or Packet System Interface (PSI) software.

wide area network (n.)

See *WAN*.

workstation (n.)

See *client*.

Index

A

Access control entries (ACEs), 3–2
Access control lists (ACLs), 1–5, 3–2
Access to files
  See also PCDISK utility
  See also RMS protection
  and RMS protection, 1–5
  in application file services, 3–2
  in common file services, 3–3
  in file services, 1–5
  in virtual disks, 5–17
Access to services
  See also Security
  changing, 3–18
  denying, 3–16, 3–18, 3–19
  disk services, 5–12
  for disk services, 1–3, 5–2, 5–3
  for file services, 3–1
  for printer services, 4–5
  for users, 1–5, 1–6, 3–19
  granting, 3–16, 3–18, 3–19
  group, 1–6, 3–18
  listing for file services, 3–17
  modifying, 5–12
  public, 1–6, 3–17, 3–18
  restricting with group codes, 7–10
  with default account, 6–15
Accounts
  See Default account
  See VMS accounts
Actual length, 3–20, A–4
  term defined, 3–13
ADA programs
ADA programs (Cont.)
  creating files compatible with file server, A–5
Adding
  application disk services, 5–3
  application file services, 3–8
  common file services, 3–6
  disk services, 5–7
  file services, 3–9, 3–11
  file services with actual length, 3–13
  file services with RMS stream format, 3–13
  groups, 6–17
  members to groups, 6–18
  nodes to databases, 11–1
  printer forms, 4–11
  printer services, 4–13
  users, 6–2
  users to groups, 6–18
ADD SERVICE /DIRECTORY command (PCSA Manager), 3–12, 3–13, 3–14
ADD USER command (PCSA Manager), 6–12
ADD WORKSTATION command (PCSA Manager), H–5
Alias
  term defined, 3–20
Application data files
  storing, 1–8
Application disk services
  See also Disk services
  adding, 5–3
  selecting for user, 6–5
Application file services
  See also File services

Application file services (Cont.)
- access to, 3–2
- adding, 3–8
- contrasted with application disk services, 1–7
- contrasted with common file services, 1–4, 1–9, 3–2
- default access, 3–18
- default location for, 3–11
- selecting for user, 6–4

Applications
- *See also* Application file services
- *See also* Common file services
- access by DOS and VMS users, 1–8
- adding to application file services, 3–8
- adding to common file services, 3–6
- adding to disk services, 5–3, 5–7
- and performance, 8–2
- and printer services, 3–14, 3–16, 5–4
- choosing disk or file services for, 1–7
- default location for, 3–11
- designed for local hard disk, 1–8
- guidelines for, 1–7
- installing, 1–7, 3–14, 5–4
- limiting users of, 3–20, 5–2
- program diskette for, 5–5
- redirecting data files in, 1–8
- security in, 3–2
- selecting for user, 6–5
- selecting languages for PCSA applications, 6–6
- storing, 1–7
- using in DOS and VMS, 3–13, A–2, A–7
- with fixed records, 3–13
- with licenses, 1–8, 3–12, 5–2

Assigning
- disk service ratings, 5–14
- passwords in VMS accounts, 6–3
- passwords to virtual disk, 5–10
- VMS priority for file server, 8–13

AUTHORIZE command (VMS)
- and passwords, 6–14
- and UIC groups, 6–17
- changing passwords, 6–14, 6–15

AUTOEXEC.BAT file

AUTOEXEC.BAT file (Cont.)
- and GRAPHICS command, 6–5

AUTOGEN procedure (VMS), 7–4, 7–8, 8–10, 8–15, 8–16

AUTOUSER.BAT file, 6–1, 6–6
- and group codes, 7–12
- changing, 6–7
- connecting to services, 6–4
- customizing editors, 6–6
- editing, 6–1
- modifying, 6–6

B

Backing up
- disk services, 9–16
- file services, 9–16
- PATHWORKS Server 3100 system, 12–2
- user accounts, 9–16
- using the PCSA Manager Menu, 9–16
- using the VMS BACKUP command, 9–18

BACKUP command (VMS), 9–18
- incremental backups, 9–18

Backup log file
- printing, 9–17

BASIC programs
- creating files compatible with file server, A–5

Binary files
- using in file services, A–4, A–7

Blank pages
- preventing on non-postscript printers, 4–20

Boot database
- restoring, 11–4

Broadcast utility
- sending messages, 10–1, 10–2
- setting up for clients, 10–2

Byte-range locking, 9–11

C

Cache, 8–2
  and closing files, 8–8
  and stream files, 8–2
  availability of, 8–5
  buffer size, 8–8
  data file for, 8–3, 8–4
  increasing on file server, 8–5, 8–7
  on disk server, 8–13
  on file server, 8–3, 8–4
  open file, 8–2, 8–4, 8–7
  size of, 8–7
  system parameters required for, 8–13, 8–14
  term defined, 8–1
Cache hit rate, 8–14
  term defined, 8–5
Cache parameters
  for disk server, 8–14
  for file server, 8–6
Carriage control information
  in DOS, A–1, A–4
  in VMS, A–1, A–4, A–7
Carriage return
  See Carriage control information
Changing
  See also Modifying
  access to file services, 3–18
  maximum disk services, 7–7
  number of clients, 7–4, 9–5
  number of connections to file services, 9–4
  open files, 9–5
  RMS protection on files, 3–6
  timeout on disk server, 7–9, 9–13
CHANNELCNT parameter, F–1, F–6
Client operating systems
  listing, 11–4
Clients
  See also Personal computers
  changing number of, 7–3, 7–4, 9–5
  connecting to services at startup, 6–4
  listing with file service connections, 9–2
Clients (Cont.)
  maintaining, 11–1
  on file server, F–5
  VAXmate clients, H–1
  Version 2.2 DECnet/PCSA Clients, H–1
CLOSE FILE_SERVER FILE command (PCSA Manager), 9–4
Closing
  open files, 9–4
Clusters, 9–10
  and file server priority, 8–13
  database for, 9–11
  file server log file and, 9–11
  limiting disk services in, 5–2, 9–15
  managing disk services in, 9–14
  sharing files, 9–10
COBOL programs
  creating files compatible with file server, A–5
Common directories
  See Common file services
Common file services
  access to, 3–2, 3–5
  adding, 3–6
  and RMS protection on files, 3–9
  client connections to, 6–4
  contrasted with application file services, 1–4, 1–9, 3–2
  default location for, 3–11
  security, 3–2
  selecting for user, 6–4
Configuring
  disk servers, 7–7
  file servers, 7–2
  Local Area System Transport (LAST), 7–9
  VAXmate clients, H–1
Connecting to services, 1–5
  and printer output, 4–24
  at client startup, 6–4
  granting access to, 1–4, 3–16, 3–17
  to application file services, 3–14
  to common file services, 3–14
  to disk services, 5–4
  using default account, 1–5, 3–5, 3–17
Connections

Connections (Cont.)
limiting for disk services, 5–2
limiting for file services, 3–12, 3–20, 9–4
listing file services, 9–2
specifying for client startup, 6–4
C programs
creating files compatible with file server, A–5
CREATE DISK command (PCSA Manager), 5–8, 5–10, 5–13
Creating
See also Adding
forms, 4–11
groups, 6–17
printer startup file, 4–5
virtual disks, 5–7
VMS accounts, 6–1

D

Data caching, 8–7
Data files
for applications, 1–8
DECnet address
defining on server, 11–1
DECnet database
adding nodes to, 11–1
deleting nodes from, 11–2
restoring, 11–4
DECnet nodes
defining on server, 11–1
displaying on print jobs, 4–24
DECservers
setting up printers on, 4–16
Default account, 3–5, 3–17, 6–15, 6–18
and printer output, 4–24
changing name of, 6–16
connecting to services, 1–5, 1–6, 3–5
disabling, 6–15
Default allocation
for virtual disks, 5–9
Default locations
for file services, 3–11, 3–12
for virtual disks, 5–7
Default responses, 2–5
Defining
forms, 4–11
group codes for servers, 7–11, 7–12
virtual disk location, 5–7
DELETE DISK command (PCSA Manager), 5–16
Deleting
disk services, 5–15
file services, 3–21
groups, 6–19
nodes from database, 11–2
remote boot clients, 11–3
user accounts, 6–12
users from groups, 6–19
virtual disks, 5–16
Denying
group access, 3–18
public access, 3–18
user access, 3–19
Device control libraries, 4–8
creating, 4–10
entries in, 4–8, 4–10
for printers listed on menu, 4–14, 4–16
merging entries, 4–14
Disconnecting
clients, 9–2
Disk quotas
and extending files, 8–7, F–3
and moving user accounts, 6–7
Disk servers, G–5
and maximum disk services on, 7–7
changing cache for, 8–13, 8–14
changing timeout, 7–9, 9–13
configuring, 7–7
database for services, 9–15
data file for, D–1
defining privileges for, 5–13
improving performance on, 8–13
monitoring, 9–12
parameters at startup, 7–7, 8–14, D–1
starting, 9–14
startup file for, 5–13
stopping, 9–14
system parameters required for, 7–8, 8–13, 8–14

Disk services
See also Remote boot clients
See also Virtual disks
access to, 1–3, 5–3
adding applications in, 5–3
and /TYPE qualifier, 5–8
backing up, 9–16
clients connected to, 9–13
connections to, 5–2
contrasted with file services, 1–7
controlling security of, 1–3, 5–1
default locations for, 5–8
deleting, 5–15
dismounting, 5–5
in clusters, 9–14
listing, 9–12
listing access to, 9–13
listing clients, 9–13
listing connections to, 9–13
listing ratings, 5–14
maximum number of, 7–7
modifying access, 5–12
mounting, 5–11
passwords for, 5–3, 5–12
permanent, 5–11
personal, 5–7
ratings for, 5–14
restoring, 9–18
temporary, 5–11
term defined, 5–10
types of, 5–8
Disk space, F–3
See also DISKQUOTA
extending virtual disk size, 5–13
limiting, 5–9
used by files in file services, 8–7, F–3
DISMOUNT DISK command (PCSA Manager), 5–6, 5–16
Dismounting
disk services, 5–5, 5–16
Displaying
See Listing
DOS byte-range locking, 9–11
DOS files
and carriage control, A–2
DOS files (Cont.)
backing up using file server, 9–18
file version limit in, 6–3
in file services, 1–3
in VMS FIXED format, A–7
in VMS STREAM format, A–7
structure of, A–1
using in file services, A–1, A–7
using in VMS, A–7
DOS operating system
listing, 11–4
using files with estimated length, A–5

E

End-of-file pointer (EOF), A–4, A–5, A–7
Entries, 4–8
creating, 4–10
merging, 4–14
Epson printers
creating printer service for, 4–9
creating print queue for, 4–9
Escape key
using with EDT editor, 4–10
using with EVE editor, 4–10
ESS$LAD_STARTUP.DAT file, 7–7, 8–14, D–1
ESS$LAST_STARTUP.DAT file, 7–9, 7–11, E–1
Estimated length, A–4
term defined, 3–13
Ethernet controllers
changing on VAXmates, H–3
Exiting
PCSA Manager Menu, 2–3
Extended LANs, 7–10

F

File access, 3–3, 3–9
File compatibility
in DOS and VMS, 3–13
File extent, 8–7
File locking, F–5
and cache, 8–8
byte-range, 9–11

File locking (Cont.)
in clusters, 9–10
Files
access to in application file services, 3–2
access to in common file services, 3–3, 3–9
actual length of, 3–13
and disk quotas, 8–7, F–3
and open file caching, 8–4, 8–8
and private locks, 9–10
AUTOEXEC.BAT, 6–5
AUTOUSER.BAT, 6–1, 6–6
byte-range locking, 9–11
closing open files, 9–4
ESS$LAD_STARTUP.DAT, 7–7, 8–14, D–1
ESS$LAST_STARTUP.DAT, 7–9, 7–11, E–1
estimated length of, 3–13
fixed format, 3–13
fixed length, 3–13
in a cluster, 9–10
LAD_STARTUP.COM, 5–13
listing open files, 9–3
MODPARAMS.DAT, 7–8, 8–15
PCFS$CACHE_STATISTICS.TXT, 8–4
PCFS$MODPARAMS.DAT, 7–8, 8–15
PCFS$MONITOR.LOG, 8–4
PCFS$STARTUP.LOG, 7–7, 8–12, 9–10
PCFS$STARTUP_PARAMS.DAT, 7–3, 7–4, 8–9, F–1
PCFS_LOGICALS.COM, 3–11
PCFS_PRINT.COM, 4–5
PCFS_SERVER.LOG file, 9–6, 9–7, 9–8
PCFS_STARTUP.COM, 8–13, 9–6
RMS protection in common file services, 3–5, 3–9
sharing in clusters, 9–10
space allocated for and performance, 8–7
stream format, 3–13
SYSTARTUP_V5.COM, 4–5, 4–12
using files in DOS and VMS, 3–13
using in actual length file services, A–5
using in DOS and VMS, 1–3, A–1
using in estimated length file services, A–5
Files (Cont.)
version limit for, 6–3, 9–15
File server log file, 9–11
defining events in, 9–9
displaying, 9–7
messages in, 9–7
name of, 9–7
printing, 9–8
starting a new file, 9–8
term defined, 9–6
using, 9–6
File servers
allocating space for files in, 8–7
and carriage control information, A–4
and locked data, F–5
and VMS priority, 8–13
collecting cache data, 8–3
configuration and performance, 8–1
configuring, 7–2
data file for, F–1
displaying cache use, 8–4
limiting clients, 9–5
limiting open files, 9–5
log file, 9–6, 9–8
monitoring, 9–1
monitoring security breaches, 9–6
parameters at startup, 7–3, F–1
performance, 8–2, 8–13
performance and packet size, 8–6
starting, 7–6, 8–12, 9–10
startup file for, 8–13, 9–6
stopping, 9–10
system parameters required for, 7–4, 8–10
File services
access to, 3–2, 3–18, 3–19
actual length, 3–13, A–4, A–5
adding, 3–9
alias for, 3–20
backing up, 9–16
common, 3–2
contrasted with disk services, 1–7
deleting, 3–21
estimated length, 3–13, A–4, A–5
fixed format, A–7

File services (Cont.)
  fixed-length, A–7
  fixed length format, 3–13
  group access to, 3–18
  in a VAXcluster, 9–10
  limiting connections to, 3–12, 3–20, 9–4
  listing, 9–2
  location for, 3–11
  modifying VMS files in, A–2
  name for, 3–11
  public access to, 3–17, 3–18
  restoring, 9–18
  RMS protection in common services, 3–3
  root directory for, 3–11
  security in, 1–4, 3–1, 3–2
  security of files in, 1–5, 3–9
  stream format, 3–13, A–7
  type of (common or application), 3–11
  user access to, 3–19
  using DOS and VMS files in, A–1
  with carriage control information, A–4
  writing to VMS files in, A–2
Fixed format, 3–20
Fixed length files, 3–13
Fixed length records, 3–13
  in VMS files, A–7
Forms, 4–1, 4–8
  adding, 4–11
  default, 4–4
  for printers listed on PCSA Manager Menu, 4–6
  landscape, 1–3, 4–1
  portrait, 1–3, 4–1
  term defined, 4–4
FORTRAN programs
  creating files compatible with file server, A–5

G

Generic queues, 4–8
  for printers listed on PCSA Manager Menu, 4–6
  name, 4–4
GRANT command (PCSA Manager), 3–21
Granting
Granting (Cont.)
  group access, 1–7, 3–18
  public access, 1–7, 3–18, 6–18
  user access, 1–7, 3–19
Group codes
  for clients, 7–12
  for servers, 7–11
  term defined, 7–10
  with remote boot, 7–12
Groups, 6–16
  adding users to, 6–18
  contrasted with UIC group codes, 6–17
  creating, 6–17
  default, 6–18
  defining, 6–16
  deleting, 6–19
  public, 6–18
  removing users, 6–19
  term defined, 6–1
  using, 6–18

H

Help
  for PCSA Manager commands, 2–9
HP LaserJet printers, 4–3
  setting up, B–1

I

Identifiers, 3–8
  in application file services, 3–2
  in common file services, 3–3
  term defined, 3–2
Installing applications, 3–14, 5–4
Interactive login, 6–3

L

LAD_STARTUP.COM file, 5–13
Landscape forms, 1–3, 4–1
Languages
  selecting for PCSA applications, 6–6
LAST
  See Local Area System Transport
LASTCP

LASTCP (Cont.)
See Local Area System Transport Control Program
Limiting
clients, 7–2, 9–5
connections to disk services, 5–2
connections to file services, 3–12, 3–20, 9–4
maximum disk services, 7–7
open files, 9–5
server access, 7–10
Listing
access to file services, 3–17
client operating systems, 11–4
clients connected to file services, 9–2
clients using disk server, 9–13
connections to disk server, 9–13
connections to file services, 9–2
disk services, 9–12, 9–13
file server cache, 8–4
file server log file, 9–7
file services, 9–2
messages in log file, 9–7
nodes, 12–8
open files, 9–3
remote boot clients, 11–3
users, 6–12
Local area networks (LANs), 7–10
restricting server access, 7–10
Local Area System Transport (LAST), 7–10, 8–16
configuring, 7–9
data file for, E–1
group codes, 7–11
monitoring memory use, 8–16
performance, 8–16
starting, 7–9
startup parameters for, 7–11, E–1
stopping, 7–10
Local Area System Transport Control Program (LASTCP), 7–9, 7–11
Local files, 9–3
Locked data, F–5
Log files
See also Backup log file

Log files (Cont.)
See also File server log file
for backup, 9–17
for cache collection on file server, 8–4
for file server startup, 7–7, 8–12, 9–10
Logicals
for virtual disk locations, 5–7
PCFS$APPLICATION, 3–11
PCFS$COMMON, 3–11
PCFS$LOG_FILES, 8–4, 9–7
PCFS$SERVICE_DATABASE, 9–11
PCSA$EDITOR_COMMAND, 6–6
SYS$SPECIFIC, 9–11
Login
interactive, 6–3
Lookaside lists
term defined, 8–16
LPT1, 6–5

M

Managing
default account, 6–15
overview of server tasks, 1–9
Memory allocation
managing, 8–16
Merging entries
in device control library, 4–14
MODIFY DISK command (PCSA Manager), 5–13
Modifying
AUTOUSER.BAT file, 6–6
MODIFY WORKSTATION command (PCSA Manager), 11–4, H–3
MODPARAMS.DAT file, 7–8, 8–15
Modules, 4–8, 4–15
defining forms, 4–11
Monitoring
disk server activity, 9–12
disk server cache, 8–13
file server activity, 9–1
file server cache, 8–4
file server performance, 8–3
lookaside lists, 8–16
MOUNT DISK command (PCSA Manager), 5–10

Mounting virtual disks, 5–10
  privileges for, 5–10

N

NET ATTRIB command, 3–11
Network key disks, 7–7, 9–12
  See also Remote boot clients
Nodes
  adding, 11–1
  deleting, 11–2
  listing, 12–8
  registered, 11–1
NPAGEDYN parameter, 7–8, G–5
  term defined, 8–14

O

Open file caching, 8–2, 8–4
  delay for, 8–8
  hit rate, 8–4
  setting, 8–7
Open file hit rate
  term defined, 8–4
Open files
  closing, 9–4
  limiting in file services, 9–5
  listing, 9–3
Operating systems
  See Client operating systems
  See DOS operating system
  See VMS operating system
OS/2 files
  backing up using file server, 9–18
  file version limit in, 6–3

P

Packets
  and server performance, 8–6
  size of, 8–6
Page file size, G–4
  PCFS$NUM_OF_WORKSTATIONS parameter and, G–4
  WSMAX parameter and, G–4
Parallel printers
  connected to user's personal computer, 4–1
PASCAL programs
  creating files compatible with file server, A–5
Passwords
  changing, 6–14, 6–15
  defining, 6–3
  expiration of, 6–14
  for disk services, 5–3
  in VMS accounts, 6–14
PATHWORKS Server 3100
  backing up, 12–2
  managing the server, 12–1
  reboot, 12–6
  restore disk, 12–4
  shutdown, 12–6
PCCOMMON file service, 3–7, 6–4
PCDISK utility, 5–17
PCFS$ADDITIONAL_CHANNELS parameter, F–1, G–4
PCFS$APPLICATION logical, 3–11
PCFS$AST_LIMIT parameter, F–1
PCFS$BUFFER_LIMIT parameter, F–1
PCFS$BUFFER_SIZE parameter, 8–8, F–2
PCFS$CACHE_OPEN_FILES parameter, 8–7
PCFS$CACHE_SIZE parameter, 8–7, F–2, G–3
PCFS$CACHE_STATISTICS.TXT file, 8–4
PCFS$CLOSE_DELAY parameter, 8–8, F–2
PCFS$CLUSTER_ROUTING parameter, F–3
PCFS$COMMON logical, 3–11
PCFS$ENQUEUE_LIMIT parameter, F–3
PCFS$EXTEND_BLOCKS parameter, 8–7, F–3
PCFS$EXTENT parameter, F–4
PCFS$FILE_LIMIT parameter, F–4
PCFS$IO_BUFFERED parameter, F–4
PCFS$IO_DIRECT parameter, F–4
PCFS$LOCK_WAIT parameter, F–5
PCFS$LOG_DELAY parameter, F–4

PCFS$LOG_FILES:PCFS$STARTUP_PARAMS.DAT file, F–1
PCFS$LOG_FILES:PCFS_SERVER.LOG file, 9–7
PCFS$LOG_FILES logical, 8–4
PCFS$MAXIMUM_WORKING_SET parameter, F–5
PCFS$MODPARAMS.DAT file, 7–8, 8–15
PCFS$MONITOR.LOG file, 8–4
PCFS$NUM_OF_WORKSTATIONS parameter, 7–3, F–5, G–2, G–4
PCFS$NUM_OF_WORKSTATONS parameter, G–2
PCFS$OPEN_FILES parameter, F–2, G–4
PCFS$OPEN_FILES_PER-WKST parameter, F–6
PCFS$PAGE_FILE parameter, F–6
PCFS$PERCENT_AVAIL_MEM parameter, F–6
PCFS$PRIORITY parameter, 8–13
PCFS$QUEUE_LIMIT parameter, F–7
PCFS$READ identifier, 3–2
PCFS$SERVICE_DATABASE logical, 9–11
PCFS$SPTREQ parameter, F–7
PCFS$STARTUP.LOG file, 7–7, 8–12, 9–10
PCFS$STARTUP_PARAMS.DAT file, 7–3, 7–4, 8–9, F–1
  VMS system resources and, G–2
PCFS$UPDATE identifier, 3–2
PCFS_LOGICALS.COM file, 3–11
PCFS_PRINT.COM file, 4–5
PCFS_SERVER.LOG file, 9–7
PCFS_STARTUP.COM file, 8–13, 9–6
PCSA$EDITOR_COMMAND logical, 6–6
PCSA applications
  selecting languages for, 6–6
PCSA Manager commands
  ADD SERVICE /DIRECTORY, 3–12, 3–13, 3–14
  ADD USER, 6–12
  ADD WORKSTATION, H–5
  CREATE DISK, 5–8, 5–10, 5–13
  DELETE DISK, 5–16
  DISMOUNT DISK, 5–6, 5–16
  GRANT, 3–21
PCSA Manager commands (Cont.)
  help for, 2–9
  MODIFY DISK, 5–13
  MODIFY WORKSTATION, 11–4, H–3
  MOUNT DISK, 5–10
  running, 2–8
  SET DISK_SERVER CHARACTERISTICS , 5–13
  SET DISK_SERVER SERVICE, 5–12, 5–15
  SET FILE_SERVER CHARACTERISTICS , 6–15
  SHOW DISK_SERVER COUNTER, 8–14
  SHOW DISK_SERVER SERVICE, 5–14
  SHOW VERSION, 7–5, 7–8, 8–11, 8–15
  STOP DISK_SERVER CONNECTIONS, 8–14
  using, 2–1, 2–8
PCSA Manager Menu
  default responses to, 2–5
  entering, 2–3
  exiting, 2–3
  moving around in, 2–4
  options available in (illus.), 2–5
  SET FILE_SERVER CHARACTERISTICS , 9–4
  tree diagram of (illus.), 2–5
  using, 2–1
Performance
  in personal computer applications, 8–2
  NPAGEDYN and, 8–14
  on disk server, 8–13
  on file server, 8–2
  on Local Area System Transport, 8–16
Permanent disk services
  term defined, 5–11
Personal computers
  and parallel printers, 4–1
Personal disks
  creating, 5–7
  mounting, 5–10
Physical queues
  name for, 4–4, 4–8, 4–14
  term defined, 4–8
PL/I programs

PL/I programs (Cont.)
- creating files compatible with file server, A–5

Portrait forms, 1–3, 4–1

Ports
- *See* Printer ports

Printer forms
- *See* Forms

Printer output, 4–24
- connecting to services and, 4–24

Printer ports, 4–9
- and printer startup file, 4–5

Printers
- blank pages and, 4–20
- HP LaserJet, B–1
- identifying output, 4–24
- listed on PCSA Manager Menu, 4–2, 4–14
- not listed on PCSA Manager Menu, 4–7, 4–13
- parallel, 4–1
- physical queue, 4–8, 4–14
- reset mode, 4–10
- selecting for user, 6–5
- with DECservers, 4–16
- without VMS queues, 4–7
- with terminal servers, 4–16
- with VMS queues, 4–13

Printer services, 4–1
- access to, 3–19, 4–14
- adding, 4–13
- adding for printers with terminal servers, 4–16
- and VMS print queues, 4–1
- default access to, 3–18, 4–5
- denying access, 3–18, 3–19
- for Epson printers, 4–9
- for printers listed on PCSA Manager Menu, 4–2, 4–14
- for printers not listed on PCSA Manager Menu, 4–7, 4–13
- for printers without VMS queues, 4–2, 4–8
- for printers with VMS queues, 4–13
- granting access, 3–18, 3–19

Printer services (Cont.)
- identifying printer output, 4–24
- LPT1, 6–5
- names for printers listed in menu (table), 4–6
- privileges for, 4–2
- selecting for user, 6–5
- subdirectories for printers listed in menu (table), 4–6

Printer startup file
- creating, 4–5
- customized, 4–5, 4–12
- default, 4–5
- name of, 4–5
- PCFS_PRINT.COM, 4–5
- term defined, 4–5

Printers without VMS queues
- adding printer services for, 4–2
- adding printer services for printers listed on PCSA Manager Menu, 4–2
- adding printer services for printers not listed on PCSA Manager Menu, 4–7

Printers with VMS queues
- adding printer services for, 4–13
- adding printer services for printers listed on PCSA Manager Menu, 4–14
- adding printer services for printers not listed on PCSA Manager Menu, 4–13

Printing
- from personal computers, 4–1
- identifying users' output, 4–24
- using printer services, 4–1

Print jobs
- identifying, 4–24

Print queues
- adding, 4–2, 4–7
- and printer services, 4–1
- creating, 4–12
- for printers listed on PCSA Manager Menu (table), 4–6
- generic, 4–8, 4–14
- physical, 4–8

Proxy files, 9–3

Public access
- denying, 3–18

Public access (Cont.)
term defined, 3–17

Q

Queues
See Print queues

R

Ratings
assigning to disk services, 5–14
term defined, 5–14
Read access
See also Access to files
See also Access to services
for disk services, 5–2
Record attributes
in VMS files, A–4
Record Management System (RMS)
and carriage control, A–1
compared to DOS, A–2
overhead for storing records, A–3
Registered nodes, 11–1
Remote boot clients
and group codes, 7–12
configuring VAXmate clients, H–5, H–8
deleting, 11–3
listing, 11–3
Remote files, 9–3
Reset mode, 4–10
Reset module
preventing blank pages in, 4–20
Restoring
boot database, 11–4
disk services, 9–18
file services, 9–18
PATHWORKS Server 3100, 12–2, 12–4
user accounts, 9–18
Return key
alternatives to, 2–4
RMS FIXED format
in file services, 3–13
RMS protection, 1–5, 3–5
changing, 3–6
RMS protection (Cont.)
on files in common file services, 3–3, 3–9
RMS sequential files
See Sequential files
RMS STREAM format
in file services, 3–13
Run-time parameters
and file server, 7–4, 8–9

S

Save set
name for, 9–19
Security
See also Access to services
and default account, 6–15
and user accounts, 1–6
in application file services, 3–2
in common file services, 3–2, 3–9
in common versus application file services, 1–4
in disk services, 1–3, 5–1, 5–10
in file services, 1–4, 3–1
in user accounts, 6–13
monitoring on file server, 9–6
on files in common file service, 3–5, 3–9
using file server log file to monitor, 9–6
Sending messages, 10–1
Sequential files
term defined, 3–13
SET DIRECTORY command, 6–3
SET DISK_SERVER CHARACTERISTICS command (PCSA Manager), 5–13
SET DISK_SERVER SERVICE command (PCSA Manager), 5–12, 5–15
SET FILE/VERSION_LIMIT command, 6–3
SET FILE/VERSION_LIMIT command (VMS), 6–3
SET FILE_SERVER CHARACTERISTICS command (PCSA Manager), 6–15, 9–4, 9–5
Setting
cache buffer size, 8–8
cache size, 8–7
delay for open file caching, 8–8

Setting (Cont.)
  open file caching, 8–7
SHOW DISK_SERVER CONNECTIONS command (PCSA Manager), 9–13
SHOW DISK_SERVER COUNTER command (PCSA Manager), 8–14
SHOW DISK_SERVER SERVICE command (PCSA Manager), 5–14
SHOW FILE_SERVER command (PCSA Manager), 9–3
SHOW FILE_SERVER CONNECTIONS command (PCSA Manager), 9–2
SHOW FILE_SERVER SERVICES command (PCSA Manager), 9–2
SHOW VERSION command (PCSA Manager), 7–5, 7–8, 8–11, 8–15
Software license agreements, 1–8
Spool subdirectory
  term defined, 4–5
SPTREQ parameters, F–7
Starting
  disk servers, 9–14
  file servers, 7–6, 8–12, 9–10
  Local Area System Transport (LAST), 7–9, 7–10, 7–12
  VMS operating system, 7–4, 8–10
Startup file
  See also AUTOUSER.BAT file
  See also Printer startup file
  for clients, 6–1
  for printer service, 4–5
  for VMS operating system, 4–5, 4–12
Startup parameters
  for disk servers, 7–7, 8–14
  for file servers, 7–3, 7–4, 8–9, F–1
  for Local Area System Transport (LAST), 7–9
STOP DISK_SERVER CONNECTIONS command (PCSA Manager), 8–14, 9–14, 9–18
STOP FILE_SERVER CONNECTIONS command (PCSA Manager), 9–3
STOP FILE_SERVER SESSION command (PCSA Manager), 9–2
Stopping
Stopping (Cont.)
  connections to file services, 9–3
  disk server, 9–14
  file server, 9–10
  Local Area System Transport (LAST), 7–10
Storing applications, 1–7
Stream files, 3–13
  and cache, 8–2
  term defined, 3–13
Stream format
  in VMS files, A–7
SYS$SPECIFIC logical
  using for file server log file, 9–11
SYS$STARTUP:ESS$LAD_STARTUP.DAT file, 8–14
SYS$STARTUP:LAD_STARTUP.COM file, 5–13
SYS$STARTUP:PCFS_PRINT.COM file, 4–5
SYS$STARTUP:SYSTARTUP_V5.COM file, 4–5, 4–12
SYSGEN parameters
  CHANNELCNT, F–1, F–6
  NPAGEDYN, G–5
  NPAGEVIR, G–5
  SPTREQ, F–7
  WSMAX, F–5, F–6
SYSTARTUP_V5.COM file, 4–5, 4–12
System parameters, 7–4, 8–10
  See also AUTOGEN procedure (VMS)
  See also VMS operating system
  and memory, 8–16
  NPAGEDYN, 7–8, 8–14, G–5
System resources
  See VMS operating system
System services
  and file services, 3–2
  disk and file, 11–4
  listing, 11–4

T

Temporary disk services
  term defined, 5–11
Terminal lines, 4–3
Terminal servers
  setting up printers on, 4–16
Text files
  in DOS and VMS, A–2, A–7
Timeout
  changing on disk server, 7–9, 9–13
Tuning
  See Performance

U

USE command, 1–5, 3–3, 3–4, 3–14, 5–4
User accounts
  See VMS accounts
  modifying, 6–6
User Authorization File (UAF), 6–13, 6–15
  See also VMS accounts
User Identification Codes (UIC), 1–5, 3–3
  contrasted with groups, 3–3, 6–17
Usernames
  See VMS usernames
User passwords, 6–3
User profiles
  and adding a user, 6–2
  form for, C–1
Users
  See also AUTOUSER.BAT file
  See also VMS accounts
  access to disk services, 1–3, 5–1
  access to files, 1–5
  access to file services, 1–4, 1–5
  access to printer services, 1–5
  accounts for, 6–3
  adding, 6–2
  adding to groups, 6–18
  connecting to services, 1–5, 3–16, 3–17
  defining name, 6–3
  defining password, 6–3
  deleting accounts for, 6–12

Users (Cont.)
  denying access to file services, 3–19
  granting access to file services, 3–16, 3–19
  listing, 6–12
  modifying their AUTOUSER.BAT file, 6–6
  removing from groups, 6–19
  specifying connections for client startup, 6–4
  startup file for, 6–1
  username for, 1–5

V

VAXclusters, 9–10
  database for services, 9–11
  file server log file and, 9–11
  sharing files, 9–10
VAXmate clients
  adding for remote boot, H–5
  changing Ethernet controller and addresses, H–3
  configuring, H–1
  configuring with remote boot, H–8
  reconfiguring on a PATHWORKS for VMS, H–2
Version limits
  in VMS files, 6–3
Virtual disks
  See also Disk services
  See also Remote boot clients
  access to, 5–13
  allocating space for, 5–9
  assigning password for, 5–10
  choosing location for, 5–7
  creating, 5–7
  default location for, 5–7
  default size, 5–9
  defining access to, 5–13
  deleting, 5–16
  directory for, 5–8
  extending size of, 5–13
  location for, 5–7
  making available to users, 5–7
  mounting, 5–6, 5–10

Virtual disks (Cont.)
  mounting with password, 5–10
VMS accounts, 6–1
  See also Default account
  and printer output, 4–24
  backing up, 9–16
  creating with PCSA Manager Menu, 6–1
  default, 6–15, 6–18
  defining, 6–3
  deleting, 6–12
  file version limit in, 6–3
  moving, 6–7, 6–11
  passwords for, 6–3, 6–14
  restoring, 9–18
  usernames for, 1–5, 6–3
VMS BACKUP command, 9–18
VMS directories
  as file service, 1–3
VMS DISKQUOTA utility
  and extending files, 8–7, F–3
  and moving user accounts, 6–7
VMS files
  and carriage control, A–1
  converting formats of, A–5
  creating for file services, A–5
  in file services, 1–3
  modifying in file services, A–2
  record attributes of, A–4
  structure of, A–1
  using in file services, A–1, A–2
  using programming languages to create, A–5
  with FIXED format, A–7
  without carriage control information, A–7
  with STREAM format, A–7
VMS identifiers, 3–2
VMS operating system
  managing memory, 8–16
  priority in, 8–13
  run-time parameters, 7–4, 8–9
  starting, 7–4, 8–10
  system parameters required for disk server, 7–8, 8–13, 8–14
  system parameters required for file server, 7–4, 8–10
VMS passwords
  defining, 6–3
  expiration of, 6–14
VMS priority
  and file server performance, 8–13
VMS queues
  See Print queues
VMS startup file, 4–5, 4–12
VMS usernames, 1–5
  See also VMS accounts
  and access to files in common file services, 3–4
  and printer output, 4–24
  defining, 6–3

W

Workstations
  See clients
WPS-PLUS
  using files on DOS and VMS, 3–13
WPS-PLUS files
  using in DOS and VMS, A–7
Write access
  See also Access to files
  See also Access to services
  for disk services, 5–2
WSMAX parameter, F–5, F–6

Reader's Comments

PATHWORKS for VMS
Server Administrator's Guide

AA–PAGWC–TK

Your comments and suggestions help us improve the quality of our publications.

Please rate the manual in the following categories:	Excellent	Good	Fair	Poor
Accuracy (product works as described)	□	□	□	□
Completeness (enough information)	□	□	□	□
Clarity (easy to understand)	□	□	□	□
Organization (structure of subject matter)	□	□	□	□
Figures (useful)	□	□	□	□
Examples (useful)	□	□	□	□
Table of contents (ability to find topic)	□	□	□	□
Index (ability to find topic)	□	□	□	□
Page design (overall appearance)	□	□	□	□
Print quality	□	□	□	□

What I like best about this manual: ____________________

____

What I like least about this manual: ____________________

____

Additional comments or suggestions: ____________________

____

____

I found the following errors in this manual:

Page Description

_____ ____________________

_____ ____________________

_____ ____________________

For which tasks did you use this manual?

□ Installation
□ Maintenance
□ Marketing
□ Operation/Use

□ Programming
□ System Management
□ Training
□ Other (please specify) __________

Name/Title ____________________

Company ____________________

Address ____________________

____

Phone ____________________ Date __________

— — Do Not Tear - Fold Here and Tape —

digital

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

DIGITAL EQUIPMENT CORPORATION
CORPORATE USER PUBLICATIONS
PKO3–1/D30
129 PARKER STREET
MAYNARD, MA 01754–9975

— — Do Not Tear - Fold Here and Tape —

Order Number:AA-PAGWC-TK
Printed in the U.S.A.